MINIMAL RELATIONS FOR CERTAIN FINITE p-GROUPS

BY
D. L. JOHNSON AND J. W. WAMSLEY

ABSTRACT

It is an open question whether or not every finite p-group G has a presentation with $d(G) = \dim H^1(G,Z_p)$ generators and $r(G) = \dim H^2(G, Z_p)$ relations; in this article, a large number of examples are given to show that such a presentation does exist for nearly all such groups for which $r(G)$ has been calculated.

0. **Introduction.** Let G be a finite p-group having a minimal generating set $\{x_1, \cdots, x_n\}$ so that, by the Burnside Basis Theorem, $n = d(G)$ is an invariant of G. If F is the free group on generators $y_1, \cdots, y_n$, we have a free presentation of G with kernel R:

$$1 \to R \to F \overset{\pi}{\to} G \to 1 \tag{1}$$

where $y_i\pi = x_i$, $1 \leqq i \leqq n$. Let $r'_\pi(G)$ ($r_\pi(G)$) be the smallest number of elements of R ($R/R'R^p$) which together with their conjugates generate R ($R/R'R^p$); then $r'_\pi(G) \geqq r_\pi(G)$, and $r'_\pi(G)$ is the smallest number of relations required to define G in terms of $x_1, \cdots, x_n$. Further, it is well known (see [3]) that

$$d(G) = \dim H^1(G, Z_p),$$
$$r_\pi(G) = \dim H^2(G, Z_p),$$

and thus $r_\pi(G) = r(G)$ is an invariant of G with $r(G) \geqq d(G)$.

Problem 1. Is $r'_\pi(G)$ an invariant of G?

We avoid this problem by defining $r'(G) = \min_\pi r'_\pi(G)$, so that

$$r'(G) \geqq r(G) \geqq d(G), \tag{2}$$

and concern ourselves with the following question.

Problem 2. For which groups G is $r'(G) = r(G)$?

Received June 3, 1970

Both these problems appear on p. 103 of [3] and, while the latter has been solved for profinite p-groups [12] where the conjectured equality is always true, it is still an open question in the case in hand.

Writing $\bar{G} = R \cap F'/[F,R]$ in accordance with (1), $\bar{G}$ is an invariant of G called the Schur multiplicator, and we know that

$$d(\bar{G}) = r(G) - d(G).$$

As a special case of problem 2 we can ask (see [11]):

Problem 3. If $d(\bar{G}) = 0$, is it true that $r'(G) = r(G)$?

The following well-known improvement of the famous theorem of Golod-Šafarevič [2] is proved in [3, p. 104]. For G a finite p-group,

$$r(G) > d(G)^2/4 \tag{3}$$

Now define $\mathbf{G}_p$ to be the class of all finite p-groups G such that $r'(G) = r(G)$; then our aim in this article is to prove, with several interesting exceptions, that $\mathbf{G}_p$ contains all those groups G for which $r(G)$ has been calculated, and to this end the exposition is divided up into seven sections. As additional motivation, we briefly discuss an application of the above ideas to extension theory.

Let $G \in \mathbf{G}_p$ be a group having a minimal presentation

$$G = \langle x_1, \cdots, x_n \mid r_1, \cdots, r_s \rangle,$$

the r_i being words in the x_j's (the equating of each of which to 1 gives a set of defining relations for G), so that $n = d(G)$, $s = r'(G) = r(G)$. We write $V_s(K) = \{(\alpha_1, \cdots, \alpha_s) \mid \alpha_i \in K,\ 1 \leqq i \leqq s\}$, the m-dimensional vector space over the field K of p elements, $Z_p = \langle y \mid y^p \rangle$, and $\hat{G} = H^2(G, Z_p)$, the group of (necessarily central) extensions of G by Z_p. Thus, $\hat{G}$ may be identified with $V_s(K)$. We now define a mapping

$$\zeta : V_s(K) \to \hat{G} = V_s(K)$$

by asserting that $(\alpha_1, \cdots \alpha_s)\zeta$ = the equivalence class of extensions containing the group

$$\langle x_1, \cdots, x_n, y \mid r_1 y^{-\alpha_1}, \cdots, r_s y^{-\alpha_s}, [x_1, y], \cdots, [x_n, y], y^p \rangle,$$

which is easily seen to be K-linear and bijective. Using the main result of [18], this construction can be generalised to any finite p-group G.

