ISRAEL JOURNAL OF MATHEMATICS, Vol. 40, Nos. 3–4, 1981

# SOME $p$-GROUPS OF FROBENIUS AND EXTRA-SPECIAL TYPE

BY

I. D. MACDONALD

ABSTRACT

Finite $p$-groups $G$ are considered having a normal subgroup $H \neq 1$ with this property: if $x \in G \setminus H$ and $z \in H$ then $x$ is conjugate in $G$ to $xz$. Some theory is developed, and reasonably complicated examples of classes 2 and 3 are constructed.

## §1. Introduction

Let $G$ be a finite group and let $H \neq 1$ be a normal subgroup of $G$.

DEFINITION. $(G, H)$ is said to have property (C) if and only if $x$ is conjugate in $G$ to $xz$, for all $x \in G \setminus H$ and all $z \in H$.

The present paper is devoted to finite $p$-groups with (C).

The above definition is essentially due to A. R. Camina [3]. We explain the context. Camina considers the following (F1) and (F2).

HYPOTHESIS (F1). $G$ is a finite group with a proper normal subgroup $H \neq 1$ and a set of irreducible non-trivial characters of $G, \chi_1, \cdots, \chi_n$, where $n$ is a natural number, such that

(a) $\chi_i$ vanishes on $G \setminus H$ and

(b) there exist natural numbers $\alpha_1, \cdots, \alpha_n > 0$ such that $\Sigma_{i=1}^n \alpha_i \chi_i$ is constant on $H^*$.

HYPOTHESIS (F2). $G$ is a finite group with a proper normal subgroup $H \neq 1$ such that if $x \in G \setminus H$, $x$ is conjugate to $xy$ $\forall y \in H$.

Camina proves that (F1) and (F2) are equivalent. He is chiefly interested in finite groups which are *not* $p$-groups for any prime $p$. As we have indicated, our

Received November 17, 1980 and in revised form July 15, 1981

interest lies exclusively in finite $p$-groups. From now on, therefore, all groups will be finite $p$-groups.

Rather few groups $G$ are known which have an $H$ such that $(G, H)$ has (C). Camina mentions the extra-special $p$-groups, in which we take $H = \delta(G)$ the commutator subgroup of $G$. (Our notation is generally that of Huppert's book [5], in which there is also to be found an account of the special and extra-special $p$-groups.) Other *ad hoc* examples can be produced. We are indebted to the referee for mentioning the semi-direct product $G$ of any cyclic $p$-group by the Sylow $p$-subgroup of its automorphism group, $H$ being the monolith of $G$; he adds "other examples of pairs $(G, H)$, with $G$ a metabelian monolithic $p$-group and $H$ its monolith, are easy to describe".

A depressingly complicated example can be concocted from the group $E_3$ of [6] which reappears in [7] and is example (iii) in §4 of [8]. In the notation of [6] $\zeta(E_3) = \langle z, f_1f_2, e_1e_2e_3f_1\rangle$, and $E_3/\langle z\rangle$ is the Burnside group B(4, 2). We take $G = E_3/\langle f_1f_2, e_1e_2e_3f_1\rangle$ and $H = \zeta(E_3)/\langle f_1f_2, e_1e_2e_3f_1\rangle$ and assert that $(G, H)$ has property (C). The reader will find that routine consideration of cases will establish this assertion.

Our primary objective is to widen the class of known examples and in particular to find non-monolithic examples.

To be more precise, we produce examples $(G, H)$ with (C) where $H = \delta(G)$ and $H$ is central, elementary abelian of order $p^n$, for every prime $p$ and every positive integer $n$. We also give examples in which $G$ has class 3 and $H$ is not central. These results make it plausible that both $H$ and $G/H$ can in general be fairly complicated.

Questions of structure therefore arise. Such theory as we develop is oriented towards our examples. However, some evidence emerges that there is a close relationship between the upper and lower central series of $G$ if $(G, H)$ has (C); the two series could conceivably coincide, particularly those terms which lie in $H$.

## §2. Central series

We start the ball rolling by proving a useful theorem.

It is clear that if $(G, H)$ has (C) and if $N \leq G$, $N < H$ then $(G/N, H/N)$ has (C).

We denote the centre of $G$ by $\zeta(G)$, and put $\zeta_1(G) = \zeta(G)$, while if $r > 1$ then $\zeta_r(G)$ is defined inductively by $\zeta(G/\zeta_{r-1}(G)) = \zeta_r(G)/\zeta_{r-1}(G)$. We also put $\zeta_0(G) = 1$. Further $\gamma_2(G) = \delta(G)$, and if $r > 2$ then $\gamma_r(G)$ is defined as $[\gamma_{r-1}(G), G]$. We put $\gamma_1(G) = G$.

LEMMA 2.1. *If $(G,H)$ has property* (C) *and $G$ has class $c$ then $H=\gamma_r(G)$ and $H=\zeta_{c-r+1}(G)$ for some $r$ satisfying $1<r\leqq c$.*

PROOF. The very definition of (C) shows that if $(G,H)$ has (C) then $\zeta(G)\leqq H$. Then $(G/\zeta(G),H/\zeta(G))$ has (C) if $H\neq\zeta(G)$. Repetition of this process gives $H=\zeta_{c-r+1}(G)$ for some $r$ with $1<r\leqq c$.

