Pacific Journal of Mathematics

THE POWER-COMMUTATOR STRUCTURE OF FINITE p-GROUPS

DEANE EUGENE ARGANBRIGHT

Vol. 29, No. 1 May 1969

PACIFIC JOURNAL OF MATHEMATICS
Vol. 29, No. 1, 1969

THE POWER-COMMUTATOR STRUCTURE OF FINITE p-GROUPS

DEANE E. ARGANBRIGHT

For a finite p-group G, G_n is the n-th element in the descending central series of G; $P(G)$ is the subgroup of G generated by the set of all x^p for x belonging to G; and $\Phi(G)$ is the Frattini subgroup of G.

Hobby has characterized finite p-groups G (for $p > 2$) in which $P(G) = \Phi(G)$. Since $\Phi(G) = G_2P(G)$, the condition $P(G) = \Phi(G)$ is clearly equivalent to $G_2 \subseteqq P(G)$. In this paper we examine the class of finite p-groups G which have the property that $G_n \subseteqq P(G_m)$ for $1 < n/m < p$. In § 2 we consider consequences of this property in the case $m = 1$. For example, if $G_{p-1} \subseteqq P(G)$, then the product of p-th powers of elements of G is the p-th power of an element of G (Theorem 2). In § 3 we examine some connections between the property $G_n \subseteqq P(G_m)$ and regularity, and obtain a characterization of regular 3-groups (Theorem 4). In § 4 we obtain bounds on the number of generators of various commutator subgroups of G in the case $G_3 \subseteqq P(G)$, $p > 3$.

For a discussion of p-groups G for which $G_2 \subseteqq P(G)$ see [6].

1. Notation. Throughout this paper G is a finite p-group. If $X_1, X_2, \cdots, X_n$ are subsets of G, then $\langle X_1, X_2, \cdots, X_n\rangle$ is the smallest subgroup of G containing all the X_i. If $X = \{x\}$ for some element x, we write $X = x$. We denote by $d(G)$ the minimal number of elements of G which generate G, while $|G|$ is the order of G. We set $P^n(G) = \langle\{x^{p^n} \mid x \in G\}\rangle$. Also, $Z(G)$ is the center of G and $\Phi(G)$ is the Frattini subgroup of G.

Simple commutators of weight n are defined inductively by setting $(x_1, x_2) = x_1^{-1}x_2^{-1}x_1x_2$ and $(x_1, \cdots, x_n) = ((x_1, \cdots, x_{n-1}), x_n)$ for $n > 2$. In addition, we define $(x, 1y) = (x, y)$ and $(x, ny) = (x, (n-1)y, y)$ for $n > 1$. For subgroups $H_1, H_2, \cdots, H_n$ of G we set

$$(H_1, H_2, \cdots, H_n) = \langle\{(h_1, h_2, \cdots, h_n) \mid h_i \in H_i\}\rangle .$$

Similarly, $(H_1, 1H_2) = (H_1, H_2)$ and $(H_1, nH_2) = (H_1, (n-1)H_2, H_2)$ for $n > 1$. The descending central series of G is defined by setting $G_1 = G$ and $G_n = (G_{n-1}, G)$ for $n > 1$. A group G is said to have *class* c if $G_{c+1} = 1$ and $G_c \neq 1$. Finally, the derived series of G is defined by setting $G^{(0)} = G$ and $G^{(i+1)} = (G^{(i)}, G^{(i)})$ for $i \geqq 0$.

2. Basic results. It is known ([4], Th. 3.1, p. 63) that whenever x and y belong to G,

$$(*) \qquad (xy)^p = x^p y^p c d$$

where $c \in P(\langle x, y\rangle_2)$ and $d \in \langle x, y\rangle_p$. Applying this result to the expression $(a^p, b) = a^{-p}(a(a, b))^p$ one can obtain the following lemma by repeated induction.