The following two assertions are immediate consequences of these remarks.

a) $d((\alpha_1,\cdots,\alpha_s)\zeta)$ is equal to $n+1$ if $(\alpha_1,\cdots,\alpha_s)=0$, and is equal to n otherwise.

b) if $|G| = p^k$, then G has a presentation with k generators and $k(k+1)/2$ relations.

Turning momentarily to arbitrary finite groups, we can ask the question:

Problem 4. Which finite groups G have presentations with $d(G)$ generators and $d(G)+d(\bar{G})$ relations?

Denoting this class of groups by $\boldsymbol{G}$, let G_k be the split extension of the direct product of k copies of Z_7 by the 'squaring' automorphism (of order 3); then it is shown in [14] that G_k does not belong to $\boldsymbol{G}$ for $k \geqq 3$, even though $|\bar{G}_k| = 1$. However, presentations are given in [20] for the groups $PSL(2,p)$, $p \geqq 3$, with two generators and three relations, and it is known [13] that $d(\overline{PSL(2,p)}) = 1$ for p odd. Hence, all these groups lie in $\boldsymbol{G}$. (Of course,

$$PSL(2,2) = \langle x,y \mid x^2y^{-3}, y^xy^{-2}\rangle \in \boldsymbol{G}).$$

1. **Groups with** $r' = d$. We consider groups G with $r' = d$. By (2), all such groups are in $\boldsymbol{G}_p$.

$d(G) = 1$. This class coincides with the class of cyclic groups:

$$G = \langle x \mid x^{p^\alpha}\rangle.$$

$d(G) = 2$. The only examples we know of such groups are certain metacyclic groups and a class of groups

$$G(\alpha,\beta) = \langle x,y \mid [x,z] = x^{p^\alpha},\ [y,z^{\pm 1}] = y^{p^\beta},\ [x,y] = z^{\pm 1}\rangle$$

given in [8] and [16].

Problem 5. What other groups are there with $r' = d = 2$?

$d(G) = 3$. The only examples known to us here are the groups

$$G_1 = \langle x,y,z \mid [x,y] = x^2,\ [y,z] = y^2,\ [z,x] = z^2\rangle,$$

$$G_2 = \langle x,y,z \mid [x,y] = x^{-2}, [y,z] = y^{-2}, [z,x] = z^{-2}\rangle$$

due to Mennicke [9], and

$$G_3 = \langle x,y,z \mid [x,z] = x^2, [x,y] = z^2, [z^{-1},y^{-1}] = y^2\rangle,$$

$$G_4 = \langle x,y,z \mid [x,z] = x^2, [x,y] = z^2, [y,z] = y^2\rangle,$$

$$G_5 = \langle x,y,z \mid [x,z] = x^{-3}, [z^{-1},y^{-1}] = y^{-3}, [x,y] = z^3\rangle,$$

$$G_6 = \langle x,y,z \mid [x,z] = x^{-3}, [y,z] = y^{-3}, [x,y] = z^3\rangle,$$

dealt with in [16].

The cases $r'(G) = d(G) = s$ for $s \geqq 4$ are precluded by (2) and (3) above.

Problem 6. Does there exist a finite p-group G with $r'(G) = 5$ and $d(G) = 4$? A likely one might be

$$G = \langle a, b, c, d \mid [a, b] = a^2, [b, c] = b^2, [c, d] = c^2, [d, a] = d^2, [a, c] = [b, d] \rangle,$$

which, if finite, must be a 2-group and so in $\boldsymbol{G}_2$, by (2) and (3).

2. **Direct products.** We first observe (see [7]) that

$$(4) \qquad \begin{cases} d(G \times H) = d(G) + d(H), \\ r(G \times H) = r(G) + r(H) + d(G)d(H). \end{cases}$$

If we now write

$$G = \langle X \mid R \rangle, \; H = \langle Y \mid S \rangle,$$

then, regarding G and H as subgroups of $G \times H$ in the usual way,

$$G \times H = \langle X, Y \mid R, S, [X, Y] \rangle,$$

so that:

$$r'(G \times H) \leqq r'(G) + r'(H) + d(G)d(H).$$

It follows from this formula, together with (2) and (4), that:

$$G, H \in \boldsymbol{G}_p \Rightarrow G \times H \in \boldsymbol{G}_p.$$

Thus, with the aid of the case $d(G) = 1$ of section 1, we see that $\boldsymbol{G}_p$ contains all finite abelian p-groups.

