MINIMAL PRESENTATIONS FOR CERTAIN METABELIAN GROUPS

D. G. SEARBY AND J. W. WAMSLEY

Abstract. Let $G$ be a finite $p$-group, $d(G) = \dim H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $r(G) = \dim H^2(G, \mathbb{Z}/p\mathbb{Z})$. Then $d(G)$ is the minimal number of generators of $G$, and we say that $G$ is a member of a class $\mathscr{C}_p$ of finite $p$-groups if $G$ has a presentation with $d(G)$ generators and $r(G)$ relations. The main result is that any outer extension of a finite cyclic $p$-group by a finite abelian $p$-group belongs to $\mathscr{C}_p$.

1. Introduction. Let $G$ be a finite $p$-group. We have

$$d(G) = \dim H^1(G, \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{Z}_p} (G|G'^p),$$
$$r(G) = \dim H^2(G, \mathbb{Z}/p\mathbb{Z}),$$

d($G$) being the minimal number of generators of $G$. If there is a presentation

$$G = F/R = \langle x_1, \ldots, x_n \mid R_1, \ldots, R_m \rangle$$

where $F$ is the free group on $x_1, \ldots, x_n; n = d(G)$, and $R$ is the normal closure in $F$ of $R_1, \ldots, R_m$, we have always $m \geq r(G) = d(R/[F, R]R^p)$ (see, for example [2]). We say that $G$ belongs to a class $\mathscr{C}_p$ of finite $p$-groups if there is such a presentation with $n = d(G)$ and $m = r(G)$. Such a presentation is said to be minimal.

$G$ is said to be an extension of a group $K$ by $H$ if $H$ is a normal subgroup of $G$, and $G/H \cong K$. $G$ is said to be an outer extension of $K$ by $H$ if $G$ is an extension of $K$ by $H$, and $d(G) = d(K) + d(H)$.

In this paper it is shown that if $K$ is a finite cyclic $p$-group, and $H$ is a finite abelian $p$-group, then any outer extension of $K$ by $H$ belongs to $\mathscr{C}_p$. The case $n=1$ has been covered in [2].

2. Basic lemmas.

Lemma 1. Let $G$ be a finite $p$-group with presentation $G = F/R$ where $d(G) = d(F)$, and let $d(R/[F, R]R^p) = m$. If $R_1, \ldots, R_m$ is any set of $m$ elements of $R$, linearly independent in $R$ modulo $[F, R]R^p$, and $K = F/S$ where $S$ is the normal closure of $R_1, \ldots, R_m$ in $F$; then $G$ is the maximal...
$p$-factor group of $K$ in the sense that if $A$ is any finite $p$-group which is a factor group of $K$, then $A$ is a factor group of $G$.

**Proof.** Let $\Gamma_k(F)$ be the $k$th term of the lower central series of $F$. Any $p$-factor group of $K=FS$ with class $k$ and exponent $q=p^k$ will necessarily be a factor group of

$$K/(\Gamma_k(F)F^s) \cong (F/S)/(\Gamma_k(F)F^sS/S) \cong F/(\Gamma_k(F)F^sS).$$

Thus it will suffice to show that

$$R \subseteq \Gamma_k(F)F^sS$$

since if so then $F/(\Gamma_k(F)F^sS)$ is a factor group of $F/R=G$, and any $p$-factor of $F/S$ will hence be a factor of $G$.

Let $U=[F,R]$ and let $T$ be the normal closure of $R^s$ in $F$; then $STU=R$ and $U=[R,F]=[STU,F] \subseteq [U,F]ST \subseteq [U,F,F]ST \subseteq \cdots$ so that $U \subseteq \Gamma_k(F)ST$ for all $k$. Now $T \subseteq F^s$ so that $UST=R \subseteq \Gamma_k(F)F^sS$ which establishes (1), and hence the lemma.

**Corollary.** Let $N=\{x_1, \ldots , x_n|R_1, \ldots , R_t\}$ where $R_1, \ldots , R_t$ is any subset of $R_1, \ldots , R_m$. If $N$ is a finite $p$-group, then $G \in \mathcal{G}_p$.

