Glasgow Math. J. **44** (2002) 443–453. © 2002 Glasgow Mathematical Journal Trust.
DOI: 10.1017/S0017089502021004З Printed in the United Kingdom

FINITE p-GROUPS IN WHICH EVERY CYCLIC SUBGROUP IS 2-SUBNORMAL

ELIZABETH A. ORMEROD

Mathematics Department, Mathematical Sciences Institute, Australian National University, Canberra ACT 0200, Australia
e-mail: Elizabeth.Ormerod@anu.edu.au

(Received 8 January, 2001; accepted 18 June, 2001)

Abstract. This paper investigates finite p-groups, $p \geq 5$, in which every cyclic subgroup has defect at most two. This class of groups is often denoted by $\mathcal{U}_{2,1}$. The main result is a theorem which characterises these groups by identifying a family of groups in $\mathcal{U}_{2,1}$, and showing that any finite p-group in $\mathcal{U}_{2,1}$, with $p \geq 5$, must be a homomorphic image of one of these groups.

2000 *Mathematics Subject Classification*. Primary 20D15. Secondary 20D35.

Introduction. In this paper we characterise finite p-groups ($p \geq 5$) in which every cyclic subgroup is subnormal of defect at most two. Let $\mathcal{U}_d$ denote the class of all groups in which every subgroup is subnormal of defect at most d, and let $\mathcal{U}_{d,n}$ denote the class of groups in which every n-generator subgroup has defect at most d. In the case $d = 1$, $\mathcal{U}_d$ is the class of Dedekind groups, and $\mathcal{U}_{1,1} = \mathcal{U}_1$. For $d = 2$, $\mathcal{U}_{2,1}$ is different from $\mathcal{U}_2$ as shown by Ormerod [**4**] for 3-groups, and Parmeggiani [**5**] for p-groups, $p \geq 3$.

In terms of this notation, we investigate the groups $\mathcal{U}_{2,1}$. Restricted to 2-generator p-groups, p odd, Mahdavianary [**3**] has shown that $\mathcal{U}_{2,1} = \mathcal{U}_2$, and that any group in $\mathcal{U}_{2,1}$ has nilpotency class at most three. Further he has shown that any group $G \in \mathcal{U}_{2,1}$ if and only if $[v, u, u] \in \langle u \rangle$ for all u and v in G. Using this, and the regularity of p-groups in $\mathcal{U}_{2,1}$, we prove the following result.

THEOREM A. *Let G be a finite p-group, $p \geq 5$. Then $G \in \mathcal{U}_{2,1}$ if, and only if, G is a homomorphic image of a group $G_p(r_1, \ldots, r_n)$, where $1 \leq r_1 \leq r_2 \leq \cdots \leq r_n$ and*

$$G_p(r_1, \ldots, r_n) = < a_1, b_1, \ldots, a_n, b_n : [b_i, a_i, a_i] = a_i^{3p^{r_i}}, [b_i, a_i, b_i] = b_i^{3p^{r_i}}, [x, a_i, b_i] =$$
$$[b_i, x, a_i] = x^{p^{r_i}}, [x, a_i, a_i] = [x, a_i, x] = [x, b_i, b_i] = [x, b_i, x] = 1,$$
$$[y, a_i, a_j] = [y, a_j, a_i] = [y, b_i, b_j] = [y, b_j, b_i] = 1, [y, a_i, b_j] =$$
$$[y, b_j, a_i] = 1, \gamma_4(G_p(r_1, \ldots, r_n)) = 1 >$$

where $1 \leq i, \quad j \leq n, \quad i \neq j, \quad x \in \{a_1, b_1, \ldots, a_n, b_n\} \backslash \{a_i, b_i\}, \quad y \in \{a_1, b_1, \ldots, a_n, b_n\} \backslash \{a_i, b_i, a_j, b_j\}$.

While writing this paper I was made aware of a similar unpublished result contained in the dissertation of M. Stadelmann [**6**]. For a group G, P. Hall [**2**] defined an ordered set of elements $p_1, \dots, p_r$ of order $\pi_1, \dots, \pi_r$ respectively, ($\pi_i \geq 1$, $i = 1, \dots, r$) as a uniqueness basis of G if every element $p \in G$ can be expressed uniquely

$$p = p_1^{x_1} \dots p_r^{x_r}$$

with $0 \leq x_i < \pi_i$ ($i = 1, \dots, r$).

Hall also showed that every regular p-group has a uniqueness basis. Stadelmann in his dissertation showed that if G is a p-group in $\mathcal{U}_{2,1}$ on n generators ($p > 3$), then there exists a uniqueness basis for G, and for each $i, j \in \{1, \dots, n\}$ there exist integers ρ_{ij} and $r_{ij} \geq 0$ such that $r_{ij} = r_{ji}$, $\rho_{ij} = -\rho_{ji}$, $r_{ii} = \rho_{ii} = 0$, $(\rho_{ij}, p) = 1$, for $i \neq j$,

$$[x_j, x_i, x_i] = x_i^{\rho_{i,j} p^{r_{ij}}}, \qquad \text{for all} \quad i, j \in \{1, \dots, n\}$$

and

$$[x_k, x_i x_j x_k, x_i x_j x_k] = (x_i x_j x_k)^{\rho_{ik} p^{r_{ik}} + \rho_{jk} p^{r_{jk}}} \qquad \text{for all} \quad i, j, k \in \{1, \dots, n\}.$$

Also, if G is a p-group with $\gamma_4(G) = 1$, and a basis $x_1, \dots, x_n$ satisfying these relations, then $G \in \mathcal{U}_{2,1}$.