LEMMA 1. *If $s, n, k \geqq 1$, then $(P(G_n), sG_k) \subseteqq P(G_{n+sk})G_{pn+sk}$.*

THEOREM 1. *Let n and m be integers and p be a prime such that $1 < n/m < p$. If $G_n \subseteqq P(G_m)$, then $G_{n+k} \subseteqq P(G_{m+k})$ for $k \geqq 0$.*

Proof. We proceed by induction on k, the case $k = 0$ being the hypothesis. Suppose that $G_{n+k} \subseteqq P(G_{m+k})$ and that G is a group of minimal order for which $G_{n+k+1} \nsubseteq P(G_{m+k+1})$. Clearly we may assume $P(G_{m+k+1}) = 1$. It follows from Lemma 1 that $(P(G_{m+k}), G) \subseteqq G_{p(m+k)+1}$. Hence $G_{n+k+1} \subseteqq (P(G_{m+k}), G) \subseteqq G_{p(m+k)+1}$. However, $p(m + k) + 1 > n + k + 1$, so $G_{n+k+1} \subset G_{n+k+1}$, a contradiction. Thus $G_{n+k+1} \subseteqq P(G_{m+k+1})$.

REMARK. We shall be most concerned with the case $m = 1$ of Theorem 1: If $G_n \subseteqq P(G)$ and $n < p$, then $G_{n+k} \subseteqq P(G_{1+k})$ for $k \geqq 0$. In Example 1 we show that this result cannot be extended to the case $n \geqq p$.

COROLLARY 1.1. *If $n < p$ and $G_n \subseteqq P(G)$, then*
(a) $(G_i)_n \subseteqq P(G_i)$ *for* $i = 1, 2, 3, \cdots$,
(b) $(P(G))_n \subseteqq P(G_n) \subseteqq P(P(G))$, *and*
(c) *for any* $x \in G$, *if* $H = \langle G_2, x\rangle$, *then* $H_n \subseteqq P(G_2) \subseteqq P(H)$.

Proof. (a) It is known ([4], Th. 2.55, p. 55) that $(G_i)_n \subseteqq G_{in}$. Since $in - (n - 1) \geqq i$ it follows from Theorem 1 that

$$G_{in} \subseteqq P(G_{in-(n-1)}) \subseteqq P(G_i) \,.$$

(b) It follows from Lemma 1 that $(P(G))_n \subseteqq (P(G), (n - 1)G) \subseteqq P(G_n)G_{p+n-1}$. By Theorem 1, $G_{p+n-1} \subseteqq P(G_p)$, so

$$(P(G))_n \subseteqq P(G_n)P(G_p) \subseteqq P(P(G)) \,.$$

(c) Since G_2 is central modulo G_3 and H/G_2 is cyclic, we have $H_2 \subseteqq G_3$. It follows that $H_i \subseteqq G_{i+1}$ for $i \geqq 2$. By Theorem 1, $G_{n+1} \subseteqq P(G_2)$. Thus $H_n \subseteqq G_{n+1} \subseteqq P(G_2) \subseteqq P(H)$.

COROLLARY 1.2. *If $n < p$, $G_n \subseteqq P(G)$, and t is an integer such that $2^t \geqq n + 1$, then $G^{(k+t-1)} \subseteqq P(G^{(k)})$ for $k \geqq 1$.*

Proof. We assume that the result holds for all groups of order less than $|G|$. It follows from Corollary 1.1 that $G^{(1)}$ satisfies the hypothesis of this corollary. Since $|G^{(1)}| < |G|$ we have

$$(**) \qquad (G^{(1)})^{(k+t-1)} \subseteqq P((G^{(1)})^{(k)})$$

for $k \geqq 1$.

