ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE @ DIRECT®

Journal of Algebra 266 (2003) 539–551

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Groups of prime-power order with a small second derived quotient

Csaba Schneider

School of Mathematics and Statistics, The University of Western Australia,
35 Stirling Highway 6009 Crawley, Western Australia, Australia

Received 30 September 2001

Communicated by Alexander Lubotzky

Abstract

For odd primes we prove some structure theorems for finite p-groups G, such that $G'' \neq 1$ and $|G'/G''| = p^3$. Building on results of Blackburn and Hall, it is shown that $\gamma_3(G)$ is a maximal subgroup of G', the group G has a central decomposition into two simpler subgroups, and, moreover, G' has one of two isomorphism types.

Keywords: Finite p-groups; Derived subgroup; Second derived subgroup

1. Introduction

It is well known that in a finite p-group G the condition $G'' \neq 1$ implies that $|G'/G''| \geqslant p^3$; see, for example, Huppert [10, III.7.10]. In this article we prove a number of results about groups in which equality holds; that is, we assume that $G'' \neq 1$ and $|G'/G''| = p^3$. Such groups have already been investigated by, among others, N. Blackburn and P. Hall. Blackburn [3] proved that the condition $|G'/G''| = p^3$ implies that G'' is abelian generated by two elements and it is nearly homocyclic. In the same article he also published a result, which he attributed to Hall, that for odd primes the same condition implies that $|G''| \leqslant p$. Here we mostly consider p-groups for odd p, and our main results are concerned with such groups.

E-mail address: csaba@maths.uwa.edu.au.
URL address: http://www.maths.uwa.edu.au/~csaba.

0021-8693/03/$ – see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/S0021-8693(03)00294-1

Let G be a finite p-group and $\gamma_i(G)$ the ith term of the lower central series, so that $\gamma_1(G) = G$, $\gamma_2(G) = G'$, etc. If $G'' \neq 1$ then we have the following chain of normal subgroups:

$$G > G' = \gamma_2(G) > \gamma_3(G) > \gamma_4(G) \geqslant G'' > 1. \tag{1}$$

If, in addition, we assume that $|G'/G''| = p^3$, then it easily follows that the order of $G'/\gamma_3(G)$ is at most p^2. The result of this simple argument is improved by the following theorem.

Theorem 1.1. *Let $p \geqslant 3$ and G be a finite p-group, such that $|G'/G''| = p^3$ and $G'' \neq 1$. Then $|G'/\gamma_3(G)| = p$ and $G'' = \gamma_5(G)$.*

The proof of this result is given in Section 3. Our second theorem, whose proof is in Section 4, is that G can be written as a central product of two simpler subgroups.

Theorem 1.2. *Let $p \geqslant 3$ and G be a finite p-group, such that $|G'/G''| = p^3$ and $G'' \neq 1$. Then G can be factorised as $G = HU$, where*

(i) *H is a normal subgroup of G generated by at most* 5 *generators*;
(ii) *$\gamma_i(H) = \gamma_i(G)$ for all $i \geqslant 2$*;
(iii) *U is a normal subgroup of G, such that $U' \leqslant \gamma_5(G)$*;
(iv) *H and U centralise each other.*

An example is given after the proof of this theorem to show that the number “5” is, in general, best possible, and that there are, in some cases, other central decompositions of G in which the subgroups can have different isomorphism types.

Our proofs are based on commutator calculus. To simplify notation, we write long commutators according to the left-normed convention; for example $[a, b, c] = [[a, b], c]$. We use the well-known commutator identities that can be found in most group theory textbooks (see, for instance, Huppert [10, III.1.2–III.1.3]). In addition to these, we need the collection formula, which is proved as Lemma VIII.1.1 by Huppert and Blackburn [11]. We mainly use this result in the simplest case when it can be stated as

$$\bigl[x^p, y\bigr] \equiv [x, y]^p \bmod \bigl(N'\bigr)^p \gamma_p(N) \quad \text{where } N = \bigl\langle x, [x, y]\bigr\rangle.$$

The Hall–Witt identity will occur in a lesser known form which can be found in Magnus, Karrass and Solitar [13] on p. 290:

$$\bigl[x, y, z^x\bigr]\bigl[z, x, y^z\bigr]\bigl[y, z, x^y\bigr] = \bigl[x, y, z[z, x]\bigr]\bigl[z, x, y[y, z]\bigr]\bigl[y, z, x[x, y]\bigr] = 1.$$

We often manipulate generating sets of groups. In order to avoid cumbersome repetitions, we introduce a piece of notation. Let G be a group, g a symbol referring to a group element, and x an element in G. After the occurrence of the expression $x \rightsquigarrow g$, the name g will refer to the element x. For example, let G be the cyclic group of order two and let g denote its non-identity element. If we perform the replacement $g^2 \rightsquigarrow g$, then the symbol g will refer to the identity element of G.

One can naturally ask whether it is possible for a fixed prime to give a classification of groups which satisfy the conditions of the previous two theorems. It is conceivable that Blackburn's [2] description of groups of maximal class with order p^6 and degree of commutativity 0 is a good starting point. However, increasing the number of generators and allowing the abelian factor to have exponent higher than p led to complications which could not be resolved within the research presented here.

