PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 32, Number 1, March 1972

ELEMENTS OF MAXIMAL ORDER IN FINITE p-GROUPS

GUY T. HOGAN

ABSTRACT. Let G be a finite p-group such that every 3-generator subgroup has class at most p. If $K(G)$ denotes the subgroup of G generated by the elements of maximal order in G, then $K(G)$ has index at most p in G.

G. Zappa proved [5] that if G is a finite p-group of class at most p, then $H_p(G)$ has index at most p in G, unless $H_p(G)=1$. Here $H_p(G)$ denotes the subgroup of G generated by those elements of G having order different from p. If we let $K(G)$ be the subgroup of G generated by the elements of maximal order in G, then, of course, $K(G)\subseteq H_p(G)$, whenever $H_p(G)\neq 1$. So we describe a construction which yields a family of examples, for each odd prime p and arbitrary exponent greater than p^2, of finite p-groups of class p with $K(G)\neq H_p(G)$. Thus, our result is a strengthening of Zappa's, although the techniques are essentially the same. Recently, I. D. Macdonald [3], [4] extended Zappa's results in a different direction.

Our main goal is the proof of the following

THEOREM. *Let G be a finite p-group such that every 3-generator subgroup has class at most p. Then $[G:K(G)]\leqq p$.*

The notation will be the same as in [1]. The computational aspect of the proof will be facilitated greatly by the following lemma.

LEMMA. *Let G be a finite p-group of exponent p^{m+1}, with the exponent of G_2 a divisor of p^m. If $y\in K(G)$, and $x\in G\setminus K(G)$, then*

$$y^{-p^m} \equiv [y, {}_{p-1}x]^{p^{m-1}} \pmod{G_{p+1}}.$$

PROOF. Since we argue modulo G_{p+1}, we may as well assume that $G_{p+1}=1$, that is, G has class at most p. From $y\in K(G)$, and $x\in G\setminus K(G)$, it follows that $xy\in G\setminus K(G)$. By the Hall-Petrescu Identity [2, Chapter III, Satz 9.4, Hilfsatz 9.5],

$$x^{p^m}y^{p^m} = (xy)^{p^m}\prod_{k=2}^{p^m} C_k^{\binom{p^m}{k}} \tag{1}$$

Presented to the Society, March 27, 1970; received by the editors May 7, 1971.
AMS 1970 *subject classifications*. Primary 20D15, 20D25.
Key words and phrases. Finite p-group, maximal order, exponent, H_p-subgroup.

where $C_k \in G_k$, and $C_p = [y, {}_{p-1}x]^a \prod_i V_i^{a_i}$, $a \equiv -1 \pmod{p}$, and each V_i has the form $[y, x, z_2, \cdots, z_{p-2}]$ with each z_j equal to x or y, and at least one equal to y. But p^m divides $\binom{p^m}{k}$ if $k < p$, and, by assumption, $c(G) \leqq p$ and $\exp(G_2)$ divides p^m. Thus, (1) reduces to

$$y^{p^m} = C_p^{\binom{p^m}{p}} = \left\{[y, {}_{p-1}x]^a \prod_i V_i^{a_i}\right\}^{\binom{p^m}{p}}. \tag{2}$$

This may be further simplified if we observe that $\binom{p^m}{p} \equiv p^{m-1} \pmod{p^m}$, so that we may replace $\binom{p^m}{p}$, in (2), by p^{m-1}. Now let W_k be the product of all the $V_i^{a_i}$'s which have weight k in x, and weight $p-k$ in y ($k = 1, 2, \cdots, p-2$), and observe that (2) remains valid if we replace x by x^r, $1 \leqq r \leqq p-1$. We then get, for each of these r,

$$y^{p^m} = \left\{[y, {}_{p-1}x^r]^a \prod_{k=1}^{p-2} W_k^{r^k}\right\}^{p^{m-1}}. \tag{3}$$

If we now multiply these $p-1$ quantities together, ignoring the ordering of the factors since they all belong to $Z(G)$, we get

$$y^{p^m(p-1)} = \left\{[y, {}_{p-1}x]^{a\sum_{r=1}^{p-1} r^{p-1}} \prod_{k=1}^{p-2} W_k^{\sum_{r=1}^{p-1} r^k}\right\}^{p^{m-1}}, \tag{4}$$

or, on further reduction,

$$y^{-p^m} = [y, {}_{p-1}x]^{ap^{m-1}\sum_{r=1}^{p-1} r^{p-1}} \prod_{k=1}^{p-2} W_k^{p^{m-1}\sum_{r=1}^{p-1} r^k}. \tag{4'}$$

But $a \equiv -1 \pmod{p}$, and $\sum_{r=1}^{p-1} r^{p-1} \equiv -1 \pmod{p}$. Furthermore, $\sum_{r=1}^{p-1} r^k \equiv 0 \pmod{p}$, if $1 \leqq k \leqq p-2$. Since the exponent of G_2 divides p^m, we see that the powers of W_k above are all equal to the identity, so that finally we have $y^{-p^m} = [y, {}_{p-1}x]^{p^{m-1}}$ which proves the lemma.