As to the closure of $\boldsymbol{G}_p$ under the formation of direct factors, very little can be said; even the following question, posed by R. A. Walton, is by no means an easy one.

Problem 7. If G, $G \times H \in \boldsymbol{G}_p$, does it follow that $H \in \boldsymbol{G}_p$?

3. **Dihedral groups and their extensions by** Z_2. The values of r for such groups have been found by Munkholm, [10], and we merely check that all the groups in question lie in $\boldsymbol{G}_2$. We define the dihedral group of order 2^n as follows:

$$D_n = \langle x, y \mid y^{2^{n-1}} = x^2 = (yx)^2 = 1 \rangle, \quad n \geqq 2,$$

whence it is clear that $d(D_n) = 2$, $r'(D_n) = 3$ for all admissible values of n. We obtain the extensions of D_n by $Z_2 = \langle a \mid a^2 \rangle$ by using the mapping ζ of section 0 to construct the following table ($n \geqq 3$):

Group	$y^{2^{n-1}}=$	$x^2=$	$(yx)^2=$	$\cong$	d	r
G_1	1	1	1	$Z_2 \times D_n$	3	6
G_2	1	1	a	$\cong$ (with G_3)	2	4
G_3	1	a	1		2	4
G_4	1	a	a		2	3
G_5	a	1	1	D_{n+1}	2	3
G_6	a	1	a	$\cong$ (with G_7)	2	2
G_7	a	a	1		2	2
G_8	a	a	a	Q_{n+1}	2	2

where Q_{n+1} is the generalised quaternion group of order 2^{n+1}:

$$Q_{n+1} = \langle x, y \mid y^{2^{n-1}} = x^2 = (yx)^2 \rangle, \qquad n \geqq 2.$$

Since the mappings

$$\omega_1 : G_2 \to G_3, \omega_2 : G_6 \to G_7,$$

given by $\omega_i(a) = a$, $\omega_i(y) = y$, $\omega_i(x) = yx$ $(i = 1,2)$, are isomorphisms and G_1, G_5, G_8 have already been dealt with there remain only three cases:

$$\begin{aligned} G_3 &= \langle x, y, a \mid y^{2^{n-1}} = 1 = (yx)^2, x^2 = a, [x,a] = [y,a] = a^2 = 1 \rangle \\ &= \langle x, y \mid y^{2^{n-1}} = 1 = (yx)^2, x^4 = 1 = [y, x^2] \rangle, \end{aligned}$$

which shows immediately that $G_3 \in \mathbf{G}_2$.

$$\begin{aligned} G_4 &= \langle x, y, a \mid y^{2^{n-1}} = 1, x^2 = a = (yx)^2, [x,a] = [y,a] = a^2 = 1 \rangle \\ &\quad \langle x, y \mid y^{2^{n-1}} = 1, x^2 = (yx)^2, [y, x^2] = x^4 = 1 \rangle, \end{aligned}$$

and since the relation $[y, x^2] = 1$ can be deduced from $x^2 = (yx)^2$, it must be superfluous, and we have a presentation of the desired type.

$$\begin{aligned} G_6 &= \langle x, y, a \mid y^{2^{n-1}} = a = (yx)^2, x^2 = [x,a] = [y,a] = a^2 = 1 \rangle \\ &= \langle x, y \mid y^{2^n} = x^2 = 1, (yx)^2 = y^{2^{n-1}}, [x, y^{2^{n-1}}] = 1 \rangle. \end{aligned}$$

First note that the relation $[x, y^{2^{n-1}}] = 1$ can be deduced from the other three, and then that the resulting presentation is shown in [11] to yield the group

$$\langle x, y \mid y^{2^n} = x^2, x^{-1} y^{2^{n-2}-1} x = y^{2^{n-2}+1} \rangle.$$

4. **Groups of order** p^3. There is only one case outstanding, namely that of the group of order p^3 (p odd) given by

$$G = \langle x, y \mid x^p = y^p = [x,y]^p = [[x,y],x] = [[x,y],y] = 1\rangle,$$

(the others being treated above or in [11]), for which $r(G) = 4$, (see [6]). It is easily seen that the relation $[x,y]^p = 1$ follows from the other four, so that G is in $\mathbf{G}_p$ as required.

Note that there can be at most two groups of order 16 outside $\mathbf{G}_2$, by the results of sections 2 and 3 (and also [11]); we hope to consider groups of orders p^4 and p^5 in a future article.