Next we use $\gamma_r(G)\leqq\zeta_{c-r+1}(G)$ (see [5] s. 262, 2.7 Satz). Suppose by way of contradiction that

$$\gamma_r(G)<\zeta_{c-r+1}(G)=H.$$

Then $(G/\gamma_r(G),H/\gamma_r(G))$ has (C), and so

$$\gamma_{r-1}(G)/\gamma_r(G)\leqq\zeta(G/\gamma_r(G))\leqq H/\gamma_r(G).$$

Then $\gamma_{r-1}(G)\leqq H=\zeta_{c-r+1}(G)$, which implies that $\gamma_c(G)\leqq\zeta_0(G)=1$, a contradiction. Therefore $\gamma_r(G)=\zeta_{c-r+1}(G)=H$.

We now take $H=\zeta(G)$.

THEOREM 2.2. *Let $(G,H)$ have property* (C), *let $H=\zeta(G)$, and let $G$ have class $c$. Then $\zeta_r(G)/\zeta_{r-1}(G)$ has exponent $p$ for $1\leqq r\leqq c$.*

PROOF. We note the important and useful fact that if $N<\zeta(G)$ then $\zeta(G/N)=\zeta(G)/N$. For it is clear that $\zeta(G/N)\geqq\zeta(G)/N$. By a remark made above $(G/N,H/N)$ has (C), and so $\zeta(G/N)\leqq H/N$. Therefore $\zeta(G/N)=\zeta(G)/N$.

Now we take $N=\zeta(G)^p$. It follows that $\zeta(G/\zeta(G)^p)=\zeta(G)/\zeta(G)^p$. By a well-known commutator identity (see [5], s. 253, 1.3 Hilfsatz) we have $[\zeta_2(G)^p,G]\leqq\zeta(G)^p$. Therefore $\zeta_2(G)^p/\zeta(G)^p\leqq\zeta(G)/\zeta(G)^p$, that is $\zeta_2(G)^p\leqq\zeta(G)$, so $\zeta_2(G)/\zeta_1(G)$ has exponent $p$.

We deduce ([5], s. 266, 2.13 Satz) that $\zeta_{r+1}(G)/\zeta_r(G)$ has exponent $p$ for each $r>1$.

$G/\zeta_{c-1}(G)$ has exponent $p$. But

$$[\gamma_{c-1}(G),\zeta_{c-1}(G)]=1$$

by [5], s. 265, 2.11 Hauptsatz. A commutator identity ([5], s. 253, 1.3 Hilfsatz) now shows that $[\gamma_{c-1}(G),G]$ has exponent $p$, that is $\gamma_c(G)$ has exponent $p$. So does $\zeta(G)$, by Lemma 2.1.

COROLLARY 2.3. *If $(G,H)$ has property* (C) *with $H=\gamma_r(G)$ then $\gamma_i(G)/\gamma_{i+1}(G)$ has exponent $p$ for $r-1\leqq i\leqq c$.*

PROOF. $\gamma_{r-1}(G)/H\leqq\zeta(G/H)$. But $H=\zeta_{c-r+1}(G)$ by the lemma, so

$\zeta(G/H) = \zeta_{c-r+2}(G)/\zeta_{c-r+1}(G)$, which has exponent $p$ by the theorem. Therefore $\gamma_{r-1}(G)/\gamma_r(G)$ has exponent $p$. The corollary follows by a standard result ([5], s. 266, 2.13 Satz).

Corollary 2.4. *If $(G, H)$ has property* (C) *and $G$ has class* 2 *then*
(i) *$G$ is a special $p$-group; and*
(ii) $H = \delta(G)$.

Proof. Clearly $H = \zeta(G) = \delta(G)$, by Lemma 2.1. By Theorem 2.2 both $H$ and $G/H$ have exponent $p$. Therefore

$$H = \phi(G) = \delta(G) = \zeta(G)$$

where $\phi$ denotes Frattini subgroup, and of course $H$ is elementary.

Corollary 2.5. *$(G, H)$ has property* (C) *and $G$ has class* 2 *and $\delta(G)$ is cyclic if and only if $G$ is extra-special and $H = \delta(G)$.*

## §3. Class 2: theory

Let $G$ have class 2, let $H = \delta(G)$, and let $(G, H)$ have (C). By Corollary 2.4, $G$ is a special $p$-group. Since not all $(G, H)$ where $G$ is a special $p$-group have (C), we need a criterion to determine which have (C) and which do not.

In the next result $d$ denotes the minimal number of generators of a finite $p$-group. All matrices have entries from the field $\mathbf{Z}_p$ of $p$ elements.

Theorem 3.1. *Let $G$ be a special $p$-group and let $H = \delta(G)$; let $d(G) = m$ and $d(H) = n$, with*

$$G = \langle a_1, \cdots, a_m \rangle, \qquad H = \langle c_1, \cdots, c_n \rangle. \tag{1}$$

*Suppose that*

$$[a_i, a_j] = c_1^{\alpha_{ij1}} \cdots c_n^{\alpha_{ijn}} \tag{2}$$

*for $1 \leqq i \leqq m$, $1 \leqq j \leqq m$, where each $\alpha_{ijk}$ lies in $\mathbf{Z}_p$, and put $A_k = [\alpha_{jik}]$ for $1 \leqq k \leqq n$.*

*Then the following are equivalent:*
(i) *$(G, H)$ has* (C);
(ii) *if $\psi_1, \cdots, \psi_n \in \mathbf{Z}_p$ are such that $\psi_1 A_1 + \cdots + \psi_n A_n$ is singular then $\psi_1 = 0, \cdots, \psi_n = 0$.*