We are now ready to prove the theorem.

PROOF. Assume the theorem false and let G be a minimal counter-example, so that $[G:K(G)] \geqq p^2$. Then there exists a subgroup $V \subseteq G$, such that $K(G) \subset V \subseteq G$, and $[V:K(G)] = p^2$. Clearly, then, $K(V) = K(G)$, and V satisfies the hypothesis of the theorem. By minimality of the order of G, this gives $V = G$, so $K(G)$ has index p^2 in G. Pick elements a, b in $G \backslash K(G)$ such that $G = \langle a, b, K(G)\rangle$ and let y be an element of order p^{m+1} = exponent of G. If $U = \langle a, b, y\rangle$, then $\exp(U) = \exp(G)$, so that $K(U) \subseteq K(G)$. Hence, $K(U) \subseteq U \cap K(G)$. Since $G = UK(G)$, then if U were a proper subgroup of G, we would have

$$p \geqq [U:K(U)] \geqq [U:U \cap K(G)] = [UK(G):K(G)] = [G:K(G)] = p^2.$$

Thus, $G = U = \langle a, b, y\rangle$, so that G is a 3-generator group, and G has class p.

With a view toward applying the lemma, we now show that G_2 has exponent dividing p^m. Let $L = \langle a, d\rangle$, where $d \in G_2$. Then L_2 is generated by

$[a, d]$ and all its conjugates in L, so that $L_2 \subseteq G_3$. Then $L_3 \subseteq G_4$, and, continuing thus, we have $L_p \subseteq G_{p+1} = 1$. This means that L has class at most $p-1$. Hence, L is a regular p-group, so that $L = K(L)$. If d had order p^{m+1}, then $L = K(L) \subseteq K(G)$. But this cannot occur since $a \in L \setminus K(G)$. Therefore, $\exp(G_2) < \exp(G)$.

Now suppose we could find $x \in G \setminus K(G)$ such that $x^p \notin K(G)$. Let $x^p = u$. By the lemma, we have

$$\begin{aligned} y^{-p^m} &= [y, {}_{p-1}u]^{p^{m-1}} = [y, {}_{p-2}u, x^p]^{p^{m-1}} \\ &= [y, {}_{p-2}u, x]^{p^m} = 1 \end{aligned}$$

since the commutators above belong to $Z(G) \cap G_2$. But this contradicts the fact that $\exp(G) = p^{m+1}$. We may assume, therefore, that a and b are so chosen that $aK(G)$ and $bK(G)$ are independent generators of $G/K(G)$. Then $a^r b^s \in K(G)$ iff $r \equiv s \equiv 0 \pmod{p}$. So, by the lemma,

$$y^{-p^m} = [y, {}_{p-1}a^r b]^{p^{m-1}}$$

where we are taking $r = 1, 2, \cdots, p-1$. Expanding on the right, recalling that G has class p, we get

$$y^{-p^m} = \left\{ \prod_{k=0}^{p-1} W_k^{r^k} \right\}^{p^{m-1}}$$

where W_k is the product of all commutators having the form

$$[y, z_1, z_2, \cdots z_{p-1}],$$

and each $z_j = a$ or b, with k of them equal to a, the remaining $p-k-1$, of course, equal to b. In particular, $W_0 = [y, {}_{p-1}b]$ and $W_{p-1} = [y, {}_{p-1}a]$. Isolating these two factors, and using the congruence $r^{p-1} \equiv 1 \pmod{p}$, if $r \not\equiv 0 \pmod{p}$, we get

$$y^{-p^m} = W_0^{p^{m-1}} W_{p-1}^{p^{m-1}} \prod_{k=1}^{p-2} W_k^{p^{m-1} r^k}.$$

Now we multiply these equations together, for $r = 1, 2, \cdots, p-1$ making use of the relation $\sum_{r=1}^{p-1} r^k \equiv 0 \pmod{p}$, if $1 \leqq k \leqq p-2$, and the fact that the exponent of G_p divides p^m. This gives

$$y^{p^m} = W_0^{-p^{m-1}} W_{p-1}^{-p^{m-1}}.$$

But, by the lemma, $y^{p^m} = W_0^{-p^{m-1}}$. This forces $W_{p-1}^{p^{m-1}} = 1$, so that, again, by the lemma, $y^{p^m} = 1$. This contradiction proves the theorem.

