MINIMAL PRESENTATIONS FOR CERTAIN GROUP EXTENSIONS

BY

J. W. WAMSLEY

ABSTRACT

If G is a finite group then $d(G)$ denotes the minimal number of generators of G. If H and K are groups then the extension, $1 \to H \to G \to K \to 1$, is called an outer extension of K by H if $d(G) = d(H) + d(K)$. Let $\mathscr{G}_p$ be the class of groups containing all finite p-groups G which 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 it is shown that if K is a non cyclic group belonging to $\mathscr{G}_p$ and H is a finite abelian p-group then any outer extension of K by H belongs to $\mathscr{G}_p$.

1. Introduction. Let G be a group, then $d(G)$ denotes the minimal number of generators of G. Define a class of finite p-groups, $\mathscr{G}_p$, as follows; G belongs to $\mathscr{G}_p$ if G is a finite p-group and G has a presentation

$$G = F/R = \{x_1, \cdots, x_n \mid R_1, \cdots, R_m\},$$

where F is free on generators $x_1, \cdots, x_n$ with $n = d(G)$ and R is the normal closure in F of $R_1, \cdots, R_m$ with $m = d(R/[F,R]R^p)$.

G is an extension of K by H if H is a normal subgroup of G and G/H is isomorphic to K. G is an outer extension of K by H if G is an extension of K by H and $d(G) = d(H) + d(K)$.

In this paper it is shown that if K is a non cyclic group belonging to $\mathscr{G}_p$ and H is a finite abelian p-group then any outer extension of K by H belongs to $\mathscr{G}_p$.

2 Basic theorems

THEOREM 2.1. *Let G be a finite p-group with presentation $G = F/R$ with $d(F) = d(G)$ and suppose $d(R/[F,R]R^p) = m$.*

If we take any set of m elements $R_1, \cdots, R_m$, of R, linearly independent in R modulo $[F,R]R^p$ and let $K = F/S$, where S is the normal closure of $R_1, \cdots, R_m$

Received September 15, 1970 and in revised form November 15, 1970

in F, then G is the maximal p-factor group of K, in the sense that if A is a finite p-group which is a factor group of K then A is a factor group of G.

PROOF. Any finite p-factor of K with class k and exponent $q = p^{\alpha}$ is a factor of

$$(F/S)/\{\Gamma_k(F)F^qS/S\} \cong F/\{\Gamma_k(F)F^qS\}$$

where $\Gamma_k(F)$ is the kth term of the lower central series of F. Therefore it will suffice to show that

$$R \subseteq \Gamma_k(F)F^qS.$$

Let $U = [F,R]$ and T the normal closure of $\{r^q \mid r \in R\} = R^q$, then $G = F/STU$ since $STU = R$.
We have $U \subseteq [R,F] = [STU,F] \subseteq [U,F]ST \subseteq [U,F,F]ST$ etc.
whence

$$U \subseteq \Gamma_k(F)ST \quad \text{for all } k,$$

however

$$T \subseteq F_q \text{ yielding}$$

$$UST = R \subseteq \Gamma_k(F)F^qS. \qquad //$$

COROLLARY 2.2. *Let* $N = \{x_1, \cdots, x_n \mid R_{i_1}, \cdots, R_{i_t}\}$ *where* $R_{i_1}, \cdots, R_{i_t}$ *is a subset of* $R_1, \cdots, R_m$. *If* N *is a finite* p*-group then* G *belongs to* $\mathscr{G}_p$.

PROOF. $K = \{x_1, \cdots, x_n \mid R_1, \cdots, R_m\}$ is a finite p-group and hence by the theorem $K = G$. //

LEMMA 23.. *Let* $G = \{x_1, \cdots, x_n \mid R_1, \cdots, R_m\} = F/R$ *and*

$$G/N = \{x_1, \cdots, x_n \mid R_1, \cdots, R_m, S_1, \cdots, S_t\} = F/S$$

then if $R_{i_1}, \cdots, R_{i_u}$ *are linearly independent in* S *modulo* $[F,S]S^p$ *they are linearly independent in* R *modulo* $[F,R]R^p$.

