

SOLUTION OF THE HUGHES PROBLEM FOR FINITE p -GROUPS OF CLASS $2p-2$

I. D. MACDONALD¹

ABSTRACT. In this paper the Hughes conjecture for finite p -groups is proved in the case of groups which are nilpotent of class $2p-2$.

If G is a group and p is a prime number then the Hughes subgroup $H_p(G)$ of G is by definition the subgroup generated by all elements of G that do *not* have order p . The conjecture of Hughes was that if $G > H_p(G) > 1$ then $H_p(G)$ must have index p in G ; see [6]. Hughes showed that the conjecture is true for $p=2$ and all G , and Straus and Szekeres [10] proved it for $p=3$ and all G . Hughes and Thompson [7] proved the corresponding result for all p and for G finite and nonnilpotent.

The most interesting cases which remain are those in which G is a finite p -group with $p \geq 5$; throughout this note we shall take G to be a finite p -group, and our results will be of most significance when $p \geq 5$. We may remark at this point that it is a nontrivial exercise to construct a p -group G_p for each prime p such that $G_p > H_p(G_p) > 1$.

Though Wall [11] has shown by means of an example that the Hughes conjecture is false for finite 5-groups and $p=5$, it is nevertheless of some interest to find sufficient conditions for the conjecture to hold. Thus Zappa [12] has shown that all is well when G is nilpotent of class p . The main result of the present note is a substantial strengthening of this:

THEOREM. *The Hughes conjecture is valid for finite p -groups of nilpotency class $2p-2$.*

It seems likely to us that class $2p-2$ cannot be replaced by a much greater class without falsifying the theorem.

The proof of this theorem depends heavily on the main result of [8], which we state again in the interests of clarity:

THEOREM [8]. *If $|G:H_p(G)| \geq p^2$, $V_p(G) \leq \zeta(G)$ and $\gamma_{2p}(G) = 1$, then $V_p(H_p(G) \cap \gamma_2(G)) = 1$.*

Received by the editors February 3, 1970.

AMS 1970 subject classifications. Primary 20D15, 20D25.

Key words and phrases. Finite p -group, Hughes subgroup, commutator collection.

¹ I thank the University of Dundee for its generosity in respect of finance and hospitality.

Copyright © 1971, American Mathematical Society

Here $V_p(G)$ is the subgroup of G generated by all the p th powers in G , $\zeta(G)$ is the centre of G , and $\gamma_n(G)$ is the n th term of the lower central series of G for each $n \geq 1$. By definition G is nilpotent of class n if and only if $\gamma_{n+1}(G) = 1$. The symbol $|G:H|$ denotes the index of the subgroup H in G .

Suppose that G is a finite p -group of class $2p-2$ such that the Hughes conjecture is not valid for G and p . We prove the theorem by deducing a contradiction. Thus we have $|G:H_p(G)| \geq p^2$ and $H_p(G) > 1$ at the outset. Next let N be a normal subgroup of G with index p in $V_p(G)$ and put $G' = G/N$. Since $H_p(G/N) \leq H_p(G)/N$ we have $|G':H_p(G')| \geq p^2$ and $H_p(G') > 1$, with of course $V_p(G') \leq \zeta(G')$. The Hughes conjecture does not hold for G' , and by dropping the prime we may and shall consider G with $V_p(G) \leq \zeta(G)$ in place of G' . The theorem of [8] shows at once that $V_p(H_p(G) \cap \gamma_2(G)) = 1$ for this G .

The rest of the proof is very like that of the theorem in [8], with the difference that the theorem of [8] itself now plays the role of the lemma of [8]; the formalism is the same in the two cases. We shall however give the full details.

Let $y \in H_p(G)$ and let $x \in G$ with $x \notin H_p(G)$. Then $x^p = (xy)^p = 1$, and

$$y^{-p}x^{-p}(xy)^p = y^{-p}.$$

Commutator collection—for facts about which see [3]—can be applied to $y^{-p}x^{-p}(xy)^p$. The first result we obtain is that $y^{-p}x^p(xy)^p \in \gamma_2(G)^p \gamma_p(G)$. Commutator collection theory tells us much more, however. The relevant commutators in $\gamma_2(G)$ all have y as an entry, so they lie in $H_p(G) \cap \gamma_2(G)$ and by a fact stated earlier they all have order p or 1. We conclude that $y^{-p} \in \gamma_p(G)$; indeed y^{-p} is a power product of certain commutators in $\{x, y\}$, each having at least p entries. As before these commutators in $\gamma_p(G)$ have order p or 1. Note that $\gamma_p(G)$ is abelian since G has class $2p-2$.

Since $|G:H_p(G)| \geq p^2$ we can find elements x_1, x_2 of G such that if $x_1^\alpha x_2^\beta \in H_p(G)$ with $0 \leq \alpha, \beta < p$ then $\alpha = \beta = 0$. We now put $x = x_1^\alpha x_2^\beta$ where $0 \leq \alpha, \beta < p$ and not both α and β are 0; later we consider all values of α and β with these restrictions, but at present α and β are fixed. Commutator expansion then gives an expression for y^{-p} which is a power product of commutators each having at least p entries from $\{y, x_1^\alpha, x_2^\beta\}$ and at least one entry from $\{y\}$. Indeed repeated expansion gives y^{-p} as a power product of commutators having at least p entries from $\{y, x_1, x_2\}$; at least one entry in each is y , and each has order p or 1.