**Proof.** Let $H=\{x_1, \ldots , x_n|R_1, \ldots , R_m\}$, then $H$ is a factor of $N$, so $H$ is a finite $p$-group, and by the lemma, $H=G$.

**Lemma 2.** Let $G=F/R=\{x_1, \ldots , x_n|R_1, \ldots , R_m\}$ and $G/N=\{x_1, \ldots , x_n|R_1, \ldots , R_m, S_1, \ldots , S_t\}=F/S$. Then if $R_{i_1}, \ldots , R_{i_s}$ 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 of $R/([F,R]R^p)$ into $S/([F,S]S^p)$ is clearly a homomorphism, and hence a linear transformation of the respective vector spaces.

**Theorem 1.** Let $K=\{x_1, \ldots , x_n|R_1, \ldots , R_m\}$ be a finite $p$-group, then $G=\{x_1, \ldots , x_n|R_1, \ldots , R_m, S_1, \ldots , S_t\}$ belongs to $\mathcal{G}_p$ if

$$H=\{x_1, \ldots , x_n|R_1, \ldots , R_m, S_1, \ldots , S_t, T_1, \ldots , T_n\}$$

has a minimal presentation $H=\{x_1, \ldots , x_n|R_1, \ldots , R_m, U_1, \ldots , U_v\}$ for suitable $U_i$.

**Proof.** By Lemma 2, $R_1, \ldots , R_m$ are linearly independent, and by Lemma 1 and the Corollary, $G \in \mathcal{G}_p$.

The following well-known theorem, which is stated without proof, is due to D. Epstein [1].

**Theorem 2.** If $G$ is a finite abelian $p$-group with $d(G)=n$, then $G$ has a minimal presentation with $n$ generators and $\frac{1}{2}n(n+1)$ relations.
Let $A$ be a finite abelian $p$-group generated by $\{a_1, \ldots, a_n\}$, and let $G = \langle a_1, \ldots, a_n, x | R_1, \ldots, R_m \rangle$ be any outer extension of a finite cyclic $p$-group by $A$. Then if $\phi(G)$ denotes the Frattini subgroup of $G$, since the extension is outer, $\phi(G) \cap A = \phi(A)$. If amongst the defining relations of $G$ there occurs

$$xa_i x^{-1} = a_i^{a_{ii}} \cdots a_i^{a_{it}}$$

i.e. $xa_i x^{-1} a_i^{-1} = a_i^{a_{ii}} \cdots a_i^{a_{it}t-1} \cdots a_i^{a_{it}}$, then since $xa_i x^{-1} a_i^{-1} \in \phi(G)$,

$$a_i^{a_{ii}} \cdots a_i^{a_{it}t-1} \cdots a_i^{a_{it}} \in \phi(A) = A^p,$$

and thus $a_{ij} \equiv 0 \pmod{p}$ if $i \neq j$, and $a_{ii} \equiv 1 \pmod{p}$.

**Lemma 3.** Let

$$G = \langle a_1, \ldots, a_n, x | a_i^{m_i}, x^{-k} a_i^{a_{ii}} \cdots a_i^{a_{it}}, xa_i x^{-1} a_i^{a_{ii}} \cdots a_i^{a_{it}} \rangle$$

$(i = 1, \ldots, n); [a_i, a_j] (i > j)$,

where $m_i = p^{\delta_i}$, $k = p^\lambda$, $\lambda_i = k_i p^{\rho_i}$, $k_i \neq 0 \pmod{p}$, $a_{ij} \equiv 0 \pmod{p}$ if $i \neq j$, $a_{ii} \equiv 1 \pmod{p}$, be an outer extension of a finite cyclic $p$-group by a finite abelian $p$-group, for which $\{a_1, \ldots, a_n, x\}$ is a minimal generating set. Then $G$ has a presentation

$$G = \langle b_1, \ldots, b_n, x | b_i^{m_i}w_i(p) (i < n), b_i^{m_i}, x^{-b_i^{t+1}} \rangle$$

$$xb_i x^{-1} b_i^{t+1} \cdots b_i^{t+1} (i < n), xb_i x^{-1} b_i^{t+1} \cdots b_i^{t+1} \rangle$$