The work in this paper is quite consistent with Stadelmann's work but gives a much clearer picture of groups in $\mathcal{U}_{2,1}$. Having found such a characterisation of groups in which every cyclic subgroup is 2-subnormal it remains to find more information about $\mathcal{U}_2$, the class of groups in which every subgroup is 2-subnormal. As mentioned earlier, $\mathcal{U}_2$ is a proper subset of $\mathcal{U}_{2,1}$, so the result in this paper should be helpful. Other subclasses of $\mathcal{U}_{2,1}$ have also been defined, namely $\mathcal{N}$, the class of groups in which every normaliser is normal, and C, the class of groups in which the commutator subgroup normalises every subgroup. The class $\mathcal{N}$ is a proper subset of $\mathcal{U}_2$ (Parmeggiani [**5**]) and for p-groups, when p is odd, the class $\mathcal{C}$ coincides with $\mathcal{W}_2$, the class of groups of Wielandt length two. However, it is not known whether or not the class of p-groups (p odd) in $\mathcal{N}$ coincides with those in $\mathcal{C}$.

Proof of Theorem A. Throughout the rest of the paper assume that $p \geq 5$. The proof of Theorem A is quite long and has many tedious calculations. We aim to keep these to a minimum, subject to providing sufficient evidence of their accuracy. The first step is to prove the sufficiency of Theorem A.

LEMMA 1. *Let $G_p(r_1, \dots, r_n)$ be a group with the presentation given in the statement of Theorem A. Then $G_p(r_1, \dots, r_n) \in \mathcal{U}_{2,1}$.*

Proof. Put $G = G_p(r_1, \dots, r_n)$, $r = r_1$, and note that G is a regular p-group. Since $r \leq r_2 \leq \dots \leq r_n$, the relations imply that $\gamma_3(G) = \langle a_1^{p^r}, b_1^{p^r}, \dots, a_n^{p^r}, b_n^{p^r} \rangle$. It follows that $\gamma_2(G)$ has exponent p^r and each generator has order p^{2r}. Since G is regular this is enough to show that G has exponent p^{2r}.

For any $u \in G$ we can write

$$u = a_1^{\alpha_1} b_1^{\beta_1} \dots a_n^{\alpha_n} b_n^{\beta_n} u'$$

where $u' \in \gamma_2(G)$ and $0 \le \alpha_i, \beta_i < p^r$. Also $u^{p^r} = a_1^{\alpha_1 p^r} b_1^{\beta_1 p^r} \dots a_n^{\alpha_n p^r} b_n^{\beta_n p^r}$. To show that $G \in \mathcal{U}_{2,1}$ it will be sufficient to show that $[x, u, u] \in \langle u \rangle$ for all $x \in \{a_1, b_1, \dots, a_n, b_n\}$. Let $x = a_i$, $1 \le i \le n$. Then

$$\begin{aligned}
[x, u, u] &= [a_i, a_1^{\alpha_1} b_1^{\beta_1} \dots a_n^{\alpha_n} b_n^{\beta_n} u', a_1^{\alpha_1} b_1^{\beta_1} \dots a_n^{\alpha_n} b_n^{\beta_n} u'] \\
&= [a_i, a_1^{\alpha_1} b_1^{\beta_1} \dots a_n^{\alpha_n} b_n^{\beta_n}, a_1^{\alpha_1} b_1^{\beta_1} \dots a_n^{\alpha_n} b_n^{\beta_n}] \\
&= \prod_{j,k} [a_i, a_j^{\alpha_j}, a_k^{\alpha_k}][a_i, a_j^{\alpha_j}, b_k^{\beta_k}][a_i, b_j^{\beta_j}, a_k^{\alpha_k}][a_i, b_j^{\beta_j}, b_k^{\beta_k}] \\
&= \Big(\prod_{j \neq i} [a_i, a_j^{\alpha_j}, b_j^{\beta_j}][a_i, b_j^{\beta_j}, a_j^{\alpha_j}][a_i, a_j^{\alpha_j}, b_i^{\beta_i}][a_i, b_i^{\beta_i}, a_j^{\alpha_j}][a_i, b_j^{\beta_j}, b_i^{\beta_i}][a_i, b_i^{\beta_i}, b_j^{\beta_j}]\Big) \\
&\qquad\qquad \times [a_i, b_i^{\beta_i}, a_i^{\alpha_i}][a_i, b_i^{\beta_i}, b_i^{\beta_i}] \\
&= \Big(\prod_{j \neq i} a_i^{\alpha_i \beta_j p^{r_j}} a_i^{-\alpha_i \beta_j p^{r_j}} a_j^{-\alpha_j \beta_i p^{r_i}} a_j^{-2\alpha_j \beta_i p^{r_i}} b_j^{-\beta_j \beta_i p^{r_i}} b_j^{-2\beta_j \beta_i p^{r_i}}\Big) \\
&\qquad\qquad \times a_i^{-3\alpha_i \beta_i p^{r_i}} b_j^{-3\beta_i^2 p^{r_i}} \\
&= u^{-3\beta_i p^{r_i}}.
\end{aligned}$$