Our results can also be viewed in a wider context. It was first shown by Hall [8, Theorem 2.57] that the conditions $i \geqslant 1$ and $G^{(i+1)} \neq 1$ imply that $|G^{(i)}/G^{(i+1)}| \geqslant p^{2^i+1}$, and $|G| \geqslant p^{2^{i+1}+i+1}$ (see also Huppert [10, III.7.10 and III.7.11]). The lower bound for the order of G has recently been improved by Mann [12] and the author [15]. Both of these improvements are, however, minor, and the order of the smallest p-group G such that $G^{(i+1)} \neq 1$ is still unknown; the smallest known examples were constructed by Evans-Riley, Newman, and the author [5]. If $p \geqslant 3$ then we also do not know how sharp Hall's lower bound is for $|G^{(i)}/G^{(i+1)}|$. As the example of the Sylow 2-subgroup of the symmetric group with degree 2^{i+2} shows, this result is best possible for $p = 2$; it is not known otherwise. Our research was originally motivated by these questions, and it is hoped that a more detailed understanding of groups with a small second derived quotient will give us a hint of the solution to some of the above problems. Some partial results can be found in the author's PhD thesis [15].

Our results are inspired by Lie algebra calculations, and it is possible to prove some of them using the Lie ring method. In fact, Theorem 1.1 can be proved by first verifying the corresponding result for Lie algebras and then using the Lie ring associated with the lower central series. This approach would lead to some interesting new results for Lie algebras, which are beyond the scope of the present article.

The paper is structured as follows. In Section 2 we prove a lemma which is a generalisation of Blackburn's Theorem 1.3 [2]. A consequence of this result is that we can often restrict our interest to groups which are generated by two or three elements. In Sections 3 and 4 we prove Theorems 1.1 and 1.2, respectively. In Section 5 we characterise the commutator subgroup of G, and show that it has one of two isomorphism types.

2. A general lemma and some consequences

We have seen in the introduction that in a finite p-group G, the conditions $|G'/G''| = p^3$ and $G'' \neq 1$ imply that $G'/\gamma_3(G)$ has order at most p^2. The aim of this section is to show that G has a subgroup H with a small generating set, such that, apart from the first term, the lower central series of H coincides with the lower central series of G. This result generalises Blackburn's Theorem 1.3 [2] and Slattery's Lemma 2.1 [16].

Lemma 2.1. *Let G be a nilpotent group and H a subgroup of G, such that $G' = H'\gamma_3(G)$. Then $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$. Moreover, H is a normal subgroup of G.*

Proof. First we prove by induction on i that $\gamma_i(G) = \gamma_i(H)\gamma_{i+1}(G)$ for all $i \geqslant 2$. By the conditions of the lemma, this is true for $i = 2$. Suppose that our claim holds for some $i - 1 \geqslant 2$, and let us show that it holds for i as well. As it is obvious that $\gamma_i(H)\gamma_{i+1}(G) \leqslant \gamma_i(G)$, we only have to prove that $\gamma_i(G) \leqslant \gamma_i(H)\gamma_{i+1}(G)$. Using the induction hypothesis and III.1.10(a) of Huppert [10], we compute

$$\begin{aligned}\gamma_i(G) &= \big[\gamma_{i-1}(G), G\big] = \big[\gamma_{i-1}(H)\gamma_i(G), G\big] = \big[\gamma_{i-1}(H), G\big]\big[\gamma_i(G), G\big] \\ &= \big[\gamma_{i-1}(H), G\big]\gamma_{i+1}(G).\end{aligned}$$

Therefore it is enough to prove that $[\gamma_{i-1}(H), G] \leqslant \gamma_i(H)\gamma_{i+1}(G)$. First we note that $\gamma_i(G) \geqslant \gamma_i(H)\gamma_{i+1}(G) \geqslant \gamma_{i+1}(G)$, and hence $\gamma_i(H)\gamma_{i+1}(G)$ is a normal subgroup of G. Using the induction hypothesis we obtain

$$\begin{aligned}\big[G, \gamma_{i-2}(H), H\big] &\leqslant \big[\gamma_{i-1}(G), H\big] = \big[\gamma_{i-1}(H)\gamma_i(G), H\big] \\ &= \big[\gamma_{i-1}(H), H\big]\big[\gamma_i(G), H\big] \leqslant \gamma_i(H)\gamma_{i+1}(G)\end{aligned}$$

and

$$\begin{aligned}\big[H, G, \gamma_{i-2}(H)\big] &\leqslant \big[G', \gamma_{i-2}(H)\big] = \big[H'\gamma_3(G), \gamma_{i-2}(H)\big] \\ &= \big[H', \gamma_{i-2}(H)\big]\big[\gamma_3(G), \gamma_{i-2}(H)\big] \leqslant \gamma_i(H)\gamma_{i+1}(G).\end{aligned}$$

Using the Three Subgroups Lemma (see [10, III.1.10(b)]), we obtain

$$\big[\gamma_{i-1}(H), G\big] = \big[\gamma_{i-2}(H), H, G\big] \leqslant \gamma_i(H)\gamma_{i+1}(G),$$

and hence our statement is correct.

Let us prove that $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$. If the nilpotency class of G is c, that is $\gamma_{c+1}(G) = 1$, then $\gamma_{c+1}(G) = \gamma_{c+1}(H) = 1$. If $\gamma_{i+1}(G) = \gamma_{i+1}(H)$ for some i, such that $3 \leqslant i + 1 \leqslant c + 1$, then, by the result of the previous paragraph,

$$\gamma_i(G) = \gamma_i(H)\gamma_{i+1}(G) = \gamma_i(H)\gamma_{i+1}(H) = \gamma_i(H).$$

Using induction, we obtain $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$. The normality of H is an easy consequence of the fact that $G' = H' \leqslant H$. □

Corollary 2.2. *Let G be a finite p-group.*

(i) *If $G'/\gamma_3(G)$ is cyclic of order p, then G has a 2-generator normal subgroup H, such that $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$.*

(ii) *If $G'/\gamma_3(G)$ is elementary abelian of order p^2, then G has a 3-generator normal subgroup H, such that $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$.*

Proof. (i) Suppose that $G'/\gamma_3(G) = \langle [a,b]\gamma_3(G)\rangle$ for some $a, b \in G$, and set $H = \langle a, b\rangle$. As we have $H'\gamma_3(G) = G'$, Lemma 2.1 implies that H is a normal subgroup and $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$.