$[b_i, b_j] (i > j, (i, j) \neq (n, 1)), b_i^{t+1} b_i^{-1} b_i^{m_n} b_i$,

where $m_i = p^{\delta_i}$, $w_i (p) \in \langle b_i^{t+1}, \ldots, b_i^{t+1} \rangle$, $k = p^\lambda$, $\pi_i = p^{\tau_i}$, $\pi_i = p^{\tau_i} (i > 1)$, $\{v_{ij}\}$ is some set of integers satisfying $v_{ij} \equiv 0 \pmod{p}$ if $i \neq j$, $v_{ii} \equiv 1 \pmod{p}$, $p^\mu$ is the exponent of $G$.

**Proof.** We may suppose $\delta_i \leq \delta_i$ for all $i$; set $\lambda_i = k_i p^{\rho_i - \delta_i}$ and $\pi_i = p^{\tau_i}$. Then $x^k = a_i^{a_{ii}} \cdots a_i^{a_{it}} \in (a_i^{a_{ii}} \cdots a_i^{a_{it}})^{v_{ij}} = b_i^{t+1}$. As $a_i^{a_{ii}} \not\equiv 0 \pmod{p}$, $\{b_1, a_2, \ldots, a_n, x\}$ is a generating set, $b_i^{t+1} \in \langle a_i^{a_{ii}} \cdots a_i^{a_{it}} \rangle$ and $[b_i, a_j] = 1$ for all $i$.

Now, let $i < n$, and suppose the required changes have been made for all $j \leq i$. Then

$$xb_i x^{-1} = b_i^{t+1} \cdots b_i^{t+1} (a_i^{a_{ii}} \cdots a_i^{a_{it}})^{v_{ii}} = b_i^{t+1} \cdots b_i^{t+1} (a_i^{a_{ii}} \cdots a_i^{a_{it}})^{v_{ii}}$$

as in the first step, where $a_i^{a_{ii}} \not\equiv 0 \pmod{p}$, $\pi_i = p^{\tau_i}$. Let $b_{i+1}$ be the term inside the brackets. Then $\{b_1, \ldots, b_{i+1}, a_{i+2}, \ldots, a_n, x\}$ is a generating set, $b_i^{m_n} \equiv (a_i^{a_{ii}} \cdots a_i^{a_{it}}) (i < n-1$, otherwise $b_i^{m_n} = 1), xb_i x^{-1} = b_i^{t+1} \cdots b_i^{t+1} (a_i^{a_{ii}} \cdots a_i^{a_{it}}) b_i^{t+1}, [b_{i+1}, a_j] = 1$ for all $j$, and all the congruences on the $\{v_{ij}\}$ hold, since the change of generators does not change the Frattini subgroup, and the remarks immediately preceding this lemma still apply.
Thus by induction we construct $b_1, \ldots, b_n$ satisfying the required relations. The process terminates at $b_n$, and we still have $xb_nx^{-1} = b_n^m \cdots b_n^{m_1}$. At this step we may go through the argument again, replacing each occurrence of $\langle a_1^p, \ldots, a_n^p \rangle$ by $\langle b_1^p, \ldots, b_n^p \rangle$. Clearly the order of each $b_j$ is a power of $p$, because $b_j^m \in \langle b_{j+1}^p, \ldots, b_n^p \rangle$, $b_{j+1}^m \in \langle b_{j+2}^p, \ldots, b_n^p \rangle$, \ldots etc., and $b_n^m = 1$, each $m_i$ being a power of $p$. Also, if the exponent of $G$ is $p^s$, we may replace the defining relation $[b_n, b_1] = 1$ by $b_n b_1 = b_n^{m_1} b_1$, where $m = 1 + \lambda p^s$ for some positive integer $\lambda$. This completes the proof.