A similar calculation shows that $[b_i, u, u] = u^{3\alpha_i p^{r_i}}$. Hence $G \in \mathcal{U}_{2,1}$. □

We now move to the rest of the proof of Theorem A. The proof relies very much on the facts that $G_p(r_1, \dots, r_n)$ has nilpotency class three, and that $p \ge 5$, ensuring that $G_p(r_1, \dots, r_n)$ is a regular group. The choice of generators is also crucial. Since 2-generator groups in $\mathcal{U}_{2,1}$ belong to $\mathcal{W}_2$, the class of groups of Wielandt length two, some properties of these groups are used extensively. When p is an odd prime, if a group G has Wielandt length two, the commutator subgroup G' is in the Wielandt subgroup. Elements of the Wielandt subgroup induce power automorphisms, and for regular finite p-groups, power automorphisms are universal (see Cooper [**1**, 5.3.1]). Hence if w is an element of the Wielandt subgroup of a regular finite p-group G, then there is an integer n such that $[w, g] = g^n$ for all $g \in G$. It follows then that if x is an element of maximal order in G and $[w, x] = x^m$ for some integer m, then $[w, g] = g^m$ for all $g \in G$. In particular, if $[w, x] = 1$ then $[w, g] = 1$ for all $g \in G$. Let $g,\ h$ be elements of a group $G \in \mathcal{U}_{2,1}$. Since $\langle g, h \rangle$ has Wielandt length two, there are integers α and $r \ge 1$ such that $[g, h, x] = x^{\alpha p^r}$ for all $x \in \langle g, h \rangle$. The integer α is not unique, since if $|x| = p^m$, $x^{\alpha p^r} = x^{\alpha(p^r + p^m)} = x^{\alpha(1+p^{m-r})p^r}$. However, the integer r remains unchanged. If $[g, h, x] \neq 1$ for all $x \in \langle g, h \rangle$, put

$$r_{gh} := \{r : [g, h, x] = x^{\alpha p^r} \text{ for all } x \in \langle g, h \rangle, (\alpha, p) = 1\}.$$

If $[g, h, x] = 1$ for all $x \in \langle g, h \rangle$, put $r_{gh} := \infty$. For every $g \in G$, set

$$\mathcal{R}(g) := \{r_{gh} : h \in G\}.$$

Also we use $\Phi(G)$ to denote the Frattini subgroup of G.

https://doi.org/10.1017/S0017089502030094 Published online by Cambridge University Press

LEMMA 2. *Let G be a group in* $\mathcal{U}_{2,1}$ *of class 3. Then*

(i) *there exists* $a \in G$ *of maximal order and* $x \in G$ *such that* $[x, a, a] \neq 1$,

(ii) *there exists a of maximal order in G and* $b \in G \backslash \langle a \rangle \Phi(G)$ *such that* $[b, a, a] \neq 1$.

Proof. (i) If $[v, u, u] = 1$ for all v, $u \in G$, then G has class 2, contrary to the assumption. So there exist u and v in G such that $[v, u, u] \neq 1$. If u is of maximal order, the proof is complete. If v is of maximal order, $[v, u, u] \neq 1$ implies $[v, u, v] \neq 1$ and again the proof is complete. If neither u nor v is of maximal order, let a be an element of maximal order. Then $|av| = |a|$ and $[av, u, u] = [a, u, u][v, u, u]$, where either $[av, u, u]$ or $[a, u, u]$ is non trivial. If $[a, u, u] \neq 1$, then $[a, u, a] \neq 1$, giving the required result. A similar result follows if $[av, u, u] \neq 1$.

(ii) From part (i) we can find x and a such that $[x, a, a] \neq 1$. If $x \notin \langle a \rangle \Phi(G)$, there is nothing to prove. If $x \in \langle a \rangle \Phi(G)$, choose $b \in G \backslash \langle a \rangle \Phi(G)$. Then $bu \in G \backslash \Phi(G)$ and either $[b, a, a]$ or $[bu, a, a]$ is non trivial. □

THEOREM 3. *Let G be a finite 3-generator p-group in* $\mathcal{U}_{2,1}$ *of class 3. Then there exist generators* $\{a, b, c\}$ *for G such that a has maximal order in G, and G has relations:*

$$[b, a, a] = a^{3p^r}, \quad [b, a, b] = b^{3p^r},$$
$$[c, a, b] = [b, c, a] = c^{p^r},$$
$$[c, a, a] = [c, a, c] = [c, b, b] = [c, b, c] = 1.$$

Proof. Choose a and b in G such that

(i) a is of maximal order in G,

(ii) $\{a, b\}$ can be extended to a set of (non redundant) generators for G, and

(iii) r_{ab} is minimal in $\cup_a \mathcal{R}(a)$ for a of maximal order in G, and b satisfying (ii).