(ii) Suppose that $G'/\gamma_3(G)$ is elementary abelian of order p^2, and suppose that $G'/\gamma_3(G) = \langle [a,b]\gamma_3(G), [c,d]\gamma_3(G)\rangle$ for some $a, b, c, d \in G$. Select a subgroup H in G as follows. If $[a,c]$, $[a,d]$, $[b,c]$, $[b,d]$ are all in $\gamma_3(G)$ then let $H = \langle a, bc, d\rangle$. Otherwise suppose without loss of generality that $[a,c] \equiv [a,b]^\alpha [c,d]^\beta \bmod \gamma_3(G)$ for some α and β, such that $0 \leqslant \alpha, \beta \leqslant p-1$, and at least one of α and β is non-zero. If $\alpha \neq 0$, then set $H = \langle a, c, d\rangle$, otherwise set $H = \langle a, b, c\rangle$. It is easy to see that $H'\gamma_3(G) = G'$, and so, using Lemma 2.1, we obtain that H is a normal subgroup and $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$. □

3. Proof of Theorem 1.1

In this section we prove Theorem 1.1.

Suppose first that G is a finite p-group, such that $|G'/G''| = p^3$ and $G'' \neq 1$. If the quotient $G'/\gamma_3(G)$ is cyclic, then Lemma 2.1 of Blackburn [2] implies that

$$G'' = \bigl[G', G'\bigr] = \bigl[G', \gamma_3(G)\bigr] \leqslant \gamma_5(G), \tag{2}$$

and there is a chain

$$G > G' = \gamma_2(G) > \gamma_3(G) > \gamma_4(G) > \gamma_5(G) \geqslant G'' > 1 \tag{3}$$

of normal subgroups. In particular, if $|G'/\gamma_3(G)| = p$, then (2) and (3) imply that $G'' = \gamma_5(G)$; similarly if $|G'/\gamma_3(G)| = p^2$, then (2) implies that $G'/\gamma_3(G)$ must be elementary abelian.

Now assume that $|G'/\gamma_3(G)| = p^2$; we show that this can only happen when $p = 2$. By Corollary 2.2, there is a 3-generator subgroup H of G, such that $\gamma_i(G) = \gamma_i(H)$ for all $i \geqslant 2$. After replacing G by H, we may assume without loss of generality that $G = \langle a, b, c\rangle$ for some $a, b, c \in G$. Moreover, from (1) it follows that $G'' = \gamma_4(G)$, and hence we may suppose that G has nilpotency class 4. As $G'/\gamma_3(G)$ is elementary abelian of order p^2, we have that there are some α, β, and γ not all zero, such that $0 \leqslant \alpha, \beta, \gamma \leqslant p-1$ and

$$[a,b]^\alpha [a,c]^\beta [b,c]^\gamma \equiv 1 \bmod \gamma_3(G).$$

If $\alpha = \beta = 0$, then $[b,c]^\gamma \equiv 1 \bmod \gamma_3(G)$, that is $[b,c] \in \gamma_3(G)$. If $\alpha = 0$ and $\beta \neq 0$, then we obtain $[a^\beta b^\gamma, c] \equiv 1 \bmod \gamma_3(G)$. If we replace $a^\beta b^\gamma \rightsquigarrow a$, then we obtain that in the new generating set $[a,c] \in \gamma_3(G)$. Similarly, if $\alpha \neq 0$ and $\beta = 0$, then we replace $a^{-\alpha} c^\gamma \rightsquigarrow a$, and obtain that after the substitution $[a,b] \in \gamma_3(G)$. If $\alpha \neq 0$, and $\beta \neq 0$, then we replace $a^{\beta/\alpha} b^{\gamma/\alpha} \rightsquigarrow a$ and $bc^{\beta/\alpha} \rightsquigarrow b$. Then it is easy to see that in the new generating set $[a,b] \in \gamma_3(G)$. After possibly reordering the generators, we may suppose without loss of generality that G is generated by three elements a, b, and c, such that

$G'/\gamma_3(G) = \langle [a,b]\gamma_3(G), [a,c]\gamma_3(G)\rangle$, and moreover $[b,c] \in \gamma_3(G)$. Note that in this case $[a,b,c] \equiv [a,c,b] \bmod \gamma_4(G)$ also holds. Then $G'' \neq 1$ and $\gamma_5(G) = 1$ imply that

$$\big[[a,b],[a,c]\big] = [a,b,a,c][a,b,c,a]^{-1} \neq 1$$

and

$$\big[[a,c],[a,b]\big] = [a,c,a,b][a,c,b,a]^{-1} \neq 1.$$

If $[a,b,a] \in \gamma_4(G)$, then $[a,b,a,c] \in \gamma_5(G)$, and hence $[a,b,a,c] = 1$. Similarly $[a,b,c] \in \gamma_4(G)$, implies that $[a,b,c,a] = 1$; therefore at least one of the elements $[a,b,a]$ and $[a,b,c]$ does not lie in $\gamma_4(G)$. Similarly, at least one of $[a,c,a]$ and $[a,b,c]$ must also lie outside $\gamma_4(G)$.