4. **Wreath products.** Let G and H be p-groups and consider the extension (split by s)

$$1 \to \underbrace{G \times G \times \cdots \times G}_{h\,=\,|H|\text{ copies}} \xrightarrow{i} G \wr H \overset{s}{\leftrightarrows} H \to 1,$$

and regard G and H as subgroups of the standard wreath product $G \wr H$ via the embeddings $g \mapsto (g,1,\cdots,1)i$ and $h \mapsto hs$ respectively. Then it is not difficult to show (see [5]) that if $G = \langle x \mid R\rangle$ and $H = \langle Y \mid S\rangle$ then

$$G \wr H = \langle X, Y \mid R, S, [X, X^A]\rangle \tag{5}$$

where A is any subset of H having the property that $H \setminus \{1\} = A \cup A^{-1}$. Now if p is odd, we can find such an A with $|A| = \frac{1}{2}(h-1)$, and it is proved in [5] that if

$$|X| = d(G),\ |R| = r(G),\ |Y| = d(H) = |S|,$$

then $r(G \wr H) = r(G) + r(H) + \frac{1}{2}(h-1)d(G)^2$, precisely the number of relations in (5) in this case, (of course, $d(G \wr H) = d(G) + d(H)$ in general). Thus we can assert that, for odd p, the class $\mathbf{G}_p$ contains the standard wreath product of two of its members, provided that the second factor has trivial multiplicator. (Note that this result is improved in [19], where it is shown that each $\mathbf{G}_p$ is closed under general wreath products; however, the presentation is too complicated to give here).

For example, denote by G_n the Sylow p-subgroup of the symmetric group on p^n letters, $n \geqq 1$, $G_0 = \{1\}$. Then for all $n \geqq 1$, $G_n \cong G_{n-1} \wr Z_p$, and we deduce from the above remarks that (for odd p):

$$d(G_n) = n,\ r(G_n) = r'(G_n) = n + \frac{1}{12}(p-1)(n-1)n(2n-1),\ n \geqq 1,$$

which agrees with a result of Bogačenko [1]. Since the Sylow p-subgroup of an arbitrary symmetric group is just a direct product of various G_n's, we can assert that for odd p $\mathbf{G}_p$ contains the Sylow p-subgroup of any finite symmetric group.

6. **Extensions of abelian groups by cyclic groups.** Let H be a cyclic group and K an abelian group and G an extension of K by H:

$$1 \to H \to G \to K \to 1.$$

Then we say the extension is outer if $d(G) = d(K) + d(H)$. In this case G has a presentation

$$G = \langle x, a_1, \cdots, a_n \mid x^{\alpha},\ a_i^{\beta_i}x^{-\gamma_i},\ a_ixa_i^{-1}x^{-\delta_i},\ a_ja_ia_j^{-1}a_i^{-1}x^{-\lambda_{ji}} \rangle,$$

where $1 \leqq i < j \leqq n$ and γ_i, $\delta_i - 1$, β_i, α and λ_{ji} are zero modulo p; then it can be shown (for example, by the methods in [15]) that

$$r(G) = \frac{n^2 + 3n}{2} + e,$$

where $e = 0$ if p divides each of the following:

(1) $(\delta_1^{\beta_i} - 1)/\alpha, \quad 1 \leqq i \leqq n,$

(2) $\gamma_i(\delta_i - 1)/\alpha, \quad 1 \leqq i \leqq n,$

(3) $\{\lambda_{ji}(\delta_j^{\beta_j} - 1)/(\delta_j - 1) + \gamma_j(\delta_i - 1)\}/\alpha, \quad 1 \leqq i < j \leqq n,$

(4) $\{\lambda_{ji}(\delta_i^{\beta_i} - 1)/(\delta_i - 1) + \gamma_i(1 - \delta_j)\}/\alpha, \quad 1 \leqq i < j \leqq n,$

(5) $\{\lambda_{ki}(1 - \delta_j) + \lambda_{ji}(\delta_k - 1) + \lambda_{kj}(\delta_i - 1)\}/\alpha, \quad 1 \leqq i < j < k \leqq n,$

and $e = 1$ otherwise. As a consequence, we deduce the following

THEOREM. *If every outer extension of an abelian group K by a cyclic group H with $d(K) \leqq 3$ belongs to $\mathbf{G}_p$, then every outer extension of an abelian group by a cyclic group belongs to $\mathbf{G}_p$.*

PROOF. Assume $n > 3$. If $e = 1$, there is nothing to prove. In the case $e = 0$, there is a triple i, j, k such that the subgroup J generated by x, a_i, a_j, a_k has $r(J) = 9$, and if $J \in \mathbf{G}_p$ then this presentation can be extended to a presentation of G with $(n^2 + 3n)/2$ relations.