Lemma 2 ensures that this choice is possible. Put $r = r_{ab}$. Then $[b, a, a] = a^{\alpha p^r}$ and $[b, a, b] = b^{\alpha p^r}$. Let $\{a, b, y\}$ be a set of generators for G. Since G is in $\mathcal{U}_{2,1}$ and every 2-generator subgroup is in $\mathcal{W}_2$ we can assume that G has the following relations;

$$[b, a, a] = a^{\rho p^r}, \quad [b, a, b] = b^{\rho p^r},$$
$$[y, a, a] = a^{\sigma p^s}, \quad [y, a, y] = y^{\sigma p^s},$$
$$[y, b, b] = b^{\tau p^t}, \quad [y, b, y] = y^{\tau p^t},$$

where ρ, σ and τ are integers and $(\rho\sigma\tau, p) = 1$, and r, s and t are positive integers. By the choice of a and b, $s \geq r$. By taking suitable powers of b and y we may assume that $\sigma = \tau = 1$. Since G has class three, a^{p^r}, b^{p^r}, a^{p^s}, y^{p^s}, b^{p^t} and y^{p^t} are central. Since the group is regular and $r \leq s$, $1 = [y, a^{p^r}] = [y, a]^{p^r} = [y^{p^r}, a]$. Similarly $[y^{p^r}, b] = 1$, $[a^{p^t}, y] = 1$ and $[a^{p^t}, b] = 1$. So if $m = \min\{r, t\}$, then $\{a^{p^m}, b^{p^m}, y^{p^m}\} \subseteq \zeta(G)$.

Assume that $[y, a, a] \neq 1$. If $[y, a, a] = 1$, then $[y, a, y] = 1$, making the following step unnecessary. Put $x = y^{\rho} b^{p^{s-r}}$. Then

$$[x, a, a] = [y^{\rho}, a, a][b^{p^{s-r}}, a, a] = a^{\rho p^t}(a^{\rho p^r})^{-p^{t-r}} = 1.$$

Since $|x| \leq |a|$, the regularity of the group gives $[x, a, x] = 1$. Also $[x, b, b] = b^{\rho p^t}$ and $[x, b, x] = x^{\rho p^t}$. So $G = \langle a, b, x \rangle$ and has relations

https://doi.org/10.1017/S0017089502030094 Published online by Cambridge University Press

$$[b, a, a] = a^{\rho p^r}, \quad [b, a, b] = b^{\rho p^r},$$
$$[x, b, b] = b^{\rho p^t}, \quad [x, b, x] = x^{\rho p^t},$$
$$[x, a, a] = [x, a, x] = 1.$$

By taking a suitable power of b we can adjust ρ. For convenience in the next step, choose $\rho = 3$.

We get further information about G by considering 2-generator subgroups of G. Each 2-generator subgroup of G has Wielandt length two with the property that its commutator subgroup is in its Wielandt subgroup. In $\langle a, bx\rangle$,

$$[a, bx, a] = [a, b, a][a, x, a] = a^{-3p^r}.$$

Hence $[a, bx, bx] = (bx)^{-3p^r} = b^{-3p^r}x^{-3p^r}$. On expansion

$$[a, bx, bx] = [a, b, b][a, b, x][a, x, b][a, x, x] = b^{-3p^r}[a, b, x][a, x, b].$$

Put $w = [x, a, b]$. Then $[a, b, x] = wx^{-3p^r}$, and from the Jacobi identity, $[x, b, a] = w^2x^{-3p^r}$. If $|b| \geq |x|$, consider $\langle b, ax\rangle$. Here

$$[b, ax, b] = [b, a, b][b, x, b] = b^{3p^r}b^{-3p^t} = b^{3(p^r-p^t)}.$$

From this, $[b, ax, g] = g^{3(p^r-p^t)-\lambda p^l}$ for $g \in \langle b, ax\rangle$, where $(\lambda, p) = 1$ and $b^{p^l} = 1$ and by the assumption on the orders of b and x, $x^{p^l} = 1$. Consequently,

$$[b, ax, ax] = (ax)^{3(p^r-p^t)-\lambda p^l} = a^{3(p^r-p^t)}x^{3(p^r-p^t)}a^{-\lambda p^l}.$$

Also

$$\begin{aligned}[b, ax, ax] &= [b, a, a][b, a, x][b, x, a][b, x, x] \\ &= a^{3p^r}w^{-1}x^{3p^r}w^{-2}x^{3p^r}x^{-3p^t} \\ &= a^{3p^r}x^{3p^r-3p^t}w^{-3}x^{3p^r},\end{aligned}$$

giving

$$w^3 = x^{3p^r}a^{3p^t}a^{\lambda p^l}.$$

If $a^{p^l} = 1$, then $w = x^{p^r}a^{p^t}$. If $a^{p^l} \neq 1$, put $3p^t + \lambda p^l = 3\bar{\tau}p^{\bar{t}}$. Then $[x, b, b] = b^{3\bar{\tau}p^{\bar{t}}}$, $[x, b, x] = x^{3\bar{\tau}p^{\bar{t}}}$, and $w = x^{p^r}y^{\bar{\tau}p^{\bar{t}}}$. By choosing a suitable power of x, we may assume $\bar{\tau} = 1$. We have shown that the following relations hold in G:

$$[b, a, a] = a^{3p^r}, \quad [b, a, b] = b^{3p^r},$$
$$[x, b, b] = b^{3p^t}, \quad [x, b, x] = x^{3p^t},$$
$$[x, a, b] = a^{p^t}x^{p^r}, \quad [b, x, a] = a^{-2p^t}x^{p^r}$$
$$[x, a, a] = [x, a, x] = 1$$

where t represents t or $\bar{t}$, as necessary. The same result is achieved by a similar calculation if $|x| > |b|$.