First we assume that $[a,b,c] \in \gamma_4(G)$. In this case we must have $[a,c,a] \notin \gamma_4(G)$ and $[a,b,a] \notin \gamma_4(G)$. As $\gamma_3(G)/\gamma_4(G)$ is cyclic of order p, there is some α, such that $0 \leqslant \alpha \leqslant p-1$ and $[a,bc^{\alpha},a] \equiv 1 \bmod \gamma_4(G)$, and we carry out the replacement $bc^{\alpha} \rightsquigarrow b$. In the new generating set $[b,c] \in \gamma_3(G)$ still holds, and, in addition, we obtain $[a,b,a] \in \gamma_4(G)$.

So without loss of generality we may assume that $[a,b,a] \in \gamma_4(G)$ and $[a,b,c] \notin \gamma_4(G)$. In this case $[a,b,c,a] = [a,c,b,a] \neq 1$, in other words $a \notin \mathsf{C}_G(\gamma_3(G))$. On the other hand, $[a,b,b,a] = [a,b,a,b]$, and hence $[a,b,b,a] = 1$. If $[a,b,b] \notin \gamma_4(G)$, then $\gamma_3(G) = \langle [a,b,b], \gamma_4(G)\rangle$, and so $a \in \mathsf{C}_G(\gamma_3(G))$, which is impossible; therefore $[a,b,b] \in \gamma_4(G)$. If $[a,c,a] \notin \gamma_4(G)$ then there is some $\alpha \neq 0$, such that $[a,c,ab^{\alpha}] \in \gamma_4(G)$; in this case we let $ab^{\alpha} \rightsquigarrow a$ and obtain $[a,c,a] \in \gamma_4(G)$. In the new generating set $[b,c] \in \gamma_3(G)$ and $[a,b,a], [a,b,b] \in \gamma_4(G)$ still hold. Then

$$\begin{aligned} 1 &= \big[[a,b],a,c\big]\big[[a,c],[a,b]\big]\big[c,[a,b],a\big] \\ &= [a,b,a,c][a,c,a,b][a,b,c,a]^{-1}[a,b,c,a]^{-1} = [a,b,c,a]^{-2}, \end{aligned}$$

that is, $[a,b,c,a]^2 = 1$, and hence $p = 2$. This completes the proof of Theorem 1.1.

4. Proof of Theorem 1.2

In the previous section we proved Theorem 1.1, and hence we know that in a group G the conditions of Theorem 1.2 imply that $|G'/\gamma_3(G)| = p$. Thus, according to Corollary 2.2, G has a 2-generator subgroup H, such that for all $i \geqslant 2$ we have $\gamma_i(G) = \gamma_i(H)$. We use this subgroup to obtain the desired factorisation. First we show that we can choose a generating set which satisfies some extra conditions.

Lemma 4.1. *Let G be a 2-generator, finite p-group, such that $|G'/G''| = p^3$, $|G'/\gamma_3(G)| = p$, and $G'' \neq 1$. Then generators a and b of G can be chosen, such that the following hold*:

(i) $\gamma_2(G)/\gamma_3(G) = \langle [b,a]\gamma_3(G)\rangle$;
(ii) $\gamma_3(G)/\gamma_4(G) = \langle [b,a,a]\gamma_4(G)\rangle$ *and* $[b,a,b] \in \gamma_4(G)$;

(iii) $\gamma_4(G)/\gamma_5(G) = \langle [b,a,a,a]\gamma_5(G)\rangle$ *and* $[b,a,a,b] \in \gamma_5(G)$;
(iv) $\gamma_5(G)/\gamma_6(G) = \langle [b,a,a,a,b]\gamma_6(G)\rangle$ *and* $[b,a,a,a,a] \in \gamma_6(G)$.

Proof. We may suppose without loss of generality that G has class 5. As noticed in the introduction, our conditions imply that the factors $G'/\gamma_3(G)$, $\gamma_3(G)/\gamma_4(G)$, and $\gamma_4(G)/\gamma_5(G)$ are cyclic with order p. Using the argument presented by Blackburn [2] in Lemma 2.9, we can choose the generating set $\{a,b\}$, so that properties (i)–(iii) hold. It follows from (2) and (3) that $G'' = \gamma_5(G)$, and $G'' = \langle [[b,a,a],[b,a]]\rangle$. As the element $[[b,a,a],[b,a]]$ is central and has order p, we have $|\gamma_5(G)| = p$, and using Blackburn's argument on p. 89, the set $\{a,b\}$ can be chosen so that the additional property (iv) also holds. □

Lemma 4.2. *Let* $p \geqslant 3$ *and* G *be a finite* p*-group, such that* $|G'/G''| = p^3$ *and* $G'' \neq 1$. *Then* G *has a minimal generating set* $\{a,b,u_1,u_2,\dots,u_r\}$*, such that*

(i) $H = \langle a,b\rangle$ *is a normal subgroup of* G*, such that* $\gamma_i(H) = \gamma_i(G)$ *for all* $i \geqslant 2$; *further,* a *and* b *are as in Lemma* 4.1;
(ii) $[a,u_i] \in \gamma_5(G)$ *for all* u_i;
(iii) $[b,u_i] \in \gamma_4(G)$ *for all* u_i;
(iv) $[u_i,u_j] \in \gamma_5(G)$ *for all* u_i *and* u_j.

In particular, $u_1,\dots,u_r \in \mathrm{C}_G(G')$.