PROOF. The natural mapping $R/[F,R]R^p$ into $S/[F,S]S^p$ is a homomorphism and hence a linear transformation of the respective vector spaces. //

The following theorem is well known and is stated without proof. (see for example [1]).

THEOREM 2.4. *Let* H *and* K *belong to* $\mathscr{G}_p$, *then the direct product of* H *and* K *belongs to* $\mathscr{G}_p$ *with minimal presentation.*

$$H \times K = \{x_1, \cdots, x_n, y_1, \cdots, y_m \mid R_1, \cdots, R_u, \ S_1, \cdots S_v, x_i y_j x_i^{-1} y_j^{-1}\}$$

where

$$H = \{x_1, \cdots, x_n \mid R_1, \cdots, R_u\} \quad and$$

$$K = \{y_1, \cdots, y_m \mid S_1, \cdots, S_v\}$$

are minimal presentations for H and K respectively. //

3. The main theorem

Let G be a split extension of K by H where H is an abelian p-group and K is a non cyclic group belonging to $\mathscr{G}_p$. *Then G has a presentation*

$$G = \{a_1, \cdots, a_n, x_1, \cdots, x_s \mid A, R, X_1, \cdots, X_s\} \ where$$

$$H = \{a_1, \cdots, a_n \mid A\} \ and$$

$$K = \{x_1, \cdots, x_s \mid R\} \ are \ presentations \ for \ H \ and \ K$$

respectively and X_i, $i = 1, \cdots, s$ *is the set of conjugacy relations of* x_i *on* a_j, $j = 1, \cdots, n$.

We may denote the n relations X_i as an $n \times n$ matrix as follows.

If $x_i a_j x_i^{-1} = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ then the jth column of X_i is the vector $(\alpha_1, \cdots, \alpha_n)$. Also if the exponent of H is P^r we may replace X_i with

$$X_i' = X_i + P^r K$$

where K is any $n \times n$ integer matrix. Conversely if $X_1, \cdots, X_s$ is any set of $n \times n$ matrices with integer entries then there exists a maximal abelian group H such that in the split extension of K by H the X_i give the conjugacy relations. If in this case H is necessarily a finite p-group we say that X_i is a p-representation of K.

LEMMA 3.1. *Let X and Y be* $n \times n$ *matrices with integer entries and* α, β, γ *powers of a prime number p. Then there exists matrices* K_1 *and* K_2 *with integer entries such that*

(i) $u = |(X + \alpha K_1)^\beta - I_n| \neq 0$,

(ii) $v = |(Y + \alpha K_2)^\gamma - I_n| \neq 0$ *and*

(iii) *the only prime dividing both u and v is p.*

PROOF. To prove (i) we consider the polynomial in z of degree $n\beta$

$$|(X + \alpha z I_n)^\beta - I_n|.$$

Let w be any integer not a root of the given polynomial and let $K_1 = wI_n$. Next let $q_1, \cdots, q_t$ be the primes different from p which divide u, then we need only show we can choose a K_2 such that $v \not\equiv 0$ modulo q_i for $i = 1, \cdots, t$ whence (ii) and (iii) follow.

We use induction on t.

Suppose $|(Y + \alpha K)^\gamma - I_n| \equiv 0$ modulo q_1 for all K then since α is a unit modulo q_1 we have.

$|Z^\gamma - I_n| \equiv 0$ modulo q_1 for all Z. In particular in the case of Z being of the form sI_n we have

$\omega^\gamma \equiv 1$ modulo q_1 for all integers ω which certainly gives a contradiction.

Assume $|(Y + \alpha K)^\gamma - I_n| \not\equiv 0$ modulo q_i, $i = 1, \cdots, j-1$.