If $t < r$, put $a' = ay^{p^{r-t}-1}$. Then $|a'| = |a|$, and $[b, a', a'] = (a')^{3p^t}$, $[b, a', b] = b^{3p^t}$, contradicting the choice of a and b. If $t \geq r$, put $c = xa^{p^{t-r}}$. Then G has the required relations. □

THEOREM 4. *Let G be a finite p-group in* $\mathcal{U}_{2,1}$. *Then there exists a set of generators* $\{a, b, x_3, \ldots, x_n\}$ *for G, where a is of maximal order in G, and the following relations are satisfied:*

$$[b, a, a] = a^{3p^r}, \quad [b, a, b] = b^{3p^r},$$
$$[x, a, b] = [b, x, a] = x^{p^r},$$
$$[x, a, a] = [x, a, x] = [x, b, b] = [x, b, x] = 1, \gamma_4(G) = 1,$$

where $x \in \{x_3, \ldots, x_n\}$.

Proof. Choose a and b in G such that
(i) a is of maximal order in G,
(ii) $\{a, b\}$ can be extended to a set of (non redundant) generators for G, and
(iii) r_{ab} is minimal in $\cup_a \mathcal{R}(a)$ for a of maximal order in G, and b satisfying (ii).

Put $r = r_{ab}$. Let $\{a, b, y_3, \ldots y_n\}$ be a set of generators for G. Put $H_i = \langle a, b, y_i \rangle$. As in Theorem 3, each group H_i has generators $\{a, b_i, x_i\}$ satisfying

$$[b_i, a, a] = a^{3p^r}, \quad [b_i, a, b_i] = b_i^{3p^r}$$
$$[x_i, a, b_i] = [b_i, x_i, a] = x_i^{p^r}$$
$$[x_i, a, a] = [x_i, a, x_i] = [x_i, b_i, b_i] = [x_i, b_i, x_i] = 1, \gamma_4(G) = 1.$$

This almost completes the proof of the theorem, except that each b_i is a (possibly different) power of the original element b. However, since each b_i satisfies $[b_i, a, a] = a^{3p^r}$ and $[b_i, a, b_i] = b_i^{3p^r}$ and b_i only differs from b_j by a power of b, b_j will also satisfy $[x_i, a, b_j] = [b_j, x_i, a] = x_i^{p^r}$. So any b_i will be suitable to satisfy the relations given in the statement of the theorem. For convenience, choose $b = b_3$. □

The statement of Theorem 4 does not yet give a presentation for a group in $\mathcal{U}_{2,1}$, but perhaps it can be thought of as a "partial presentation". The designation "partial presentation" is used for convenience and refers to the presentation of a group of which the group having the "partial presentation" is a quotient. Call this partial presentation $\mathcal{P}_1$. We define a series of partial presentations, $\mathcal{P}_k$, on the generating set D_k, where

$$D_k = \{a_1, b_1, \ldots, a_k, b_k, x_{2k+1}, \ldots, x_n\},$$

and a_i is of maximal order in $\langle a_i, b_i, \ldots, a_k, b_k, x_{2k+1}, \ldots, x_n \rangle$, $1 \leq i \leq k$. The partial presentation $\mathcal{P}_1$ is given by:

$$[b_1, a_1, a_1] = a_1^{3p^{r_1}}, \quad [b_1, a_1, b_1] = b_1^{3p^{r_1}},$$
$$[x, a_1, b_1] = [b_1, x, a_1] = x^{p^{r_1}},$$
$$[x, a_1, a_1] = [x, a_1, x] = [x, b_1, b_1] = [x, b_1, x] = 1,$$

https://doi.org/10.1017/S0017089502030094 Published online by Cambridge University Press

where $x \in D_k \backslash \{a_1, b_1\}$. The partial presentation $\mathcal{P}_k$ is given by:

$$\begin{aligned}
&[b_i, a_i, a_i] = a_i^{3p^{r_i}}, \quad [b_i, a_i, b_i] = b_i^{3p^{r_i}},\\
&[x, a_i, b_i] = [b_i, x, a_i] = x^{p^{r_i}},\\
&[x, a_i, a_i] = [x, a_i, x] = [x, b_i, b_i] = [x, b_i, x] = 1,\\
&[y, a_i, a_j] = [y, a_j, a_i] = [y, b_i, b_j] = [y, b_j, b_i] = 1,\\
&[y, a_i, b_j] = [y, b_j, a_i] = 1,
\end{aligned}$$

where $i, j \in \{1, \ldots, k\}$, $i \neq j$, and $x \in D_k - \{a_i, b_i\}$, $y \in D_k - \{a_i, b_i, a_j, b_j\}$.

THEOREM 5. *Let G be a finite p-group of class three in $\mathcal{U}_{2,1}$ on n generators, and let k be a positive integer such that $2k \leq n$. Then there exists a set of generators D_k as given above, such that G has a partial presentation $\mathcal{P}_k$.*

The next series of lemmas is used in the proof of this theorem. In these lemmas the group G has class three and is defined as follows:

$$G = \langle a_1, b_1, \ldots, a_{k-1}, b_{k-1}, x_{2k-1}, \ldots, x_n \rangle$$

where the generators satisfy the relations $\mathcal{P}_{k-1}$, $2 \leq 2k \leq n$, and

$$H_i = \langle a_i, b_i, \ldots, a_{k-1}, b_{k-1}, x_{2k-1}, \ldots, x_n \rangle,$$

and a_i is of maximal order in H_i, $1 \leq i \leq k-1$. Also

$$H_k = \langle x_{2k-1}, \ldots, x_n \rangle$$

LEMMA 6. *Let a be an element of maximal order in the subgroup H_k of G and let $b \in H_k$ such that $[b, a, a] = a^{3p^t}$, $[b, a, b] = b^{3p^t}$ for some integer t. Then there exists an integer r such that*

$$[b, a, a] = a^{3\rho p^r}, \quad [b, a, b] = b^{3\rho p^r} \quad \textit{and} \quad [a_1, a, b] = [b, a_1, a] = a^{\rho p^r}.$$