Proof. First recall Hall's theorem that $|G''| = p$, and so (3) implies that G has class 5. Select $a,b \in G$, such that the subgroup $H = \langle a,b\rangle$ and its generators are as in Lemma 4.1. It is easy to see that a,b are linearly independent modulo the Frattini subgroup of G. Therefore they can be viewed as elements of a minimal generating set $\{a,b,u_1,\dots,u_r\}$. Now suppose that for each $i \in \{1,\dots,r\}$, $[u_i,a] \equiv [b,a]^{\alpha_i}$ and $[u_i,b] \equiv [b,a]^{\beta_i}$ modulo $\gamma_3(G)$ with some $\alpha_i,\beta_i \in \{0,\dots,p-1\}$. Then $[u_ib^{-\alpha_i}a^{\beta_i},b] \in \gamma_3(G)$ and also $[u_ib^{-\alpha_i}a^{\beta_i},a] \in \gamma_3(G)$. If we perform the replacement $u_ib^{-\alpha_i}a^{\beta_i} \rightsquigarrow u_i$, then it is easy to see that $\{a,b,u_1,\dots,u_r\}$ is also a minimal generating set for G and

$$[a,u_i],[b,u_i] \in \gamma_3(G) \quad \text{for all } i \in \{1,\dots,r\}.$$

Now suppose that for all $i \in \{1,\dots,r\}$ we have

$$[u_i,a] \equiv [b,a,a]^{\alpha_i}[b,a,a,a]^{\beta_i} \bmod \gamma_5(G)$$

for some $\alpha_i,\beta_i \in \{0,\dots,p-1\}$. Then computing modulo $\gamma_5(G)$ we obtain

$$\begin{aligned}
&\bigl[u_i[b,a]^{-\alpha_i}[b,a,a]^{-\beta_i},a\bigr]\\
&\quad= \bigl[u_i[b,a]^{-\alpha_i},a\bigr]\bigl[u_i[b,a]^{-\alpha_i},a,[b,a,a]^{-\beta_i}\bigr]\bigl[[b,a,a]^{-\beta_i},a\bigr]\\
&\quad\equiv [u_i,a]\bigl[u_i,a,[b,a]^{-\alpha_i}\bigr]\bigl[[b,a]^{-\alpha_i},a\bigr]\bigl[[b,a,a]^{-\beta_i},a\bigr]\\
&\quad\equiv [u_i,a][b,a,a]^{-\alpha_i}[b,a,a,a]^{-\beta_i} \equiv 1.
\end{aligned}$$

If we replace $u_i[b,a]^{-\alpha_i}[b,a,a]^{-\beta_i} \rightsquigarrow u_i$, then $[u_i,a] \in \gamma_5(G)$. Since the images of the u_i over the Frattini subgroup did not change, the set $\{a,b,u_1,\dots,u_r\}$ is still a minimal generating system for G. We show that this generating set satisfies the properties required by the lemma.

We claim that $[u_i,b] \in \gamma_4(G)$ for all $i \in \{1,\dots,r\}$. To prove this we observe that

$$1 = \bigl[b,a,u_i[u_i,b]\bigr]\bigl[u_i,b,a[a,u_i]\bigr]\bigl[a,u_i,b[b,a]\bigr] = \bigl[b,a,[u_i,b]\bigr][b,a,u_i][u_i,b,a],$$

and thus

$$\begin{aligned}[b,a,u_i] &= [u_i,b,a]^{-1}\bigl[b,a,[u_i,b]\bigr]^{-1} = \bigl[[b,u_i]^{-1},a\bigr]^{-1}\bigl[[u_i,b],[b,a]\bigr] \\ &= [b,u_i,a]\bigl[[u_i,b],[b,a]\bigr]. \end{aligned} \tag{4}$$

In particular, $[b,a,u_i] \in \gamma_4(G)$. Now consider

$$1 = \bigl[[b,a],a,u_i\bigl[u_i,[b,a]\bigr]\bigr]\bigl[u_i,[b,a],a[a,u_i]\bigr]\bigl[a,u_i,[b,a][b,a,a]\bigr] = [b,a,a,u_i].$$

We can obtain similarly $[b,a,a,a,u_i] = 1$. As $[u_i,b] \in \gamma_3(G)$, $[u_i,b] \equiv [b,a,a]^{\varepsilon_i}$ modulo $\gamma_4(G)$ for some $\varepsilon_i \in \{0,\dots,p-1\}$. The Hall–Witt identity implies that

$$\begin{aligned} 1 &= \bigl[[b,a],u_i,b\bigl[b,[b,a]\bigr]\bigr]\bigl[b,[b,a],u_i[u_i,b]\bigr]\bigl[u_i,b,[b,a][b,a,u_i]\bigr] \\ &= \bigl[[b,a],u_i,b\bigr]\bigl[[u_i,b],[b,a]\bigr]. \end{aligned}$$

Using (4) we get $[b,a,u_i,b] = [b,a,a,a,b]^{-\varepsilon_i}$. Moreover,

$$\bigl[[u_i,b],[b,a]\bigr] = \bigl[[b,a,a]^{\varepsilon_i},[b,a]\bigr] = [b,a,a,a,b]^{-\varepsilon_i},$$

and thus $[b,a,a,a,b]^{-2\varepsilon_i} = 1$, from which it follows that $\varepsilon_i = 0$, that is $[u_i,b] \in \gamma_4(G)$.