By Theorem 2.54 of [4], $G^{(t)} \subseteqq G_{2^t}$. Hence for $k = 1$ it follows from Theorem 1 that $G^{(t)} \subseteqq G_{n+1} \subseteqq P(G_2) = P(G^{(1)})$. If $k > 1$ we replace k by $k - 1$ in (**) and obtain

$$G^{(k+t-1)} = (G^{(1)})^{(k-1+t-1)} \subseteqq P((G^{(1)})^{(k-1)}) = P(G^{(k)}) .$$

REMARK. When $n = t = 2$ in Corollary 1.2 we obtain Theorem 2 of [6].

We now show that Theorem 1 for the case $m = 1$ cannot be extended to include $n \geqq p$.

EXAMPLE 1. Let $\langle a\rangle \wr \langle b\rangle$ be the wreath product of $\langle a\rangle$ by $\langle b\rangle$, where $a^p = b^{p^r} = 1$ and $r > 0$. Then $G_p \subseteqq P(G)$, $P(G_2) = 1$, and $G_{p^r} \neq 1$.

It is clear that the property $G_n \subseteqq P(G)$, $n < p$, is inherited by factor groups and preserved by direct products. By the following example we show that this property is not always inherited by a subgroup H of G.

EXAMPLE 2. Let $W = \langle a\rangle \wr \langle b\rangle$, where $a^p = b^p = 1$. For $2 \leqq n \leqq p - 1$, set $H = W/W_{n+1}$ and $H_n = \langle z\rangle$. Let $\langle d\rangle$ be the cyclic group of order p^2, and G be the group formed by taking the direct product of H and $\langle d\rangle$ with the amalgamation $d^p = z$. Then $G_n = H_n = \langle z\rangle = P(G)$, while $P(H) = 1$.

THEOREM 2. *If $G_n \subseteqq P(G)$ and $n < p$, then for any $x_1, \cdots, x_k$ in G, there is an element h in G such that $x_1^p \cdots x_k^p = h^p$.*

Proof. The result is clear if G is abelian. Suppose that G is nonabelian and that the theorem holds for all groups H with $|H| < |G|$. It follows from (*) that $(x_1 \cdots x_k)^p = x_1^p \cdots x_k^p g_1^p \cdots g_t^p g$, where $g_i \in G_2$ for $1 \leqq i \leqq t$ and $g \in G_p$. By Theorem 1, $G_p \subseteqq P(G_2)$, so there exist elements $g_{t+1}, \cdots, g_r$ in G_2 such that $g = g_{t+1}^p \cdots g_r^p$.

By Corollary 1.1, $(G_2)_n \subseteqq P(G_2)$. Since $|G_2| < |G|$ it follows from the induction hypothesis applied to G_2 that $g_1^p \cdots g_t^p g_{t+1}^p \cdots g_r^p = y^p$, where $y \in G_2$. That is, $x_1^p \cdots x_k^p = (x_1 \cdots x_k)^p s^p$, where $s = y^{-1}$ is in

G_2. Next set $x = x_1 \cdots x_k$ and let $H = \langle G_2, x \rangle$. By Corollary 1.1, $H_n \subseteqq P(H)$. It follows from the Burnside Basis Theorem (see e.g. [3], p. 176) that $d(G) = d(G/K)$ if K is a normal subgroup of G and $K \subseteqq \Phi(G)$. Thus, since G is nonabelian, $H \subset G$. Hence, applying the induction hypothesis to H, $x^p s^p = h^p$ for some h in H. Therefore $x_1^p \cdots x_k^p = h^p$.

COROLLARY 2.1. *If* $G_n \subseteqq P(G)$ *and* $n < p$, *then* $P(P(G)) = P^2(G)$.

REMARK. The results of Theorem 2 and Corollary 2.1 are the best possible. That is, if $n \geqq p$ then it does not follow from $G_n \subseteqq P(G)$ that the products of p-th powers are p-th powers or that $P(P(G)) = P^2(G)$. For if we let $G = \langle a \rangle \wr \langle b \rangle$, where $a^{p^2} = b^{p^2} = 1$, then it can be shown that $G_p \subseteqq P(G)$, while $b^{-p}(ba_0)^p$ is not a p-th power for some $a_0, b \in G$, and $P^2(G) \neq P(P(G))$.