Proof. Note that $[a_1, ab, a_1] = 1$ which implies that

$$1 = [a_1, ab, ab] = [a_1, a, b][a_1, b, a].$$

Put $w := [a_1, a, b] = [b, a_1, a]$. By the Jacobi identity $w^2 = [b, a, a_1]$. Further $[a, a_1 b, a] = a^{-3p^t}$ which implies

$$[a, a_1 b, a_1 b] = (a_1 b)^{-3p^t - 3\lambda p^l} = a_1^{-3p^t} b^{-3p^t} a_1^{-3\lambda p^l}$$

where $(\lambda, p) = 1$ and $a^{p^l} = 1$. Also

$$\begin{aligned}
[a, a_1 b, a_1 b] =& [a, a_1, b][a, b, a_1][a, b, b]\\
=& w^{-3} b^{-3p^t}.
\end{aligned}$$

https://doi.org/10.1017/S0017089502030094 Published online by Cambridge University Press

From this we get $w^3 = a_1^{3p^t+3\lambda p^l}$. If $a^{p^l} = 1$, put $r := t$ and we have the required result. Otherwise, put $3\rho p^r := 3p^t + 3\lambda p^l$ which gives $w = a_1^{\rho p^r}$. Then $[b, a, a] = a^{3\rho p^r}$ and $[b, a, b] = b^{3\rho p^r}$. □

LEMMA 7. *Let a be an element of maximal order in the subgroup H_k of G and let $b \in H_k$ such that $[b, a, a] = a^{3p^r}$, $[b, a, b] = b^{3p^r}$. If also $[a_1, a, b] = [b, a_1, a] = a^{p^r}$, then $[u, a, b] = [b, u, a] = u^{p^r}$ for $u \in \{b_1, a_2, b_2, \dots, a_{k-1}, b_{k-1}\}$.*

Proof. If $|u| = |a_1|$, then $[u, ab, u] = 1$ giving $1 = [u, ab, ab] = [u, a, b][u, b, a]$. If $|u| < |a_1|$, then $|ua_1| = |a_1|$ and

$$[ua_1, ab, ua_1] = [u, a, u][u, a, a_1][u, b, u][u, b, a_1][a_1, a, u][a_1, a, a_1][a_1, b, u][a_1, b, a_1].$$

If $u \neq b_1$ all these terms are trivial. If $u = b_1$, then

$$[u, a, a_1] = a^{p^{r_1}}, \quad [a_1, a, u] = a^{-p^{r_1}}, \quad [u, b, a_1] = b^{p^{r_1}}, \quad [a_1, b, u] = b^{-p^{r_1}},$$

and all other terms are trivial. In all cases $[ua_1, ab, ua_1] = 1$. So

$$\begin{aligned} 1 = [ua_1, ab, ab] &= [u, a, b][u, b, a]a_1^{p^r} a_1^{-p^r} \\ &= [u, a, b][u, b, a]. \end{aligned}$$

Put $w := [u, a, b] = [b, u, a]$ and $w^2 = [b, a, u]$. If $|a| = |a_1|$, then $[a, ub, a] = a^{-3p^r}$ implies

$$(ub)^{-3p^r} = [a, ub, ub] = w^{-3} b^{-3p^r}.$$

Thus $w = u^{p^r}$. If $|a| < |a_1|$, then $|aa_1| = |a_1|$ and

$$[aa_1, ub, aa_1] = \begin{cases} (aa_1)^{-3p^{r_1}-3p^r} & \text{if } u = b_1, \\ (aa_1)^{-3p^r} & \text{otherwise.} \end{cases}$$

So, if $u = b_1$,

$$(b_1 b)^{-3p^{r_1}-3p^r} = [aa_1, b_1 b, b_1 b] = b_1^{-3p^{r_1}} b^{-3p^{r_1}-3p^r} w^{-3},$$

giving $w = b_1^{p^r}$. If $u \neq b_1$ a similar calculation gives $w = u^{p^r}$, as required. □

LEMMA 8. *Let a be an element of maximal order in the subgroup H_k of G and let $b, x \in H_k$ such that $|[a_1, a, b]| \geq |[a_1, a, x]|$, $[a_1, a, b] = a_1^{p^r}$, and $[a, x, x] = [a, x, a] = 1$. Then there exists $x' = xb^m$ such that $[x', a, a_1] = [x', a_1, a] = 1$.*