We now prove that $u_1,\dots,u_r \in \mathrm{C}_G(G')$. We have already seen that $[b,a,a]$, $[b,a,a,a]$ are centralised by the u_i, so it suffices to prove that $[b,a,u_i] = 1$ for all $i \in \{1,\dots,r\}$. This is clear because

$$1 = \bigl[b,a,u_i[u_i,b]\bigr]\bigl[u_i,b,a[a,u_i]\bigr]\bigl[a,u_i,b[b,a]\bigr] = [b,a,u_i].$$

It remains to show that $[u_i,u_j]$ lies in $\gamma_5(G)$ for all $i,j \in \{1,\dots,r\}$. It easily follows using the Hall–Witt identity that $[u_i,u_j,a] = 1$ and $[u_i,u_j,b] = 1$, therefore $[u_i,u_j] \in Z(H) \cap H' = \gamma_5(H) = \gamma_5(G)$. The proof is complete. □

Proof of Theorem 1.2. Choose a generating set $\{a,b,u_1,u_2,\dots,u_r\}$ for G as in the previous lemma. In the first stage of the proof we show that this generating set can be modified so that, in addition to the properties required by Lemma 4.2, one of the following holds:

(a) $u_1,\dots,u_r \in \mathrm{C}_G(a)$; or

(b) $u_2,\dots,u_r \in \mathsf{C}_G(\langle a,u_1\rangle)$.

If $u_1,\dots,u_r \in \mathsf{C}_G(a)$ then (a) holds and we are done. Suppose that there is at least one u_i which does not centralise a. Without loss of generality we may assume that $[u_1,a]=[b,a,a,a,b]$. If $[u_i,a]=[b,a,a,a,b]^{\alpha_i}$ for some $i\in\{2,\dots,r\}$, then let $u_iu_1^{-\alpha_i} \rightsquigarrow u_i$. In this way we obtain a generating set $\{a,b,u_1,\dots,u_r\}$, such that $[u_1,a]=[b,a,a,a,b]$ and $\langle u_2,\dots,u_r\rangle \leqslant \mathsf{C}_G(a)$.

If $u_2,\dots,u_r$ centralise u_1, then (b) holds and we are done. We assume without loss of generality that $[u_2,u_1]=[b,a,a,a,b]$. If $[u_i,u_1]=[b,a,a,a,b]^{\beta_i}$ for some $i\in\{3,\dots,r\}$, then let $u_iu_2^{-\beta_i} \rightsquigarrow u_i$. In this way we obtain a generating set, such that $u_2,\dots,u_r$ centralise a, and $u_3,\dots,u_r$ centralise u_1. Repeating this process, we construct a generating set $\{a,b,u_1,\dots,u_k,\dots,u_r\}$, such that

1. $[u_1,a]=[b,a,a,a,b]$;
2. $u_2,\dots,u_r$ centralise a;
3. $[u_{i+1},u_i]=[b,a,a,a,b]$ for all $i\in\{1,\dots,k-1\}$;
4. $[u_{k+1},u_k]=1$;
5. $u_{i+2},\dots,u_r$ centralise u_i for all $i\in\{1,\dots,k\}$.

Now if k is even then substitute $au_2u_4\cdots u_k \rightsquigarrow a$. After this change property (a) holds. If k is odd then replace $u_1u_3\cdots u_k \rightsquigarrow u_1$; in this case property (b) holds.

We continue with the second stage of the proof. Suppose that the generating set $\{a,b,u_1,\dots,u_r\}$ is as in Lemma 4.2 and, in addition, property (a) holds. First assume that all the u_i centralise b modulo $\gamma_5(G)$. If $[u_i,b]=[b,a,a,a,b]^{\gamma_i}$ for some $i\in\{1,\dots,r\}$ and $\gamma_i\in\{0,\dots,p-1\}$, then let $u_i[b,a,a,a]^{-\gamma_i} \rightsquigarrow u_i$. Then $H=\langle a,b\rangle$ and $U=\langle u_1,\dots,u_r\rangle$ satisfy the assertions of the theorem.

Suppose that some of the u_i do not centralise b modulo $\gamma_5(G)$, and assume without loss of generality that $[u_1,b]=[b,a,a,a][b,a,a,a,b]^{\gamma_1}$. Perform $u_1[b,a,a,a]^{-\gamma_1} \rightsquigarrow u_1$ to obtain $[u_1,b]=[b,a,a,a]$. If $[u_i,b]\equiv[b,a,a,a]^{\gamma_i} \bmod \gamma_5(G)$ with some $i\in\{2,\dots,r\}$, then substitute $u_iu_1^{-\gamma_i} \rightsquigarrow u_i$. After this there is some δ_i, such that $0\leqslant\delta_i\leqslant p-1$ and $[u_i,b]=[b,a,a,a,b]^{\delta_i}$; then replace $u_i[b,a,a,a]^{-\delta_i} \rightsquigarrow u_i$. This way we obtain $[u_1,b]=[b,a,a,a]$ and, moreover, $\langle u_2,\dots,u_r\rangle \leqslant \mathsf{C}_G(b)$. If $u_2,\dots,u_r$ centralise u_1, then choose $H=\langle a,b,u_1\rangle$ and $U=\langle u_2,u_3,\dots,u_r\rangle$ and we are done. Suppose that this is not the case and $[u_2,u_1]=[b,a,a,a,b]$. Then, as in the first part of the proof, select a generating set $\{a,b,u_1,\dots,u_k,\dots,u_r\}$, such that the following additional properties hold:

1. $[u_1,b]=[b,a,a,a]$;
2. $u_2,\dots,u_r$ centralise b;
3. $[u_{i+1},u_i]=[b,a,a,a,b]$ for all $i\in\{1,\dots,k-1\}$;
4. $[u_{k+1},u_k]=1$;
5. $u_{i+2},\dots,u_r$ centralise u_i for all $i\in\{1,\dots,k\}$.