3. Regularity. A p-group G is *regular* if for each pair of elements a, b of G, $(ab)^p = a^p b^p c$ where $c \in P(\langle a, b \rangle_2)$. If G is not regular, G is called *irregular*. It follows from (*) that G is regular if $\langle a, b \rangle_p \subseteqq P(\langle a, b \rangle_2)$ for each 2-generator subgroup $\langle a, b \rangle$ of G. By comparison, $G_p \subseteqq P(G_2)$ whenever $G_n \subseteqq P(G)$ and $n < p$. In addition, the result of Theorem 2 is also true in regular p-groups. Thus the property $G_n \subseteqq P(G)$, $n < p$, is similar to regularity. However, neither of these properties implies the other, as is shown in the next two examples.

First we construct a regular group G for which $G_{p-1} \not\subseteq P(G)$.

EXAMPLE 3. Let $W = \langle a \rangle \wr \langle b \rangle$, where $a^p = b^p = 1$. Set $G = W/W_p$. Since $W_p = P(W)$, clearly $G_{p-1} \neq 1$ and $P(G) = 1$. However, G has class $p - 1$, and is thus regular ([4], Corollary 4.13, p. 73).

Next we construct an irregular group G for which $G_2 \subseteqq P(G)$.

EXAMPLE 4. Let $H = \langle a, b \rangle$, where $a^{p^p} = b^{p^{p-1}} = 1$ and $b^{-1}ab = a^{p+1}$. Then $(a, nb) = a^{p^n}$, so $H_2 \subseteqq \langle a^p \rangle$. Thus $|H_2| = p^{p-1}$ and $H_{p+1} = 1$. On the other hand, $(a, (p-1)b) \neq 1$, so $H_p \neq 1$. Thus H has class p, H_2 is abelian and $d(H) = 2$. It follows from Theorem 1.4 of [7] that there is a positive integer n such that if $H_i = H (i = 1, \cdots, n)$, then $G = H_1 \times \cdots \times H_n$ is irregular. However, it is clear that $G_2 \subseteqq P(G)$.

We know from Example 4 that $G_2 \subseteqq P(G)$ does not imply regularity. However, in that example $d(G) > 2$. We now show that in a finite 2-generator p-group $(p \neq 2)$ $G_2 \subseteqq P(G)$ does imply regularity.

THEOREM 3. *Let* G *be a finite* p*-group* $(p \neq 2)$ *with* $G_2 \subseteqq P(G)$

and $d(G) = 2$. *Then* G *is regular.*

Proof. By Theorem 1, $G_3 \subseteqq P(G_2)$. Hence $d(G_2/P(G_2)) \leqq d(G_2/G_3)$. It follows from Theorem 2.83 of [4] that $d(G_2/G_3) \leqq 1$. By Corollary 1.1, $(G_2)_2 \subseteqq P(G_2)$, so $G_2/P(G_2)$ is an elementary abelian p-group. Thus $[G_2: P(G_2)] \leqq p$, and G is regular by Theorem 2.3 of [5].

We next obtain a characterization of regular 3-groups.

THEOREM 4. *If* G *is a finite* 3-*group, then* G *is regular if, and only if,* $H_3 \subseteqq P(H_2)$ *for each* 2-*generator subgroup* H *of* G.

Proof. It follows from (*) that the latter condition implies regularity. On the other hand, if G is regular, then all subgroups of G are regular. Alperin ([1], Lemma 3.1.1, p. 96) has shown that if H is a regular 2-generator 3-group, then its derived group is cyclic. Hence $H_3 \subseteqq P(H_2)$.

REMARK. If $p = 3$ or $p = 2$ and G is a regular 2-generator p-group, then $G_p \subseteqq P(G_2)$. However, these are the only primes for which this result holds, since the Burnside group of exponent p and 2 generators has class greater than p when $p > 3$.