Proof. A general element $x$ of $G$ has the form $a_1^{\phi_1} \cdots a_m^{\phi_m} c$ where $\phi_1, \cdots, \phi_m \in \mathbf{Z}_p$ and $c \in \delta(G)$. Note that $x \in \delta(G)$ if and only if $\phi_1 = 0, \cdots, \phi_m = 0$. So

$$\begin{aligned}[x, a_i] &= [a_1, a_i]^{\phi_1} \cdots [a_m, a_i]^{\phi_m} \\ &= (c_1^{\alpha_{1i1}} \cdots c_n^{\alpha_{1in}})^{\phi_1} \cdots (c_1^{\alpha_{mi1}} \cdots c_n^{\alpha_{min}})^{\phi_m} \\ &= c_1^{\beta_{i1}} \cdots c_n^{\beta_{in}}\end{aligned}$$

where

$$\beta_{ij} = \alpha_{1ij}\phi_1 + \cdots + \alpha_{mij}\phi_m .$$

Put $B = [\beta_{ij}]$. Thus $B$ is an $m \times n$ matrix. We assert that $B = [A_1\Phi, \cdots, A_n\Phi]$ where $\Phi^t = [\phi_1, \cdots, \phi_m]$ and t denotes transpose. For the $(i, j)$-th entry of $[A_1\Phi, \cdots, A_n\Phi]$ is the $i$-th row of $A_j\Phi$, which is $[\alpha_{1ij}, \cdots, \alpha_{mij}]\Phi$, as required.

Next we show that if either (i) or (ii) holds then $m \geqq n$. Suppose (i) holds. If $x \notin \delta(G)$ then $|G : C(x)| = p^n$ by (C), while $|C(x)| \geqq p^{n+1}$, because $G$ has class 2; so $m > n$. Suppose (ii) holds. The first columns $\gamma_1(A_1), \cdots, \gamma_1(A_n)$ of $A_1, \cdots, A_n$ respectively form a set of $n$ vectors in $m$-dimensional space, so if $n > m$ then $\psi_1\gamma_1(A_1) + \cdots + \psi_n\gamma_1(A_n) = 0$ for some non-zero $\psi_1, \cdots, \psi_n$. It follows that $\psi_1 A_1 + \cdots + \psi_n A_n$ is singular. By (ii) $\psi_1 = 0, \cdots, \psi_n = 0$, a contradiction, so $m \geqq n$.

Clearly $(G, H)$ has (C) if and only if $\operatorname{rank} B = n$ for all $\Phi \neq \mathbf{0}$; note that $B$ is $m \times n$ with $m \geqq n$. Now rank $B = n$ if and only if the columns are linearly independent. These are $A_1\Phi, \cdots, A_n\Phi$. They are linearly independent if and only if $\psi_1 A_1 \Phi + \cdots + \psi_n A_n \Phi = 0$ implies $\psi_1 = 0, \cdots, \psi_n = 0$. This is equivalent to condition (ii).

This completes the proof of Theorem 3.1. Because the power structure of $G$ is not essentially used, it is clear that a vector space form of the theorem could be given.

Next we seek further restrictions on the integers $m, n$ of Theorem 3.1. The manner of definition of $\alpha_{ijk}$ ensures that the matrices $A_1, \cdots, A_n$ are skew-symmetric. So $\psi_1 A_1 + \cdots + \psi_n A_n$ is skew-symmetric. But a skew-symmetric $m \times m$ matrix is singular if $m$ is odd. In our case, therefore, $m$ is even. Put $m = 2d$.

Now consider the equation

$$\det(\psi_1 A_1 + \cdots + \psi_n A_n) = 0.$$

The left-hand side is a polynomial of total degree $m = 2d$ in $n$ unknowns $\psi_1, \cdots, \psi_n$ in $\mathbf{Z}_p$. This polynomial is in fact the square of another, the Pfaffian of $\psi_1 A_1 + \cdots + \psi_n A_n$. So essentially we have an equation $f(\psi_1, \cdots, \psi_n) = 0$ whose left-hand side is a homogeneous polynomial of degree $d$ in $n$ variables.

At this point we need a standard result of Chevalley and Warning; see [4] and

[9]. It states that the number of solutions of a polynomial equation $f(\psi_1, \cdots, \psi_n) = 0$ of total degree $d$ in $n$ variables $\psi_1, \cdots, \psi_n$ in $\mathbf{Z}_p$ is divisible by $p$, provided $n > d$. In particular, if $f$ is homogeneous, so that $\mathbf{0}$ is one solution, then there must be a non-zero solution.

So if $n > d$ then $\det(\psi_1 A_1 + \cdots + \psi_n A_n) = 0$ has a non-zero solution. In our case, therefore, $n \leqq d$.

We have now proved:

THEOREM 3.2. *If the matrices $A_1, \cdots, A_n$ of Theorem* 3.1 *satisfy condition* (ii) *of that Theorem then $m$ is even, and $m \geqq 2n$.*

## §4. Class 2: examples

The matrices $A_1, \cdots, A_n$ of Theorem 3.1 are skew-symmetric. They also satisfy the condition, which is additional in the case $p = 2$, that $\alpha_{iik} = 0$ for $1 \leqq i \leqq m$, $1 \leqq k \leqq n$. If we have a set of such matrices satisfying condition (ii) of Theorem 3.1, then we can construct a group $G$ with $H = \delta(G)$ such that $(G, H)$ has (C) and $A_1, \cdots, A_n$ are its matrices as in the theorem. For instance, we can define the commutator structure of $G$ by (1) and (2) and simply take $a_i^p = 1$ for $1 \leqq i \leqq m$. In general, there will be many choices of $G$.