The case $n = 1$ is dealt with in [17], where it is shown that every outer extension of a cyclic group by a cyclic group belongs to $\mathbf{G}_p$; for the cohomology of these groups, see [4], [15].

7. **Examples of groups which may not belong to $\mathbf{G}_p$.** Let G be a three-generator, three-relation group with $d(G/G') = 3$. For example, let G be the Mennicke group

$$G = \langle x, y, z \mid [x, y] = x^p,\ [y, z] = y^p,\ [z, x] = z^p \rangle,$$

and let G^p stand for the maximum p-factor group of G; in our example,

$$G^p = \langle x, y, z \mid [x, y] = x^p\ [y, z] = y^p, [z, x] = z^p, x^{p^2}y^{p^2}z^{p^2} = 1 \rangle .$$

Then G^p has trivial multiplicator for $p > 3$, while there are no 'known' three-generator, three-relation p-groups for $p > 3$, and so one arrives at an example of a p-group which may or may not belong to G_p. (Note that [18] shows that G^p has three relations modulo R', where $G = F/R$, but as yet we have not been able to determine these either).

REFERENCES

1. I. V. Bogačenko, *On the structure of the cohomology ring of the Sylow subgroup of a symmetric group*, Izv. Akad. Nauk. SSSR, Ser. Mat. **27** (1963), 937–942.

2. E. S. Golod and I. R. Šafarevič, *On the class field tower*, Izv. Akad. Nauk. SSSR, Ser. Mat. **28** (1964), 261–272.

3. K. W. Gruenberg, *Some cohomological topics in group theory*, Queen Mary College Mathematics Notes, London (1967).

4. A. I. Kostrikin and I. R. Šafarevič, *Homology groups of nilpotent algebras*, Dokl. Akad. Nauk. SSSR **115** (1957), 1066-1069.

5. D. L. Johnson, *Minimal relations for certain wreath products*, to appear in Canad. J. Math.

6. G. Lewis, *The integral cohomology rings of groups of order p^3*, Trans. Amer. Math. Soc. **132** (1968), 501–529.

7. R. C. Lyndon, *The cohomology theory of group extensions*, Duke Math. J. **15** (1948), 271-292.

8. I. D. Macdonald, *On a class of finitely presented groups*, Canad. J. Math. **14** (1962), 602–613.

9. J. Mennicke, *Einige endliche Gruppen mit drei Erzeugenden und drei Relationen*, Arch. Math. **10** (1959), 409–418.

10. H. J. Munkholm, *Mod 2 cohomology of $D2^n$ and its extensions by Z_2*, Preprint series no. 6 (1968/69), Mathematisk Institute, Aarhus.

11. B. H. Neumann, *On some finite groups with trivial multiplicator*, Publ. Math. Debrecen **4** (1955), 190-194.

12. I. R. Šafarevič, *Algebraic number fields*, Proc. Int. Cong. of Math., Stockholm (1962), 163–175.

13. I. Schur, *Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.

14. R. G. Swan, *Minimal resolutions for finite groups*, Topology **4** (1965), 193–208.

15. C. T. C. Wall, *Resolutions for extensions of groups*, Proc. Cambridge Philos. Soc. **57** (1961), 221–225.

16. J. W. Wamsley, *A class of three-generator, three-relation groups*, to appear in Canad. J. Math.

17. J. W. Wamsley, *The deficiency of metacyclic groups*, to appear in Proc. Amer. Math. Soc.

18. J. W. Wamsley, *The multiplicators of finite nilpotent groups*, to appear in Bull. Austral. Math. Soc.

19. J. W. Wamsley, *The deficiency of wreath products of groups*, to appear in Canad. J. Math.

20. H. J. Zassenhaus, *A presentation of the groups PSL(2,p) with three defining relations*, Canad. J. Math. **21** (1969), 310-311.

UNIVERSITY OF NOTTINGHAM, ENGLAND
FLINDERS UNIVERSITY, AUSTRALIA.