EXAMPLE. We construct a family of examples, for each odd prime p and exponent p^{r+1}, $r \geqq 2$, of finite p-groups, G, of class p, with $[G : K(G)] = p$, and $H_p(G) = G$.

Let p be any odd prime, and $r>1$ be an integer. Let

$$A = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_{p-1}\rangle \times \langle b\rangle,$$

with $|a_1|=p^{r+1}$, $|a_k|=p^r$, for $1<k<p$, and $|b|=p^{r-1}$. Define an automorphism, x, of A by

$$\begin{aligned} a_k^x &= a_k a_{k+1} \quad \text{for } 1 \leqq k < p-1, \\ a_{p-1}^x &= a_{p-1}a_1^{-p}b, \\ b^x &= ba_2^p. \end{aligned}$$

Let G be the split extension of A by $\langle x\rangle$. For convenience, let $a_p=ba_1^{-p}$. Then $G=\langle a_1, x\rangle$ is metabelian so the formulas of Lemma 3 in [1] may be used to simplify some of the computations below.

$$\begin{aligned} [a_1, {}_k x] &= [a_k, x] = a_{k+1}, \qquad 1 \leqq k < p-1, \\ [a_1, {}_{p-1}x] &= [a_{p-1}, x] = a_1^{-p}b = a_p, \\ [a_1, {}_p x] &= [a_p, x] = [b, x][a_1, x]^{-p} = a_2^p a_2^{-p} = 1. \end{aligned}$$

Thus, G has class p, and $\exp(G_2)=p^r$. For any $a\in A$,

$$[a, x^{p^r}] = \prod_{j=1}^{p^r} [a, {}_j x]^{\binom{p^r}{j}} = \prod_{j=1}^{p-1} [a, {}_j x]^{\binom{p^r}{j}} = 1,$$

and inspection of the corresponding equations for $[a, x^{p^{r-1}}]$ shows that x has order p^r. Now A has exponent p^{r+1}, and if $1\leqq k<p^r$, $a\in A$, we find, by Lemma 3 of [1],

$$(ax^{-k})^{p^r} = a^{p^r} \prod_{0<i+j<p^r} [a, {}_i x^k, {}_j a]^{\binom{p^r}{i+j+1}} x^{-kp^r}$$

which simplifies to

$$(ax^{-k})^{p^r} = a^{p^r}[a, {}_{p-1}x]^{k^{p-1}\binom{p^r}{p}} = a^{p^r}[a, {}_{p-1}x]^{k^{p-1}p^{r-1}}$$

since $\binom{p^r}{p}\equiv p^{r-1} \pmod{p^r}$, and $\exp(G_2)=p^r$. But the element above has order at most p, so that $\exp(G)=p^{r+1}$. Taking $a=a_1$, we see that $(a_1x^{-p})^{p^r}=a_1^{p^r}\neq 1$, so that $a_1x^{-p}\in K(G)$. Since $A\subseteq K(G)$, this gives $x^{-p}\in K(G)$. Hence, $A\langle x^p\rangle\subseteq K(G)$. The elements of $G\backslash A\langle x^p\rangle$ are all expressible in the form ax^{-k} for $k\not\equiv 0 \pmod p$, so for these values of k we have $k^{p-1}\equiv 1 \pmod p$. Writing $a=\prod_{i=1}^{p} a_i^{e_i}$ we have

$$(ax^{-k})^{p^r} = (a_1^p a_p)^{e_1 p^{r-1}} = b^{e_1 p^{r-1}} = 1.$$

Hence, $K(G)=A\langle x^p\rangle$, and, of course, $[G:K(G)]=p$. Finally, $x\in H_p(G)$, and $a_1\in H_p(G)$, so $H(G)=G_p$.

REFERENCES

1. G. T. Hogan and W. P. Kappe, *On the H_p-problem for finite p-groups*, Proc. Amer. Math. Soc. **20** (1969), 450–454. MR **39** #312.

2. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967. MR **37** #302.

3. I. D. Macdonald, *The Hughes problem and others*, J. Austral. Math. Soc. **10** (1969), 475–479. MR **40** #7353.

4. ———, *Solution of the Hughes problem for finite p-groups of class $2p-2$*, Proc. Amer. Math. Soc. **27** (1971), 39–42.

5. G. Zappa, *Contributo allo studio del problema di Hughes sui gruppi*, Ann. Mat. Pura Appl. (4) **57** (1962), 211–219. MR **25** #1210.

DEPARTMENT OF MATHEMATICS, STATE UNIVERSITY COLLEGE OF NEW YORK, ONEONTA, NEW YORK 13820