THEOREM 4.1. *For each prime $p$, each even positive integer $m$ and each positive integer $n$ with $m \geqq 2n$, there is a group $G$ of class* 2 *such that $|G : \delta(G)| = p^m$, $H = \delta(G)$, $|H| = p^n$, and $(G, H)$ has* (C).

PROOF. By the preceding remarks it suffices to find a set of $n$ matrices, each $m \times m$, satisfying Theorem 3.1(ii); we need of course $\alpha_{jik} = -\alpha_{ijk}$ and $\alpha_{iik} = 0$ for appropriate $i, j, k$. It even suffices to find such matrices with $m = 2n$, for the corresponding groups will have factor groups appropriate to each $n$ with $2n \leqq m$.

Given $p$ and $n$, there exists an irreducible monic polynomial of degree $n$ over $\mathbf{Z}_p$. Choose one such polynomial and let $C$ be its companion matrix. If $1 \leqq k \leqq n$ then put $C_k = C^{k-1}$. Put

$$A_k = \begin{bmatrix} 0 & C_k \\ -C_k^t & 0 \end{bmatrix}$$

where t denotes transpose. We assert that $A_1, \cdots, A_n$ satisfy Theorem 3.1(ii).

If $\det(\psi_1 A_1 + \cdots + \psi_n A_n) = 0$ then $\det(\psi_1 C_1 + \cdots + \psi_n C_n) = 0$, so $\det(\psi_1 I + \psi_2 C + \cdots + \psi_n C^{n-1}) = 0$. So put $r(x) = \psi_1 + \psi_2 x + \cdots + \psi_n x^{n-1}$. We have $\det r(C) = 0$, while the characteristic polynomial $q$ of $C$ is irreducible and has degree $n$. If $r$ is not the zero polynomial then we can find, using the division algorithm, a polynomial $s$ satisfying $\det s(C) = 0$ and having smaller degree than $r$. Repetition of this argument gives a contradiction. So $r$ is the zero polynomial; $\psi_1 = 0, \cdots, \psi_n = 0$, as required.

Since the $A_k$ have the required skew-symmetric properties this completes the proof of the theorem.

There is no reason to think that the examples just specified are other than very particular. The reader may verify for himself that a change of generating set for $G$ induces a congruence transformation on the $A_k$. The problem of classifying all $A_1, \cdots, A_n$ satisfying Theorem 3.1(ii) up to congruence looks depressingly hard. One case, however, deserves a mention. If $n = 1$, so that we have the extra-special groups, then a suitable change of generators will present the skew-symmetric matrix $A_1$ in its canonical form; and as $A_1$ is non-singular this form must be

$$\begin{bmatrix} 0 & w_1 \\ -w_1 & 0 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 0 & w_d \\ -w_d & 0 \end{bmatrix}.$$

That is to say, $G$ is exhibited as a central product — a known result about extra-special groups. Even here we do not get an up-to-isomorphism classification, of course, as we have said nothing about the power structure.

## §5. Class 3: theory

We now probe the structure of $G$ in the class-3 case, with $H = \gamma_2(G)$. In saying "$G$ has class 3", we are (as usual) excluding the cases in which $G$ has class 2. While our main aim consists of the examples of §6, Theorem 5.2 is of interest in its own right.

The following notation is used in this section. By $\zeta, \zeta_2, \gamma_2, \gamma_3$ we mean $\zeta(G)$, $\zeta_2(G)$, $\gamma_2(G)$, $\gamma_3(G)$ respectively; $C$ denotes $C_G(\gamma_2(G))$.

The first result is a technical lemma expressing the Jacobi–Witt identity in a useful form. In groups of class 3 this identity is

$$[u, v, w][v, w, u][w, u, v] = 1; \tag{3}$$

see [5], s. 259, Aufgabe 1.

LEMMA 5.1. *Let $G$ be a finite $p$-group of class 3 such that $(G, \gamma_2(G))$ has (C). Choose $b \in C(\gamma_2(G)) \setminus \gamma_2(G)$ and put*

$$B = \langle x \in G : [b, x] \in \gamma_3(G) \rangle.$$

*Then* $B \leqq C$.

PROOF. Choose $x \in B$ and in (3) put $u = x$, $v = b$, $w$ arbitrary. Here $[b, x, w] = 1$ as $x \in B$, and $[x, w, b] = 1$ as $b \in C$. Therefore (3) gives $[w, b, x] = 1$. But $(G, \gamma_2)$ has (C) and $b \not\in \gamma_2$, so $[w, b]$ takes all values in $\gamma_2$ as $w$ varies. It follows that $x \in C$.