If k is even then set

$$H=\langle a,b,u_1u_3\cdots u_{k-1},u_2u_4\cdots u_k\rangle$$

and

$$U = \langle u_2, u_3, \ldots, u_{k-1}, u_{k+1}, \ldots, u_r \rangle.$$

If k is odd then let $H = \langle a, b, u_1 u_3 \cdots u_k \rangle$ and $U = \langle u_2, u_3, \ldots, u_r \rangle$. In both cases the subgroups H and U are as required.

In the case of property (b), we consider the group $G_1 = \langle a, b, u_2, \ldots, u_r \rangle$ and choose subgroups H_1 and U_1 according to the process described in the previous paragraph. Then note that H_1 and U_1 satisfies the prescribed conditions. Moreover H_1 can be generated by at most four elements. For G we can choose the subgroups $H = \langle H_1, u_1 \rangle$ and $U = U_1$. □

The following example shows that the number "5" in Theorem 1.2 is the best possible. This construction can be generalised, and it is not difficult to see that similar examples exist for all p.

Example 4.3. Consider the pro-5-group G given by the pro-5-presentation

$$\begin{aligned}\bigl\{a, b, u_1, u_2, u_3 \mid{}& a^5, b^5, u_1^5, u_2^5, u_3^5, [b,a,b], [b,a,a,a,a], [b,a,a,a,b][a,u_1], [a,u_2],\\ & [a,u_3], [b,u_1], [b,a,a,a][b,u_2], [b,u_3], [u_1,u_2], [u_1,u_3],\\ & [b,a,a,a,b][u_2,u_3]\bigr\}.\end{aligned}$$

Then, using the ANU p-Quotient Program [9,14], it is easy to see that G is a finite 5-group and $\gamma_5(G) = G'' \neq 1$. Suppose that $G = HU$ is a factorisation of G as in the theorem. Then U centralises H, and in particular, $U \leqslant \mathsf{C}_G(G')$. Using a computer algebra system, such as GAP [6] or MAGMA [1], it is easy to compute that $\mathsf{C}_G(G') = \langle u_1, u_2, u_3, [b,a,a,a] \rangle$, and that no subgroup of G generated by less than 5 generators can be taken for H in Theorem 1.2.

In Theorem 1.2 the subgroup U satisfies $|U'| \leqslant p$. The non-abelian p-groups with this property were classified by S.R. Blackburn [4]. Unfortunately, the isomorphism types of H and U are not uniquely determined by the isomorphism type of G. The following example illustrates this fact.

Example 4.4. Let $p \geqslant 5$ and let G denote the pro-p-group given by the pro-p-presentation

$$\begin{aligned}\bigl\{a, b, u_1, u_2, u_3 \mid{}& a^p, b^p, u_1^{p^3}, u_2^{p^2}, u_3^{p^2}, [b,a,b], [b,a,a,a,a], [b,a,a,a,b][a,u_1],\\ & [a,u_2], [b,u_1], [b,u_2], [u_1,u_2], [u_3,a], [u_3,b], [u_3,u_1],\\ & [b,a,a,a,b][u_3,u_2]\bigr\}.\end{aligned}$$

Then G has the obvious factorisation $G = H_1 U_1$, where $H_1 = \langle a, b, u_1 \rangle$ and $U_1 = \langle u_2, u_3 \rangle$. The group G also admits a factorisation $G = H_2 U_2$, where $H_2 = \langle a u_3, b, u_1 \rangle$ and $U_2 = \langle u_1 u_2^{-1}, u_3 \rangle$. It is easy to see that $H_1 \ncong H_2$ and $U_1 \ncong U_2$.

5. A characterisation of the derived subgroup

The following lemma was already known to Burnside. Its proof is an easy exercise, and can also be found in Huppert [10, III.7.8].

Lemma 5.1. *In a finite p-group G, if $Z(G')$ is cyclic then so is G'.*

Suppose that G is a p-group for some odd p, such that $|G'/G''| = p^3$ and $G'' \neq 1$. As $|G''| = p$, the subgroup G' has order p^4 and its derived subgroup G'' is cyclic with order p. By the previous lemma $Z(G')$ cannot be cyclic. The following result gives more information on the structure of G'.

Lemma 5.2. *The quotient G'/G'' is elementary abelian.*

Proof. Recall that Hall's theorem implies that $\gamma_6(G) = 1$. Using Corollary 2.2, assume that G is generated by two elements a and b which are chosen as in Lemma 4.1. Then G'/G'' is generated by the images of $[b,a]$, $[b,a,a]$ and $[b,a,a,a]$. Since the centre of G' is $\langle [b,a,a,a], G''\rangle$, we must have $[b,a,a,a]^p = 1$ by Lemma 5.1.

Suppose that $[b,a]^p \not\equiv 1 \bmod \gamma_4(G)$. Then $[b,a]^p\gamma_4(G)$ generates the quotient $\gamma_3(G)/\gamma_4(G)$ and in particular $[[b,a]^p, [b,a]] \neq 1$, which is clearly impossible. Suppose now that $[b,a]^p \not\equiv 1 \bmod \gamma_5(G)$. Then

$$\bigl[[b,a]^p, b\bigr] \equiv [b,a,b]^p = 1 \bmod \bigl(N'\bigr)^p \gamma_p(N),$$

where $N = \langle [b,a], [b,a,b]\rangle$. This yields $[[b,a]^p, b] = 1$, which is a contradiction. Now suppose that $[b,a,a]^p \not\equiv 1 \bmod \gamma_5(G)$. Then

$$\bigl[[b,a,a]^p, b\bigr] \equiv [b,a,a,b]^p = 1 \bmod \bigl(N'\bigr)^p \gamma_p(N),$$

where $N = \langle [b,a,a], [b,a,a,b]\rangle$. Again, this leads to a contradiction. □

Our last main result is a characterisation of G'. For odd primes let X_{p^3} and Y_{p^3} denote the non-abelian p-groups of order p^3 and exponent p and p^2, respectively. The symbol C_p denotes the cyclic group of order p.