Note. In the above proof, $v_{ij}$ may be replaced by $v_{ij} + sp^n$ for some integer $s$, and for all $i$ and $j$.

**Lemma 4.** Let $A(t), B(t)$ and $C(t)$ be rational polynomials in $t$, $\mu$ a fixed nonzero integer, and $K$ and $L$ infinite sets of integers. Then it is possible to choose integers $k \in K$ and $\lambda \in L$ such that the polynomials $A(t)$ and $D(t) = \kappa B(t) + \lambda C(t) + \mu$ are coprime.

**Proof.** Let $A(t)$ be factorized over the rationals into irreducible factors $A_1(t), \ldots, A_r(t)$. For each $i$, $1 \leq i \leq r$, there are four possibilities:

(i) $A_i(t) | B(t)$ and $A_i(t) | C(t)$—then $A_i(t) | D(t)$ for all $\kappa$ and $\lambda$.

(ii) $A_i(t) | B(t)$ and $A_i(t) | C(t)$—then there is at most one $\lambda$ such that $A_i(t) | D(t)$, since if $k_1$ and $k_2$ have this property:

\[ A_i(t) | \kappa_1 B(t) + \lambda_1 C(t) + \mu \quad \text{and} \quad A_i(t) | \kappa_2 B(t) + \lambda_2 C(t) + \mu, \]

hence $A_i(t) | (\kappa_1 - \kappa_2)B(t) + (\lambda_1 - \lambda_2)C(t)$ which is impossible unless $\lambda_1 = \lambda_2$.

(iii) $A_i(t) | B(t)$ and $A_i(t) | C(t)$—then there is at most one $\kappa$ such that $A_i(t) | D(t)$—the proof is as for (ii).

(iv) $A_i(t) | B(t)$ and $A_i(t) | C(t)$—then for each $\kappa \in K$, there is at most one $\lambda \in L$ for which $A_i(t) | D(t)$ and conversely, since if, for $\kappa \in K$ and $\lambda_1$ and $\lambda_2 \in L$,

\[ A_i(t) | \kappa B(t) + \lambda_1 C(t) + \mu \quad \text{and} \quad A_i(t) | \kappa B(t) + \lambda_2 C(t) + \mu, \]

then $A_i(t) | (\lambda_1 - \lambda_2)C(t)$, which is impossible unless $\lambda_1 = \lambda_2$. Similarly for the converse.

Now, define $K_1 \subset K$ by $\kappa \in K_1$ iff for some $i$, case (iii) applies, and $\kappa \in K$ is the unique integer permitted by the argument, and define $L_1 \subset L$ similarly. As $K_1$ and $L_1$ are finite, $K' = K - K_1$ and $L' = L - L_1$ are infinite, and clearly if $\kappa \in K'$ and $\lambda \in L'$, $A_i(t) | D(t)$ if (i), (ii) or (iii) applies. Choose any $\kappa \in K'$ and define $L_2 \subset L'$ by $\lambda \in L_2$ iff for some $i$, case (iv) applies and $\lambda$ is the unique second member of the pair $(\kappa, \lambda)$ permitted by the argument. Then $L_2$ is finite, so $L'' = L' - L_2$ is infinite, and by the construction, if $\kappa \in K'$, $\lambda \in L''$, then

\[ A_i(t) | \kappa B(t) + \lambda C(t) + \mu \quad \text{for each} \quad i = 1, \ldots, r. \]

Hence $A(t)$ and $\kappa B(t) + \lambda C(t) + \mu$ are coprime.
Lemma 5. Let \( p, q_1, \ldots, q_r \) be distinct primes, then it is possible to find an integer \( k \) such that, for \( n > 0 \),
\[
(1 + kp^n)^n - 1 \not\equiv 0 \pmod{q_1, \ldots, q_r}.
\]

Proof. \( p^n \) is prime to \( q_1 \cdot \cdots \cdot q_r \), so by the division algorithm there exists an integer \( k \) such that \( kp^n \equiv -1 \pmod{q_1 \cdot \cdots \cdot q_r} \). Then
\[
(1 + kp^n)^n - 1 \equiv -1 \pmod{q_1 \cdot \cdots \cdot q_r}
\]
so
\[
(1 + kp^n)^n - 1 \equiv -1 \pmod{q_1, \ldots, q_r}.
\]