THEOREM 5.2. *Let $G$ be a finite $p$-group of class* 3 *such that* $(G, \gamma_2(G))$ *has* (C), *and let*

$$|G : \gamma_2(G)| = p^m, \qquad |\gamma_2(G) : \gamma_3(G)| = p^n.$$

*Then* (i) $(G, \gamma_3(G))$ *has* (C); *and* (ii) $m = 2n$ *and $n$ is even.*

PROOF. We recall from Corollary 2.3 that $G/\gamma_2$, $\gamma_2/\gamma_3$ and $\gamma_3$ all have exponent $p$. Initially we prove the theorem under the additional assumption that $\gamma_3$ has order $p$. Since $|G : C(x)| \leqq p$ for each $x \in \gamma_2$, this implies that $|G : C| \leqq p^n$. As in the proof of Theorem 3.1 $m > n$, so $C > \gamma_2$; Lemma 5.1 will therefore be applicable.

Choose $a \in G \setminus C$ and put

$$A = \langle x \in G : [a, x] \in \gamma_3(G) \rangle.$$

Since $(G/\gamma_3, \gamma_2/\gamma_3)$ has (C) we obtain

$$|G : A| = p^n. \tag{4}$$

Let $b$ and $B$ be as in Lemma 5.1. Note that $a \not\in B$ (for otherwise we would have $a \in C$, a contradiction). It follows that $b \not\in A$. Recall that $b \in C \setminus \gamma_2$. Therefore $C \cap A \leqq \gamma_2$, and so $C \cap A = \gamma_2$.

Next we have

$$|G : C| \leqq p^n \tag{5}$$

as $|\gamma_2 : \gamma_3| = p^n$ and $|\gamma_3| = p$. So by (4) and (5)

$$p^m = |G : \gamma_2| = |G : C \cap A| \leqq |G : C|\,|G : A| \leqq p^{2n}.$$

By Theorem 3.2, $m \geqq 2n$. Therefore $m = 2n$; and (5) becomes

$$|G : C| = p^n. \tag{5'}$$

The inclusion $\zeta \leqq \gamma_2$ holds because $(G, \gamma_2)$ has (C). If $|\gamma_2 : \zeta| = p^k$ then $|G : C| \leqq p^k$, still under the assumption $|\gamma_3| = p$. Therefore $n = k$, and so $\zeta = \gamma_3$.

If $a \in \gamma_2 \backslash \gamma_3$ then $a \not\in \zeta$, and the conjugates of $a$ form the coset $a\gamma_3$. Thus $(G, \gamma_3)$ has (C).

Now we prove that $n$ is even. If $x \in C \backslash \gamma_2$ then $|G : C(x)| = p^{n+1}$ (because $(G, \gamma_2)$ has (C)). So by (5′), $[x, C] \neq 1$, and $x \not\in \zeta(C)$. It follows that $\zeta(C) = \gamma_2(G)$. In particular $\delta(C) \neq 1$.

Let $b$ and $B$ be as in Lemma 5.1. Then $B \leqq C$. But as $(G/\gamma_3, \gamma_2/\gamma_3)$ has (C), $|G : B| = p^n$. Therefore $B = C$. The definition of $B$ now gives $\delta(C) \leqq \gamma_3(G)$. Therefore $\delta(C) = \gamma_3(G)$.

Since $\gamma_2(G) = \zeta(C)$ we have $|G : \zeta(C)| = p^m$ with of course $m = 2n$, and so by (5′) $|C : \zeta(C)| = p^n$. However $|\delta(C)| = |\gamma_3(G)| = p$. By Corollary 2.5 or Theorem 3.2, $n$ is even.

This completes the proof of (i) and (ii) under the assumption that $\gamma_3(G)$ has order $p$. We now relax that assumption. It is necessary to prove only (i).

Choose $x \in \gamma_2 \backslash \gamma_3$ and suppose by way of contradiction that $[x, G] < \gamma_3$. Choose a subgroup $N$ which contains $[x, G]$ and has index $p$ in $\gamma_3$. Let $\gamma_3 = \langle N, z \rangle$ and put $G' = G/N$. Thus $(G', \gamma_3(G'))$ has (C) and $\gamma_3(G')$ has order $p$. Therefore there exists $y \in G$ for which $[xN, yN] = zN$, that is $[x, y] \in zN$. But $[x, y] \in N$ and $z \not\in N$. This is a contradiction. Therefore $[x, G] = \gamma_3$, and $(G, \gamma_3)$ has (C).

Corollary 5.3. *If $G$ is a finite $p$-group of class 3 such that $(G, \gamma_2(G))$ has (C) then $\gamma_2(G) = \zeta_2(G)$ and $\gamma_3(G) = \zeta(G)$.*

Proof. Use Lemma 2.1.

We now take generators and relations:

$$(6) \qquad G = \langle a_1, \cdots, a_{2n} \rangle, \quad \gamma_2(G) = \langle c_1, \cdots, c_n, \gamma_3(G) \rangle, \quad \gamma_3(G) = \langle z \rangle;$$

$$(7) \qquad [a_i, a_j] = c_1^{\alpha_{ij1}} \cdots c_n^{\alpha_{ijn}} z^{\beta_{ij}} \qquad (1 \leqq i \leqq 2n, 1 \leqq j \leqq 2n);$$

$$(8) \qquad [c_i, a_j] = z^{\chi_{ij}} \quad (1 \leqq i \leqq n, 1 \leqq j \leqq 2n).$$

(The element $z$ is of course central in $G$.)

The constants $\alpha_{ijk}, \beta_{ij}, \chi_{ij}$ lie in $\mathbf{Z}_p$ and must satisfy numerous conditions. As before, we put

$$A_k = [\alpha_{jik}] \qquad (1 \leqq k \leqq n).$$

Then the $A_k$ satisfy condition (ii) of Theorem 3.1 because $(G/\langle z \rangle, \gamma_2(G)/\langle z \rangle)$ has (C).