Theorem 5.3. *If $p \geqslant 3$ and G is a finite p-group, such that $|G'/G''| = p^3$ and $G'' \neq 1$, then G' is isomorphic to $X_{p^3} \times C_p$ or to $Y_{p^3} \times C_p$.*

Proof. Recall that by Hall's theorem $|G'| = p^4$. For $p \geqslant 5$ the list of groups with order p^4 can be found in Huppert [10, III.12.6]. For $p = 3$ one can find this list as part of GAP [6] or MAGMA [1]. It is easy to see that the only groups which satisfy the conditions on G' are $X_{p^3} \times C_p$ and $Y_{p^3} \times C_p$. □

Example 5.4. Let G be a group of maximal class of order p^6 for $p \geqslant 5$ with degree of commutativity 0. Then $|G'/G''| = p^3$ and by Theorem 3.2 of Blackburn [2] $G' \cong$

$X_{p^3} \times C_p$. An example for such a group is the pro-p-group described by the pro-p-presentation

$$G = \{a, b \mid a^p,\ b^p,\ [b, a, b],\ [b, a, a, a, a]\}.$$

If $p = 3$ then the pro-3-group described by the pro-3-presentation

$$\{a, b \mid a^9,\ b^9,\ [a, b]^3,\ [b, a, b],\ [b, a, a, a, a]\}$$

contains $X_{27} \times C_3$ as derived subgroup. This can easily be checked using the p-Quotient Program [9,14].

Example 5.5. If $p \geqslant 3$ and G denotes the pro-p-group given by the pro-p-presentation

$$\{a, b \mid a^{p^2},\ b^{p^2},\ [b, a]^p = [b, a, a, a, b],\ [b, a, b],\ [b, a, a, a, a]\},$$

then $G' \cong Y_{p^3} \times C_p$.

Corollary 5.6. *If $p \geqslant 5$ and G is a finite p-group, such that $G' \cong X_{p^3} \times C_p$, then $G^p \leqslant Z(G)$. If $p \geqslant 3$ and G is a finite p-group, such that $G' \cong Y_{p^3} \times C_p$, then $G^{p^2} \leqslant Z(G)$.*

Proof. We only prove the first statement; the proof of the second is very similar. It is enough to prove that $u^p \in Z(G)$ for all $u \in G$. So let $u \in G$ and notice that $[v, u] \in G'$ for all $v \in G$. By the collection formula

$$[v, u^p] \equiv [v, u]^p = 1 \bmod (N')^p \gamma_p(N) \quad \text{where } N = \langle u, [u, v] \rangle.$$

If $p \geqslant 5$ then $(N')^p \gamma_p(N) = 1$ therefore $[v, u^p] = 1$. □

Acknowledgment

Much of the research presented in this paper was carried out while I was a PhD student at The Australian National University in Canberra. I am grateful to my supervisor, Mike Newman, for his many suggestions; and to Cheryl Praeger and Eamonn O'Brien for their helpful comments on a draft.

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997) 235–265, doi:10.1006/jsco.1996.0125.
[2] N. Blackburn, On a special class of p-groups, Acta Math. 100 (1958) 45–92.
[3] N. Blackburn, The derived group of a 2-group, Math. Proc. Cambridge Philos. Soc. 101 (1987) 193–196.
[4] S.R. Blackburn, Groups of prime power order with derived subgroup of prime order, J. Algebra 219 (1999) 625–657, doi:10.1006/jabr.1998.7909.

[5] S. Evans-Riley, M.F. Newman, C. Schneider, On the soluble length of groups with prime-power order, Bull. Austral. Math. Soc. 59 (1999) 343–346.

[6] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.2, Aachen, St. Andrews, 2000, http://www.gap-system.org.

[7] K.W. Gruenberg, J.E. Roseblade (Eds.), The Collected Works of Philip Hall, Clarendon Press, Oxford, 1988.

[8] P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. (2) 36 (1934) 29–95, or collected works [7].

[9] G. Havas, M.F. Newman, E.A. O'Brien, ANU p-quotient program, Version 1.4, Available from ftpmaths.anu.edu.au/pub/algebra/PQ, or as part of GAP [6] and MAGMA [1], 1996.

[10] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.

[11] B. Huppert, N. Blackburn, Finite Groups II, Springer-Verlag, Berlin, 1982.

[12] A. Mann, The derived length of p-groups, J. Algebra 224 (2000) 263–267, doi:10.1006/jabr.1998.8045.

[13] W. Magnus, A. Karrass, D. Solitar, Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations, Interscience Publishers, New York, 1966.

[14] M.F. Newman, E.A. O'Brien, Application of computers to questions like those of Burnside II, Internat. J. Algebra Comput. 6 (1996) 593–605.

[15] C. Schneider, Some results on the derived series of finite p-groups, PhD thesis, The Australian National University, Canberra, 2000.

[16] M.C. Slattery, Character degrees and nilpotence class in p-groups, J. Austral. Math. Soc. (Ser. A) 57 (1994) 76–80.