Proof. The proof is similar to the previous proofs, and $[a_1, ax, a_1] = 1$ implies $1 = [a_1, ax, ax] = [a_1, x, a][a_1, a, x]$. Put $w := [a_1, a, x] = [x, a_1, a]$ and $w^2 = [x, a, a_1]$. Also $[a, a_1x, a] = 1$, but since a is not necessarily of maximal order in G we can only deduce that there exist integers λ and $l \geq 1$ such that $(\lambda, p) = 1$, $a^{p^l} = 1$ and $[a, a_1x, a_1x] = (a_1x)^{-3\lambda p^l} = a_1^{-3\lambda p^l}$. Upon expansion $[a, a_1x, a_1x] = [a, a_1, x][a, x, a_1] = w^{-3}$, giving $w = a_1^{\lambda p^l}$. If $a_1^{p^l} = 1$, then $w = 1$ and we put $x' = x$. Otherwise put $x' = xb^{-\lambda p^{l-r}}$. The condition on the orders of $[a_1, a, b]$ and $[a_1, a, x]$ ensures that $l \geq r$. Then $[a_1, a, x'] = [x', a_1, a] = 1$, giving the required result. □

https://doi.org/10.1017/S0017089502030094 Published online by Cambridge University Press

LEMMA 9. *Let a be an element of maximal order in the subgroup H_k of G and assume that $[z, a, b] = [b, z, a] = z^{p^r}$ for $z \in \{a_1, b_1, \ldots, a_{k-1}, b_{k-1}\}$. Let $x \in H_k$ such that $[x, a_1, a] = [x, a, a_1] = 1$. Then $[u, a, x] = [u, x, a] = 1$ for $u \in \{b_1, a_2, b_2, \ldots, a_{k-1}, b_{k-1}\}$.*

Proof. Again, the proof is similar to previous proofs. If $|u| = |a_1|$, then $[u, ax, u] = 1$ implies $1 = [u, ax, ax] = [u, a, x][u, x, a]$. If $|u| < |a_1|$, then $|a_1u| = |a_1|$, together with $[a_1u, ax, a_1u] = 1$, implies $1 = [a_1u, ax, ax] = [u, a, x][u, x, a]$. Set $w := [u, a, x] = [x, u, a]$ and $w^2 = [x, a, u]$. If $|a| = |a_1|$, then $[a, ux, a] = 1$ implies $1 = [a, ux, ux] = [a, u, x][a, x, u] = w^{-3}$, giving $w = 1$, as required. If $|a| < |a_1|$, then $|aa_1| = |a_1|$. In this case

$$[aa_1, ux, aa_1] = \begin{cases} (aa_1)^{-3p^r} & \text{if } u = b_1, \\ 1 & \text{otherwise.} \end{cases}$$

Hence

$$[aa_1, ux, ux] = \begin{cases} (ux)^{-3p^r} & \text{if } u = b_1, \\ 1 & \text{otherwise.} \end{cases}$$

In either case, upon expansion of the commutators, we get $w^3 = 1$, which implies $w = 1$, completing the proof. □

Proof of Theorem 5. The partial presentation $\mathcal{P}_1$ is given by Theorem 4. Assume that the group G has partial presentation $\mathcal{P}_{k-1}, 2 < k \leq 2n$. We prove the theorem by deriving the presentation $\mathcal{P}_k$. Let $H_k = \langle x_{2k-1}, \ldots, x_n \rangle$. Assume that H_k has class three. By Theorem 4 there exist generators $\{a, b, z_{2k+1}, \ldots, z_n\}$ for H_k with the following properties:

$$\begin{aligned} &[b, a, a] = a^{3p^t}, \quad [b, a, b] = b^{3p^t}, \\ &[z, a, b] = [b, z, a] = z^{p^t}, \\ &[z, a, a] = [z, a, z] = [z, b, b] = [z, b, z] = 1, \gamma_4(H_k) = 1, \end{aligned}$$

where $\langle a \rangle \cap \langle b \rangle = 1$, and $z \in \{z_{2k+1} \ldots, z_n\}$. Since

$$[x, a_i, b_i] = [b_i, x, a_i] = x^{p^{r_i}} \quad \text{and} \quad [x, a_i, a_i] = [x, a_i, x] = [x, b_i, b_i] = [x, b_i, x] = 1$$

for $i \in \{1, \ldots, k\}$ and $x \in D_k - \{a_i, b_i\}$, for each i these relations are also true for $x \in \langle D_k - \{a_i, b_i\} \rangle$. In particular,

$$[v, a_i, b_i] = [b_i, v, a_i] = v^{p^{r_i}} \quad \text{and} \quad [v, a_i, a_i] = [v, a_i, v] = [v, b_i, b_i] = [v, b_i, v] = 1$$

for $v \in \{a, b, z_{2k+1} \ldots, z_n\}$.

To prove the theorem we need to define r_k and then show that

$$[u, a, b] = [b, u, a] = u^{p^{r_k}}, \tag{10}$$

for $u \in \{a_1, b_1, \ldots, a_{k-1}, b_{k-1}\}$. Then we need to show that

$$[z, a, u] = [z, u, a] = [z, b, u] = [z, u, b] = 1 \tag{11}$$

for $z \in \{z_{2k+1} \dots, z_n\}$ (or an appropriate set of generators) and u as above. Lemma 6 provides an integer, call it r_k, such that

$$[b, a, a] = a^{3\rho p^{r_k}}, \quad [b, a, b] = b^{3\rho p^{r_k}} \quad \text{and} \quad [a_1, a, b] = [b, a_1, a] = a^{\rho p^{r_k}},$$

where $\rho p^{r_k} := p^t + \lambda p^l$, $(\lambda, p) = 1$ and $a^{p^l} = 1$. Since a has maximal order in H_k, we also have that $[z, a, b] = [b, z, a] = z^{\rho p^{r_k}}$ for $z \in \{z_{2k+1} \dots, z_n\}$. By choosing a suitable power of b we can assume that $\rho = 1$. Lemma 7 now completes the proof of (10).