We choose the $a$'s so that

$$\langle a_{n+1}, \cdots, a_{2n}, \gamma_2(G) \rangle \leqq C(\gamma_2(G)).$$

Another way of saying this is that $\chi_{ij} = 0$ for $1 \leqq i \leqq n$ and $n < j \leqq 2n$.

At this point we must give some thought to the structure of $G$ as a group rather than as a group with (C). The main constraint on the commutator structure is given by the Jacobi–Witt identity (3).

We calculate:

$$\begin{aligned} [a_i, a_j, a_k] &= [c_1^{\alpha_{ij1}} \cdots c_n^{\alpha_{ijn}} z^{\beta_{ij}}, a_k] \\ &= [c_1, a_k]^{\alpha_{ij1}} \cdots [c_n, a_k]^{\alpha_{ijn}} \\ &= z^{\omega}, \end{aligned}$$

$$\omega = \alpha_{ij1}\chi_{1k} + \cdots + \alpha_{ijn}\chi_{nk}.$$

Note that if $k > n$ then $a_k \in C(\gamma_2(G))$, so $[a_i, a_j, a_k] = 1$ and the above $\omega$ is 0.

Next we apply (3) with $u = a_i$, $v = a_j$, $w = a_k$ in two special cases.

(i) Let $n < i \leqq 2n$, $n < j \leqq 2n$, $1 \leqq k \leqq n$. Then (3) becomes

$$[a_i, a_j, a_k] = 1$$

and we find that

$$\alpha_{ij1}\chi_{1k} + \cdots + \alpha_{ijn}\chi_{nk} = 0. \tag{9}$$

(ii) Let $1 \leqq i \leqq n$, $1 \leqq j \leqq n$, $n < k \leqq 2n$. Then (3) becomes

$$[a_i, a_k, a_j] = [a_j, a_k, a_i]$$

and we find that

$$\alpha_{ik1}\chi_{1j} + \cdots + \alpha_{ikn}\chi_{nj} = \alpha_{jk1}\chi_{1i} + \cdots + \alpha_{jkn}\chi_{ni}. \tag{10}$$

We now define further matrices as follows:

$$B_k = [\alpha_{k,n+i,j}] \qquad (1 \leqq k \leqq n);$$

$$X = [\chi_{ij}];$$

and we let $x_1, \cdots, x_n$ denote the columns of $X$. Thus $B_k$ is $n \times n$ and $X$ is taken to be $n \times n$; recall that $\chi_{ij} = 0$ if $j > n$. Then (10) becomes

$$B_i x_j = B_j x_i \qquad (1 \leqq i, j \leqq n). \tag{11}$$

We are also concerned with the "lower left" $n \times n$ submatrix of $A_k$, so we put

$$A'_k = [\alpha_{j,n+i,k}] \qquad (1 \leqq k \leqq n);$$

thus $1 \leqq i \leqq n$ and $1 \leqq j \leqq n$ in $A'_k$.

## §6. Class 3: examples

So far we have not produced a single group $G$ of class 3 such that $(G, \gamma_2(G))$ has (C). We shall speedily remedy this lack. The key to the construction is equation (11). This seems intractable in general, but if we choose the $A_k$ to be the special matrices of §4, related to companion matrices, then progress is possible.

LEMMA 6.1. *Let $n$ be a positive integer. Choose a monic polynomial of degree $n$ and let $C$ be its companion matrix. Define matrices $B_1, \cdots, B_n$ as follows: if $1 \leqq i \leqq n$ and $1 \leqq k \leqq n$ then row $i$ of $B_k$ is row $k$ of $C^{i-1}$. Then there exists an $n \times n$ matrix $X$ whose columns $x_1, \cdots, x_n$ satisfy the equations*

$$B_k x_l = B_l x_k \qquad (1 \leqq k \leqq n, 1 \leqq l \leqq n)$$

*if and only if both $X$ and $CX$ are symmetric.*

PROOF. The equations $B_k x_l = B_l x_k$ are equivalent to

$$\rho_i(B_k x_l) = \rho_i(B_l x_k) \qquad (1 \leqq i, k, l \leqq n)$$

where $\rho_i$ denotes row $i$. These are equivalent to each of the three following sets of equations:

$$\rho_i(B_k)x_l = \rho_i(B_l)x_k \qquad (1 \leqq i, k, l \leqq n);$$

$$\rho_k(C^{i-1})x_l = \rho_l(C^{i-1})x_k \qquad (1 \leqq i, k, l \leqq n);$$

$$(C^{i-1}X)^t = C^{i-1}X \qquad (1 \leqq i \leqq n).$$

So we have to show that $C^{i-1}X$ is symmetric for $1 \leqq i \leqq n$ if and only if $X$ and $CX$ are symmetric. Suppose that $X$, $CX$ and $C^{i-1}X$ are symmetric where $i \geqq 2$ is fixed. Then

$$(C^iX)^t = (C^{i-1}X)^tC^t = C^{i-1}X^tC^t = C^{i-1}(CX)^t = C^iX$$

and so $C^iX$ is symmetric. This completes the proof.