3. The main theorem.

Theorem 3. Let
\[
G = \{a_1, \ldots, a_n, x \mid a_i^{m_i}, x^{-k}a_1^{11} \cdots a_n^{11}, xa_i^{-1}x^{-1}a_i^{11} \cdots a_n^{11} (i = 1, \ldots, n); [a_i, a_j] (i > j)\}
\]
where \( m_i = p^{\beta_i}, k = p^\delta, \lambda_i = k, \mu_i \equiv 0 \pmod{p}, \alpha_{ij} \equiv 0 \pmod{p} \) if \( i \neq j \), \( \alpha_{ii} \equiv 1 \pmod{p} \), be any outer extension of a finite cyclic \( p \)-group by a finite abelian \( p \)-group for which \( d(G) = n + 1 \). Then \( G \in \mathcal{S}_p \).

Proof. By Lemma 3, \( G \) has a presentation
\[
G = \{b_1, \ldots, b_n, x \mid x^{-k}b_1^{11} \cdots b_n^{11}, x b_1^{11} \cdots x b_n^{11} [b_i, b_j] (i > j, (i, j) \neq (n, 1)), b_1^{-1} b_n^{-1} b_n^{11}, b_n^{11} \}
\]
where \( k = p^\delta, \tau_1 = p^{\beta_1}, \tau_i = p^{\alpha_i} (i > 1), v_{ij} \equiv 0 \pmod{p} \) if \( i \neq j \), \( v_{ii} \equiv 1 \pmod{p} \), \( m = 1 + \lambda p^n, m_i = p^{\tau_i}, m_i (p) \in \{b_1^{11}, \ldots, b_n^{11}\} \). We abbreviate this presentation to
\[
G = \{b_1, \ldots, b_n, x \mid R_1, \ldots, R_t, b_n^{11} w_1 (p) (i < n), b_n^{11}\}.
\]
With this notation we define
\[
K = \{b_1, \ldots, b_n, x \mid R_1, \ldots, R_t\},
\]
and
\[
H = \{b_1, \ldots, b_n, x \mid R_1, \ldots, R_t, b_n^{11} w_1 (p) (i < n), b_n^{11} b_j^7 (j = 1, \ldots, n)\}.
\]
Now \( H \) is an elementary abelian group, and by Theorem 2, has a minimal presentation with \( \frac{1}{2} (n + 1)(n + 2) \) relations—but \( t = 1 + n + C_n^2 = \frac{1}{2} (n + 1) \times (n + 2) - n \), so \( H \) has a minimal presentation
\[
H = \{b_1, \ldots, b_n, x \mid R_1, \ldots, R_t, b_j^7 (j = 1, \ldots, n)\},
\]
and \( H \in \mathcal{S}_p \). Thus \( R_1, \ldots, R_t \) are linearly independent, and to apply
Theorem 1 and thereby prove the theorem, it remains only to show that for a suitable choice of \( \nu_i \) and \( \lambda \), \( H \) is a \( p \)-group.

We have \( x^i=b_1^i \) so \( x b_1^{-i} x^{-1}=b_1^{-i} \), which implies \( b_i^{(v_{i-1}) x^{-1} x^{x_{i+1}}} b_1^{x_i}=1 \),

\[
x b_1^{x_i} x^{-1} = x b_1^{(1-v_{i-1}) x^{-1} x^{x_{i+1}}} b_1^{x_i} = b_2^{x_i},
\]

which implies \( b_1^{(v_{i-1}) x_{i+1} b_2^{x_i-1} x_{i+1}} b_1^{x_i}=1 \). We continue as in the last step for \( b_3, \ldots, b_{n-2} \), obtaining \( x b_2^{x_{n-2} x_{n-1} x^{-1}} b_2^{x_{n-2} x_{n-1}} = b_2^{x_{n-2} x_{n-1}} \) which implies

\[
b_1^{v_{n-2} x_{n-2} x_{n-1}} \ldots b_1^{(v_{n-2} x_{n-1}) x_{n-1}} b_2^{x_{n-2} x_{n-1}}=1.
\]