As in the proof of Theorem 4, if G_i is cyclic, then $G_{i+1} \subseteqq P(G_i)$. In particular, $G_3 \subseteqq P(G_2)$ if $d(G_2) = 1$. If $d(G_2) = 2$ a theorem of Blackburn gives a similar result.

THEOREM 5. *Let* G *be a finite p-group such that* $d(G_2) = 2$. *Then* $G_4 \subseteqq P(G_2)$.

Proof. We may assume $P(G_2) = 1$. It follows from Theorem 1 of [2] that $[G_2: P(G_2)] \leqq p^2$, so $G_4 = 1$.

We now show that for each prime p and each integer $n \geqq 3$, there is a finite p-group G such that $d(G_2) = n$ and $G_4 \not\subseteqq P(G_2)$. This shows that the result of Theorem 5 is not true if $d(G_2) > 2$.

EXAMPLE 5. Let $W = \langle a \rangle \wr \langle b \rangle$, where $a^p = b^{p^3} = 1$. Then $|W_i/W_{i+1}| = p$ for $i \geqq 2$ and W has class p^3. Thus $W_5 \neq 1$. Let $H = W/W_5$. Then H_2 is an elementary abelian p-group, $d(H_2) = 3$, $H_4 \neq 1$, and $P(H_2) = 1$. Thus $H_4 \not\subseteqq P(H_2)$. If $n = 3$ we may let $G = H$. If $n > 3$, let D be one of the nonabelian groups of order p^3. Then $|D_2| = p$. Let K be the group formed by taking the direct product on $n - 3$ copies of D. Set $G = H \times K$. Then $G_2 = H_2 \times K_2$ and $d(G_2) = d(H_2) + (n - 3) = n$. Clearly $G_4 \not\subseteqq P(G_2)$.

4. Bounds on generators of commutator subgroups. Hobby ([6], Th. 3, p. 855) has shown that the condition $G_2 \subseteqq P(G)$ $(p > 2)$ imposes restrictions on the generating elements of $G^{(i)}$ for $i \geqq 0$. In this section we obtain similar results in the case $G_3 \subseteqq P(G)$ and $p > 3$. The procedure used here can be extended to the general case $G_n \subseteqq P(G)$, $n < p$, although the estimates thus obtained are not as precise.

THEOREM 6. *Suppose* $p > 3$, $G_3 \subseteqq P(G)$, *and* $d = d(G)$. *Then* $d(G_3) \leqq (1/2)d(d^2 - 1)$.

Proof. We may assume $\Phi(G_3) = 1$. It then follows from Theorem 1 that $G_4 \subseteqq P(G_2)$ and $G_5 \subseteqq P(G_3) = 1$. Also $P(G_2)$ is abelian, since

$$(P(G_2))_2 \subseteqq (P(G_2), G_2) \subseteqq P(G_4)G_{2(p+1)} = 1$$

by Lemma 1.

We next claim that $d(P(G_2)) \leqq d(G_2/G_3)$. For if $d(G_2/G_3) = t$, then there exist elements $g_1, \cdots, g_t$ in G_2 such that for each $g \in G_2$, $g = g_1^{m(1)} \cdots g_t^{m(t)}h$ for some integers $m(i)$ and $h \in G_3$. It follows from (*) that $g^p = (g_1^p)^{m(1)} \cdots (g_t^p)^{m(t)}h^p cd$, where h^p and c are elements of $P(G_3)$ and $d \in G_{2p}$. Hence $h^p = c = d = 1$ and the assertion follows.

Since $P(G_2)$ is abelian and $G_4 \subseteqq P(G_2)$ we thus have $d(G_4) \leqq d(G_2/G_3)$. Hence

$$\begin{aligned} d(G_3) &\leqq d(G_3/G_4) + d(G_4) \\ &\leqq d(G_3/G_4) + d(G_2/G_3) \\ &\leqq (1/2)d^2(d-1) + (1/2)d(d-1) , \end{aligned}$$

where the last inequality follows from Theorem 2.83 of [4].