LEMMA 6.2. *The equations $B_k x_l = B_l x_k$ of the previous lemma always have a non-singlar solution.*

PROOF. Given $B$ as below we may choose $X$ as indicated:

$$C = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_1 \\ 1 & 0 & \cdots & 0 & a_2 \\ 0 & 1 & \cdots & 0 & a_3 \\ \cdots & & & & \\ 0 & 0 & \cdots & 1 & a_n \end{bmatrix}; \quad X = \begin{bmatrix} -a_2 & -a_3 & \cdots & -a_n & 1 \\ -a_3 & -a_4 & \cdots & 1 & 0 \\ \cdots & & & & \\ -a_n & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

We leave it to the reader to verify that

$$CX = \begin{bmatrix} a_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -a_3 & -a_4 & \cdots & -a_n & 1 \\ 0 & -a_4 & -a_5 & \cdots & 1 & 0 \\ \cdots & & & & & \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix},$$

a symmetric matrix. This completes the proof.

We note in passing that the $X$ just given is in fact $B_n^{-1}$; and that further solutions of the equations are obtained when $X$ is replaced by $CX, C^2X$, etc.

We start the construction of groups. Our examples $G$ are to have generators as in (6); we take $m = 2n$ and we shall want $n$ even. We have to specify the constants $\alpha_{ijk}, \beta_{ij}, \chi_{ij}$ appearing in (7) and (8). The $\alpha_{ijk}$ are to be as in §4; thus $A_k = [\alpha_{jik}]$ for $1 \leqq k \leqq n$ where

$$A_k = \begin{bmatrix} 0 & C_k \\ -C'_k & 0 \end{bmatrix},$$

$C_k = C^{k-1}$, and $C$ is a certain companion matrix. The matrix $[\beta_{ij}]$ is to be $2n \times 2n$, skew-symmetric and $\beta_{ii} = 0$; we also require that the submatrix $[\beta_{ij} : n < i \leqq 2n,\ n < j \leqq 2n]$ is non-singular (note that $n$ is even). Finally the $\chi_{ij}$ are given by the matrix $X$ of the last lemma, with $\chi_{ij} = 0$ for $1 \leqq i \leqq n < j \leqq 2n$.

Now we consider the group structure. It is convenient to take $p > 3$, for then $G$ is a regular $p$-group; we can put $a_i^p = 1$ for $1 \leqq i \leqq 2n$, $G$ has exponent $p$, and we can forget about the power structure. (No doubt there are plenty of examples with $p = 2$ or 3. Those we construct will illustrate once again the richness of the exponent-$p$ variety for $p > 3$.)

We also have to reckon with the commutator structure. This is a matter of verifying the Jacobi–Witt identity (3) with $u, v, w$ from $\{a_1, \cdots, a_{2n}\}$. In certain cases this is rendered easy enough by the presence of blocks of zeros in $A_k$. The harder cases are those related to (9) and (10) of §5. We defined $B_k$ in §5 essentially by the rule: $\gamma_j(B_k) = \gamma_k(A'_j)$, where $\gamma_j$ denotes column $j$. However we defined $B_k$ in the lemmas of this section by the rule: $\rho_i(B_k) = \rho_k(C^{i-1})$ where $\rho_i$ denotes row $i$. It turns out that there is no discrepancy, because of the fact that the latter $B_k$ is symmetric. To see this, let us temporarily denote the $(i, j)$-th entry of $C^k$ by $\gamma_{i,j,k}$. It may be verified that because $C$ is a companion matrix we have $\gamma_{i,j+1,k} = \gamma_{i,j,k+1}$ for $1 \leqq i \leqq n$, $1 \leqq j < n$, $0 \leqq k < n$. Iteration gives $\gamma_{i,j,k} = \gamma_{i,k,j}$ provided $1 \leqq j \leqq n$ and $1 \leqq k \leqq n$. This is the result that proves $B_k$ is symmetric.

So our lemmas apply, and the choice of $X$ ensures that (9) and (10) hold. Hence the Jacobi–Witt identity (3) is verified.

It follows that $G$ has order $p^{3n+1}$ and class 3. (In dealing with the structure of $G$ we have used ideas of the nilpotent quotient algorithm rather freely; see [8]. An alternative approach is to use extension theory.)

Finally we have to show that $(G, \gamma_2(G))$ has (C). There are two cases.

(i) Let $x = x_1x_2$ where $x_1 = a_1^{\phi_1}\cdots a_n^{\phi_n}$ and $x_2 \in C(\gamma_2(G))$. Put $\Phi = [\phi_1, \cdots, \phi_n]$ and suppose that $\Phi \neq \mathbf{0}$. Since $X$ is non-singular there exists $\Psi \neq \mathbf{0}$ for which $\Phi X \Psi = -1$. Put $y = c_1^{\psi_1}\cdots c_n^{\psi_n}$ where $\Psi^t = [\psi_1, \cdots, \psi_n]$. Then

$$\begin{aligned}[x, y] &= [x_1x_2, y] = [x_1, y]\\ &= [a_1^{\phi_1}\cdots a_n^{\phi_n}, c_1^{\psi_1}\cdots c_n^{\psi_n}]\\ &= \prod [c_i, a_j]^{-\psi_i\phi_j}\end{aligned}$$

where the product is taken over $1 \leqq i \leqq n$, $1 \leqq j \leqq n$. By (8) $[x, y] = z$.