Let $z \in \{z_{2k+1} \dots, z_n\}$. If $[a_1, a, z] = [a_1, z, a] = 1$, put $z' := z$. Otherwise, from the proof of Lemma 8, $[a_1, a, z] = a_1^{\lambda p^l}$, where $a^{p^l} = 1$. Since $[b, a, a] = a^{p^{r_k}} \neq 1$, this ensures that $l \geq r_k$ and $\|[a_1, a, b]\| \geq \|[a_1, a, z]\|$. In this case, replace z by $z' = zb^{\lambda p^l}$. Then $\{a, b, z'_{2k+1}, \dots, z'_n\}$ generates H_k, and $[z, a, a_1] = [z, a_1, a] = 1$ for $z \in \{z'_{2k+1}, \dots, z'_n\}$. It is also true that $[z, a_i, b_i] = [b_i, z, a_i] = z^{p^{r_i}}$, and $[z, a_i, a_i] = [z, a_i, z] = [z, b_i, b_i] = [z, b_i, z] = 1$, $1 \leq i \leq k-1$. Lemma 9 now completes the first part of (11), namely, that $[z, a, u] = [z, u, a] =$ for $z \in \{z'_{2k+1}, \dots, z'_n\}$ and $u \in \{a_1, b_1, \dots, a_{k-1}, b_{k-1}\}$.

To complete the proof of (11) we first consider $[z, a_1, b]$. If $|b| = |a|$ we can again use Lemma 8, with a small modification, to show that $[z', a_1, b] = [z', b, a_1] = 1$, where $z' = za^m$, for some integer m and $z \in \{z'_{2k+1}, \dots, z'_n\}$. If $|b| < |a|$, we use Lemma 8 also, for $a' = ab$ noting that $[a_1, a', a] = a_1^{-p^{r_k}}$. With a slight modification to the proof of Lemma 8, we again find $z' = za^m$ for some integer m such that for each z', $[z', a_1, a'] = [z', a', a_1] = 1$. Since $[z', a_1, a] = [z, a_1, a][a^m, a_1, a] = 1$ and $[z', a, a_1] = 1$, this is enough to show that $[z', a_1, b] = [z', b, a_1] = 1$. Again the relations already established for $z \in \{z'_{2k+1}, \dots, z'_n\}$ also hold for $z \in \{z''_{2k+1}, \dots, z''_n\}$, and $H_k = \langle a, b, z''_{2k+1}, \dots, z''_n \rangle$. Lemma 9 now completes the proof of (11).

We consider the situation when H_k has class two. In this case choose a so that a has maximal order in H_k, and choose b so that $b \in H_k \backslash \Phi(H_k)$ and $\|[a_1, a, b]\| \geq \|[a_1, a, x]\|$ for any $x \in H_k \backslash \Phi(H_k)$. If $[a_1, a, x] = 1$ for all $x \in H_k$, the choice of b is arbitrary. Choose $\{z_{2k+1} \dots, z_n\}$ so that $\{a, b, z_{2k+1} \dots, z_n\}$ is a generating set for H_k. With the convention that $[b, a, a] = a^{3p^t}$ for some integer $t \geq |a|$, the proof follows as for the case when H_k has class three.

If we now put $a_k := a$, $b_k := b$ and $u_i := z''_i$, $2k + 1 \leq i \leq n$, then the generators $\{a_1, b_1, \dots, a_k, b_k, u_{2k+1}, \dots, u_n\}$ for G satisfy the relations $\mathcal{P}_k$. □

Proof of Theorem A. If G has class less than three, the theorem is true. So assume that G has class three and is a group on m generators. If m is even put $n = m/2$. Then by Theorem 4 G has the partial presentation P_n. This is the required presentation, except that the integers r_i might not be ordered as stated in the Theorem. By changing the labelling of the generators we can ensure that $r_1 \leq r_2 \leq \dots \leq r_n$.

If m is odd, put $n = (m + 1)/2$. Then from Theorem 4 G has the partial presentation P_{n-1}, on generators $D_{n-1} = \{a_1, b_1, \dots, a_{n-1}, b_{n-1}, x_m\}$. Again, by changing the labelling of the generators, we can ensure that $r_1 \leq \dots \leq r_{n-1}$.Put $a_n = x_m$ and $r_n = \exp(G) + 1$. Then G is a homomorphic image of $G(r_1, \dots, r_n)$. □

REFERENCES

1. C. Cooper, Power automorphisms of a group, *Math. Z.* **107** (1968), 335–356.

2. P. Hall, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* (2) **36** (1933), 29–95.

3. S. K. Mahdavianary, A classification of 2-generator p-groups, $p \geq 3$, with many subgroups 2-subnormal, *Arch. Math. (Basel)* **43** (1987), 97–107.

4. E. A. Ormerod, Groups of Wielandt length two, *Math. Proc. Camb. Phil. Soc.* **110** (1991), 229–244.

5. G. Parmeggiani, On finite p-groups of odd order with many subgroups 2-subnormal, *Comm. Algebra* **24** (1996), 2707–2719.

6. M. Stadelmann, *Gruppen mit vielen Subnormalteilern vom Defekt zwei* (Dissertation, Würzburg, 1976).