Then as before suppose

$$|(Y + \alpha K + \alpha q_1 q_2 \cdots q_{j-1} H)^\gamma - I_n| \equiv 0$$

modulo q_j for all H, then we get a contradiction. //

LEMMA 3.2. *Let G be a split extension of a non cyclic group, K, belonging to $\mathcal{G}_p$ by an abelian p-group, H, then we may choose the conjugacy relations X_i such that they are a p-representation of K.*

PROOF. Let x and y be any two of the generators of K occuring in a minimal presentation of K, and let X and Y be the corresponding matrices of conjugation. Further let H be of exponent P^r and P^α, P^β the orders of x and y respectively.

Replace X and Y with

$$X_1 = X + P^r K_1 \text{ and}$$

$$Y_1 = Y + P^r K_2 \text{ such that}$$

$u = |X_1^{p^\alpha} - I_n| \neq 0$,

$v = |Y_1^{p^\beta} - I_n| \neq 0$ and the only prime dividing both u and v is p.

Then the set of relations given by $X_1 = I_n^{p^\alpha}$ and $Y_1 = I_n^{p^\beta}$ imply that H must be a finite p-group. //

THEOREM 3.3. *Let K be any non cyclic group belonging to $\mathcal{G}_p$ and H a finite abelian p-group. Then any outer extension, G, of K by H belongs to $\mathcal{G}_p$.*

PROOF. Let K and H have presentations

$K = \{x_1, \cdots, x_s \mid S\}$ and

$H = \{a_1, \cdots, a_n \mid A\}$ respectively, then G has a presentation

$G = \{a_1, \cdots, a_n \mid x_1, \cdots, x_s \mid A, S, X\}$ where X is the set of conjugacy relations each of the form

$$x_i a_j x_i^{-1} = a_1^{\alpha_n} \cdots a_n\ , \text{ with } \alpha_k \text{ depending on } i \text{ and } j.$$

Since the extension is outer then $\alpha_k \equiv 0$ modulo p for $k \neq j$, otherwise a_k could be deleted from the generating set, whence modulo $H^p = \{b^p \mid b \in H\}$ the conjugacy relations reduce to relations of the form

$$x_i a_j x_i^{-1} = a_j^{\alpha_j} \text{ whence } \alpha_j = 1 \text{ modulo } p.$$

With $N = H^p$ in Lemma 2.3 the conjugacy relations which reduce to commuting relations in G/N together with the commuting relations of H and the defining relations of K are linearly independent modulo $[F, R]R^p$ where $G = F/R$.

However by Lemma 3.2 we may choose these relations such that they define a finite p-group and hence by Corollary 2.2 belongs to $\mathscr{G}_p$. //

The case with K cyclic appears more difficult since the different types need different proofs. However the theorem still appears to hold. For example for p odd let

$$G = \{a, b, c \mid ab = ba,\ a^{p^2} = b^{p^2} = c^p = 1,\ cac^{-1} = a^{1+p},\ cbc^{-1} = b^{1+p}\}.$$

Then it can be shown for example by the methods in [2] that $\dim H^2(G, Z_p) = 4$. Hence if G belongs to $\mathscr{G}_p$, G should have 4 defining relations and in fact it has. We have

$$G = \{a, b, c \mid c^p = a^{p^2},\ cac^{-1} = a^{1+p},\ cbc^{-1} = b^{1+p},\ a^{-1}ba = b^{1+kp^2}\}$$

where k is chosen such that the greatest common divisor of $(1+p)^p - 1$ and $(1+kp^2)^{p^2} - 1$ is p^2 which can be done as in Lemma 3.1.

References

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

2. C. T. C. Wall, *Resolutions for extensions of groups*, Proc. Cambridge Philos. Soc. **57** (1961), 251–255.

School of Mathematical Sciences
The Flinders University of South Australia