(ii) Let $x = x_{21}x_{22}$ where $x_{21} = a_{n+1}^{\phi_{n+1}}\cdots a_{2n}^{\phi_{2n}}$ and $x_{22} \in \gamma_2(G)$. Put $\Phi = [\phi_{n+1}, \cdots, \phi_{2n}]$ and suppose that $\Phi \neq \mathbf{0}$. Since $[\beta_{ij} : n < i \leqq 2n, n < j \leqq 2n]$ is non-singular there exists $\Psi \neq 0$ for which $\Phi[\beta_{ij}]\Psi \neq 0$. Put $y = a_{n+1}^{\psi_{n+1}}\cdots a_{2n}^{\psi_{2n}}$ where $\Psi^t = [\psi_{n+1}, \cdots, \psi_{2n}]$. Then

$$\begin{aligned}[x, y] &= [x_{21}x_{22}, y] = [x_{21}, y]\\ &= [a_{n+1}^{\phi_{n+1}}\cdots a_{2n}^{\phi_{2n}}, a_{n+1}^{\psi_{n+1}}\cdots a_{2n}^{\psi_{2n}}]\\ &= \prod [a_i, a_j]^{\phi_i\psi_j}\end{aligned}$$

where the product is taken over $n < i \leqq 2n$, $n < j \leqq 2n$. By (7) $[x, y] = z$.

We summarize the material of this section in our final result:

THEOREM 6.3. *For each prime $p > 3$ there is a finite $p$-group of class* 3 *such that $(G, \gamma_2(G))$ has property* (C).

## §7. A generalization

The referee has contributed a very neat result which generalizes the evenness of $m$ in Theorem 3.2 and hence the evenness of $n$ in Theorem 5.2.

THEOREM 7.1. *If $(G, H)$ has* (C) *and $|G : H| = p^k$ then $k$ is even.*

PROOF. Let $x_1, x_2$ be elements of $G \setminus H$ such that $x_1H$ and $x_2H$ are conjugate in $G/H$. Then $x_1^y = x_2h$ for some $y \in G$ and some $h \in H$. By (C) $x_2h$ is conjugate to $x_2$ in $G$. Therefore $x_1$ and $x_2$ are conjugate in $G$.

We can assume that $|H| = p$, replacing $G$ by a suitable factor group. Let $r(G)$ denote the number of conjugacy classes in $G$. Then we have

$$r(G) = r(G/H) + p - 1.$$

Congruences of P. Hall give further information about $r(G)$:

$$r(G) \equiv |G| \ (\mathrm{mod}(p^2 - 1)),$$

$$r(G/H) \equiv |G/H| \ (\mathrm{mod}(p^2 - 1));$$

see [5], s. 549, 15.2 Satz. Thus

$$|G| \equiv |G/H| + p - 1 \ (\mathrm{mod}(p^2 - 1)).$$

Since $p^{k+1} \equiv p^k + p - 1$ with $k$ odd gives a contradiction, $k$ is even.

## Acknowledgements

I have to thank Dr. Camina for sending me his $p$-group problem and for interesting me in it, before [3] was published.

Professor John Duncan, University of Stirling, contributed the germ of the idea that a set of matrices satisfying Theorem 3.1 (ii) might be found by looking at a set of matrix powers. He also proved a number of theorems which eventually boiled down to the lemmas of §6. I thank him for his help.

Dr. Stephen D. Cohen, University of Glasgow, provided references [4] and [9], which were quite unknown to me. Dr. Cohen is particularly to be thanked for making the first general construction of matrices satisfying Theorem 3.1 (ii) (and, in doing so, for keeping work going at a crucial stage). Our first attempt at the construction was based on the observation that if $S$ is a *symmetric* $n \times n$ matrix with entries from $\mathbf{Z}_p$ and with irreducible characteristic polynomial, and if each element $x$ of each matrix in $\{I, S, \cdots, S^{n-1}\}$ is replaced by $\left[\begin{smallmatrix} 0 & x \\ -x & 0 \end{smallmatrix}\right]$, then a set of matrices with the required properties results. Dr. Cohen gave a method of constructing $S$ for each $n$ and for "large" $p$ (depending on $n$); however it has been pointed out that his results are contained in two papers of Bender ([1], [2]).

Finally I have to thank the referee for his careful and generous help. In addition to pinpointing various false statements he is responsible for an improvement to Theorem 2.2, for Corollary 2.3, and in particular for major improvements to Theorem 5.2 and to its proof. Theorem 7.1 is also due to him.

## References

1. E. A. Bender, *Classes of matrices over an integral domain*, Illinois J. Math. **11** (1967), 697–702.
2. E. A. Bender, *Characteristic polynomials of symmetric matrices*, Pacific J. Math. **25** (1968), 433–441.
3. A. R. Camina, *Some conditions which almost characterize Frobenius groups*, Israel J. Math. **31** (1978), 153–160.
4. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1935), 73–75.
5. B. Huppert, *Endliche Gruppen. I*, Springer-Verlag, Berlin–Heidelberg–New York, 1967.
6. I. D. Macdonald, *Some examples in the theory of groups*, Mathematical Essays Dedicated to A. J. Macintyre, Ohio Univ. Press, Athens, Ohio, 1970, pp. 263–269.
7. I. D. Macdonald, *An application of coset enumeration*, Austral. Comput. J. **6** (1974), 46–48.
8. I. D. Macdonald, *A computer application to finite p-groups*, J. Austral. Math. Soc. **17** (1974), 102–112.
9. E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1935), 76–83.

Department of Mathematics
University of Stirling
Stirling, Scotland