THEOREM 7. *Suppose* $p > 3$ *and* $k \geqq 2$. *Let* $x_1, x_2, \cdots, x_d$ *be coset representatives of a minimal basis of the abelian group* $G_k/G_k^{(1)}$. *If* $G_3 \subseteqq P(G)$, *then there exist integers* $n(i)$ *such that*

$$(G_k)^{(1)} = \langle x_1^{p^{n(1)}}, \cdots, x_d^{p^{n(d)}} \rangle .$$

Proof. In any p-group, $(G_k)_2 \subseteqq G_{2k}$. Since $k \geqq 2$ it follows from Theorem 1 that $G_{2k} \subseteqq P(G_{2k-2}) \subseteqq P(G_k)$. Thus the theorem follows from Theorem 3 of [6].

COROLLARY 7.1. *Suppose* $G_3 \subseteqq P(G)$ *where* $p > 3$. *If* $k \geqq 2$ *and if* G_k *can be generated by* d *elements, then* $(G_k)^{(i)}$ *can be generated by* d *elements for* $i = 1, 2, 3, \cdots$.

A p-group G is called *p-abelian* if $(xy)^p = x^p y^p$ for all elements x, y of G. The properties of p-abelian groups used below may be found in [6] (p. 853).

THEOREM 8. *If* $p > 3$, $G_3 \subseteqq P(G)$, *and* $d = d(G)$, *then* $d(G^{(i)}) \leqq (1/2)d(d+1)$ *for* $i = 1, 2, 3, \cdots$.

Proof. We first consider the case $i = 1$. The result is clearly true in this case if $|G| = p$. Suppose the theorem is true when $i = 1$ for all groups H with $|H| < |G|$. We may assume $\Phi(G^{(1)}) = 1$. By Theorem 2.83 of [4], $d(G^{(1)}/G_3) \leqq (1/2)d(d-1)$. A p-group G is p-abelian modulo $P(G^{(1)})G_p$. Since $p > 3$, $G_p \subseteqq P(G_{p-2}) = 1$, so $P(G^{(1)})G_p = 1$ and G is p-abelian. Hence $d(P(G)) \leqq d$. In a p-abelian group $P(G) \subseteqq Z(G)$, so $P(G)$ is abelian. Since $G_3 \subseteqq P(G)$ we have $d(G_3) \leqq d$, so

$$d(G^{(1)}) < d(G^{(1)}/G_3) + d(G_3) \leqq (1/2)d(d+1) .$$

Thus the theorem is true for $i = 1$.

For $i > 1$, Corollary 7.1 yields.

$$d(G^{(i)}) = d((G^{(1)})^{(i-1)}) \leqq d(G^{(1)}) \leqq (1/2)d(d+1) .$$

The author wishes to thank the referee for his suggestions.

BIBLIOGRAPHY

1. J. L. Alperin, *On a special class of regular p-groups*, Trans. Amer. Math. Soc. **106** (1963), 77-99.

2. N. Blackburn, *On prime-power groups in which the derived group has two generators*, Proc. Camb. Phil. Soc. **53** (1957), 19-27.

3. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

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

5. ———, *On a theorem of Frobenius*, Proc. Lond. Math. Soc. (2) **40** (1936), 468-501.

6. C. Hobby, *A characteristic subgroup of a p-group*, Pacific J. Math. **10** (1960), 853-858.

7. P. M. Weichsel, *Regular p-groups and varieties*, Math. Zeit. **95** (1967), 223-231.

Received November 9, 1967, and in revised form July 15, 1968. This paper contains portions of the author's doctoral thesis at the University of Washington. The research was supported in part by the National Science Foundation under grant NSF GP-5691.

IOWA STATE UNIVERSITY

Pacific Journal of Mathematics

Vol. 29, No. 1 May, 1969