The crux of the matter is the exponent of each commutator with entries in $\{y, x_1, x_2\}$. We lose no generality in assuming that all

commutators are in a basic form, and (since G has class $2p-2$) at most $2p-3$ entries are from $\{x_1, x_2\}$. Then, as shown in [8], collection theory indicates that the exponent of each commutator is some polynomial in $\{\alpha, \beta\}$ whose total degree does not exceed $2p-3$. Hence we have

$$y^{-p} = \prod c_{ij}^{\alpha^i \beta^j},$$

where the c_{ij} are power products of commutators with at least p entries from $\{y, x_1, x_2\}$, and the product is taken over all nonnegative i, j with $1 \leq i+j \leq 2p-3$.

As α and β range over their possible values we obtain a (multiplicatively written) system of linear equations in the c_{ij} and y^p with integers modulo p for coefficients. In the lemmas which follow it is made clear that these equations imply $y^p=1$ and so $H_p(G)=1$, a contradiction which completes the proof of the theorem. We remark that the lemmas are written in additive notation and that at this stage we use in the essential way the fact that G has class $2p-2$.

LEMMA 1. *If the equations $\sum_{1 \leq j \leq p-1} \beta^j z_j = 0$ hold for $1 \leq \beta \leq p-1$ over the field of p elements, then $z_{p-1} = 0$.*

PROOF. Consider the matrix involved in this system of $p-1$ linear equations in z_1, \dots, z_{p-1} . As Brisley shows in [1, p. 66] it can be put into a triangular form by certain permissible row operations, and from this form it is evident that each z_j is 0. In particular $z_{p-1} = 0$.

LEMMA 2. *If the equations $\sum_{0 \leq i+j \leq 2p-3} \alpha^i \beta^j z_{ij} = 0$ hold for $0 \leq \alpha < p$, $0 \leq \beta < p$ and not both α and β equal to 0, over the field of p elements, then $z_{00} = 0$.*

PROOF. We intend of course that neither i nor j takes negative values. Fix α at some nonzero value, put $\beta = 0$ in the equations, and on subtraction we have

$$\sum_{1 \leq i+j \leq 2p-3; i \geq 0, j > 0} \alpha^i \beta^j z_{ij} = 0.$$

Lemma 1 therefore gives $\sum_{0 \leq i \leq p-2} \alpha^i z_{i, p-1} = 0$ for each nonzero α (note that $\gamma_{2p-1}(G)=1$). On applying Lemma 1 again we have $z_{0, p-1} = 0$. But substitution of $\alpha = 0$ gives $\sum_{0 \leq j \leq 2p-3} \beta^j z_{0j} = 0$ for $1 \leq \beta \leq p-1$. This time Lemma 1 gives $z_{00} + z_{0, p-1} = 0$, and we conclude that $z_{00} = 0$. This proves Lemma 2, and with it the theorem.

We conclude with some remarks on the work of Hogan and Kappe [5], who show that the Hughes conjecture is valid for finite meta-

belian p -groups and all primes p . Their proof may be much shortened by noting that the Hughes conjecture is correct for finite p -groups of class $p+1$, by the theorem above. We indicate yet another argument. Let G be metabelian with $H_p(G) > 1$ and $|G:H_p(G)| \geq p^2$; as usual we assume that $V_p(G) \leq \zeta(G)$. Since $G/V_p(G)$ is a metabelian group of exponent p it satisfies the law $(x, (p-1)y) = 1$ by a theorem of Meier-Wunderli [9]. Hence the law $(x, (p-1)y, z) = 1$ holds in G . It now follows from a theorem of Gupta and Newman [2] on metabelian groups that G has class p , and at this point the Zappa theorem gives the required result.

We might ask whether a finite metabelian p -group can have any of the properties (Pi) mentioned in [8]. We have just proved that it cannot have (P1), which at once implies the impossibility of (P2) and (P3). Elementary commutator arguments dispose of (P4). However we have not managed to do anything with (P5); that is to say we are unable to solve the problem of Hobby [4] for finite metabelian p -groups.

REFERENCES

1. Warren Brisley, *On varieties of metabelian p -groups, and their laws*, J. Austral. Math. Soc. 7 (1967), 64–80. MR 34 #7646.
2. N. D. Gupta and M. F. Newman, *On metabelian groups*, J. Austral. Math. Soc. 6 (1966), 362–368. MR 34 #2694.
3. Marshall Hall, Jr., *The theory of groups*, Macmillan, New York, 1959. MR 21 #1996.
4. C. R. Hobby, *Nearly regular p -groups*. Canad. J. Math. 19 (1967), 520–522. MR 35 #6757.
5. Guy T. Hogan and Wolfgang P. Kappe, *On the H_p -problem for finite p -groups*, Proc. Amer. Math. Soc. 20 (1969), 450–454. MR 39 #312.
6. D. R. Hughes, *A problem in group theory*, Bull. Amer. Math. Soc. 63 (1957), 209.
7. D. R. Hughes and J. G. Thompson, *The H_p -problem and the structure of H_p -groups*, Pacific J. Math. 9 (1959), 1097–1101. MR 21 #7248.
8. I. D. Macdonald, *The Hughes problem and others*, J. Austral. Math. Soc. 10 (1969), 475–479.
9. H. Meier-Wunderli, *Metabelsche Gruppen*, Comment. Math. Helv. 25 (1951), 1–10. MR 12, 671.
10. E. G. Straus and G. Szekeres, *On a problem of D. R. Hughes*, Proc. Amer. Math. Soc. 9 (1958), 157–158. MR 20 #73.
11. G. E. Wall, *On Hughes' H_p problem*, Proc. Internat. Conference Theory of Groups (Canberra, 1965), Gordon and Breach, New York, 1967, pp. 357–362. MR 36 #2686.
12. G. Zappa, *Contributo allo studio del problema di Hughes sui gruppi*, Ann. Mat. Pura Appl. (4) 57 (1962), 211–219. MR 25 #1210.

THE UNIVERSITY OF DUNDEE, DUNDEE, SCOTLAND