For \( b_{n-1} \) we recall that \( b_n b_1=b_1 b_n \) applies, and we derive

(i) \( b_1^{v_{n-1} x_{n-1}} b_2^{v_{n-2} x_{n-2} x_{n-1}} \ldots b_1^{v_{n-1} x_{n-1}} b_2^{x_{n-2} x_{n-1}}=1. \)

From this and the preceding equations, \( b_1^{x_i} \in \text{gp}(b_1) \), so \( b_1^{x_i} \in \text{gp}(b_1) = \text{gp}(x^i) \) so that \( x b_1^{x_i} x_{i+1} b_1^{x_i}=x_{i+1} b_1^{x_i} \), and

(ii) \( b_1^{v_{n-1} x_{n-1}} b_2^{v_{n-2} x_{n-2} x_{n-1}} \ldots b_1^{v_{n-1} x_{n-1}} b_2^{x_{n-2} x_{n-1}}=1. \)

where in (i) and (ii), \( S(m) \) and \( T(m) \) are polynomials in \( m \), which are independent of \( \nu_{n}, \nu_{n-1} \) and \( \nu_{n-1} \). From (i) and (ii) and earlier derivations, we may derive

\[
b_1^{x_{n-1}} b_2^{v_{n-2} x_{n-2} x_{n-1}} \ldots b_1^{v_{n-1} x_{n-1}} b_2^{x_{n-2} x_{n-1}}=1.
\]

where \( c_1 \) and \( c_2 \) are nonzero integers independent of \( \nu_{n} \). Thus

\[
b_1^{v_{n-1} x_{n-1}} b_2^{v_{n-2} x_{n-2} x_{n-1}} \ldots b_1^{v_{n-1} x_{n-1}} b_2^{x_{n-2} x_{n-1}}=1.
\]

By suitable choice of \( \nu_{n} \) we may ensure that

\[
c_3 = (\nu_{n} - 1) c_1 - c_2 
eq 0;
\]

then \( b_1^{\psi(m)}=1 \), where \( \psi(m)=(\nu_{n} - 1) c_1 - c_2 T(m)+c_2. \)

Also, from (i): \( b_n b_1 b_n^{-1}=b_1 \), so \( b_n^{x} b_1 b_n^{-x}=b_1^{x} \). If we put \( \sigma=p^{x_i} x_{i+1} \), then \( b_1^{x} \) is a power of \( b_1 \), so \( b_n^{x} b_1 b_n^{-x}=b_1 \), and we have

(iii) \( b_1^{m^x-1}=1, \quad b_1^{\psi(m)}=1, \)

so that \( |b_1| \) is the greatest common divisor of \( m^x-1 \) and \( \psi(m) \). Now \( S(m) \) and \( T(m) \) are independent of \( \nu_{n-1} \) and \( \nu_{n} \), so that by Lemma 4 we can choose these coefficients so that the polynomials have no common factor containing \( m \).

Now if two polynomials are coprime in this sense, the Euclidean algorithm shows that it is possible to find a linear combination of them which is an integer, say \( q_1 \cdots q_k p^n \) if \( |b_1| \) divides \( m^x-1 \) and \( \psi(m) \), then it must divide this number, whence, since \( m=1+\lambda p^n \), by Lemma 5 it is possible to choose \( \lambda \) such that \( m^x-1 \) is prime to \( q_1, \ldots, q_k \). From
this we deduce that $|b_1|$ is a power of $p$, and thus that the order of every generator is $p$-power.

Thus $K$ is a finite $p$-group, and by the earlier remarks, this is sufficient to complete the proof.

REFERENCES


SCHOOL OF MATHEMATICS, THE FLINDERS UNIVERSITY OF SOUTH AUSTRALIA, BEDFORD PARK, SOUTH AUSTRALIA