PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 32, Number 2, April 1972

# MINIMAL PRESENTATIONS FOR CERTAIN METABELIAN GROUPS

D. G. SEARBY AND J. W. WAMSLEY

ABSTRACT. Let $G$ be a finite $p$-group, $d(G)=\dim H^1(G, Z/pZ)$ and $r(G)=\dim H^2(G, Z/pZ)$. Then $d(G)$ is the minimal number of generators of $G$, and we say that $G$ is a member of a class $\mathcal{G}_p$ 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 $\mathcal{G}_p$.

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

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

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

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

where $F$ is the free group on $x_1, \cdots, x_n$; $n=d(G)$, and $R$ is the normal closure in $F$ of $R_1, \cdots, R_m$, we have always $m \geqq r(G)=d(R/[F, R]R^p)$ (see, for example [2]). We say that $G$ belongs to a class $\mathcal{G}_p$ 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 $G/H \simeq K$. $G$ 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 $\mathcal{G}_p$. 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 $R_1, \cdots, R_m$ 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 $R_1, \cdots, R_m$ in $F$; then $G$ is the maximal*

Received by the editors January 25, 1971.
*AMS* 1970 *subject classifications*. Primary 20D15, 20F05.
*Key words and phrases*. Presentation, outer extension, finite cyclic $p$-group, finite abelian $p$-group, Frattini subgroup.

*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 $K=F/S$ with class $k$ and exponent $q=p^\alpha$ will necessarily be a factor group of

$$K/(\Gamma_k(F)F^q) \cong (F/S)/(\Gamma_k(F)F^qS/S) \cong F/(\Gamma_k(F)F^qS).$$

Thus it will suffice to show that

$$R \subseteq \Gamma_k(F)F^qS \tag{1}$$

since if so then $F/(\Gamma_k(F)F^qS)$ 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 $R^q$ 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 $T\subseteq F^q$ so that $UST=R\subseteq \Gamma_k(F)F^qS$ which establishes (1), and hence the lemma.

COROLLARY. *Let $N=\{x_1, \cdots, x_n|R_{i_1}, \cdots, R_{i_t}\}$ where $R_{i_1}, \cdots, R_{i_t}$ is any subset of $R_1, \cdots, R_m$. If N is a finite p-group, then $G\in\mathcal{G}_p$.*

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

LEMMA 2. *Let $G=F/R=\{x_1, \cdots, x_n|R_1, \cdots, R_m\}$ and $G/N = \{x_1, \cdots, x_n|R_1, \cdots, R_m, S_1, \cdots, S_t\}=F/S$. Then if $R_{i_1}, \cdots, R_{i_s}$ 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 $K=\{x_1, \cdots, x_n|R_1, \cdots, R_m\}$ be a finite p-group, then $G=\{x_1, \cdots, x_n|R_1, \cdots, R_m, S_1, \cdots, S_t\}$ belongs to $\mathcal{G}_p$ if*

$$H = \{x_1, \cdots, x_n \mid R_1, \cdots, R_m, S_1, \cdots, S_t, T_1, \cdots, T_n\}$$

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

PROOF. By Lemma 2, $R_1, \cdots, R_m$ 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 $\{a_1, \cdots, a_n\}$, and let $G=\{a_1, \cdots, a_n, x | R_1, \cdots, R_m\}$ 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

$$xa_ix^{-1} = a_1^{\alpha_{i1}} \cdots a_i^{\alpha_{ii}} \cdots a_n^{\alpha_{in}}$$

i.e. $xa_ix^{-1}a_i^{-1} = a_1^{\alpha_{i1}} \cdots a_i^{\alpha_{ii}-1} \cdots a_n^{\alpha_{in}}$, then since $xa_ix^{-1}a_i^{-1} \in \phi(G)$,

$$a_1^{\alpha_{i1}} \cdots a_i^{\alpha_{ii}-1} \cdots a_n^{\alpha_{in}} \in \phi(A) = A^p,$$

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

LEMMA 3. *Let*

$$G = \{a_1, \cdots, a_n, x \mid a_i^{m_i}, x^{-k}a_1^{\lambda_1} \cdots a_n^{\lambda_n}, xa_i^{-1}x^{-1}a_1^{\alpha_{i1}} \cdots a_n^{\alpha_{in}} \\ (i = 1, \cdots, n); [a_i, a_j] (i > j)\},$$

*where* $m_i = p^{\beta_i}$, $k = p^{\delta}$, $\lambda_i = k_ip^{\delta_i}$, $k_i \not\equiv 0 \pmod p$, $\alpha_{ij} \equiv 0 \pmod p$ *if* $i \neq j$, $\alpha_{ii} \equiv 1 \pmod p$, *be an outer extension of a finite cyclic p-group by a finite abelian p-group, for which* $\{a_1, \cdots, a_n, x\}$ *is a minimal generating set. Then G has a presentation*

$$G = \{b_1, \cdots, b_n, x \mid b_i^{m_i}w_i(p) (i < n), b_n^{m_n}, x^{-k}b_1^{\pi_1}, \\ xb_i^{-1}x^{-1}b_1^{\nu_{i1}} \cdots b_i^{\nu_{ii}}b_{i+1}^{\pi_{i+1}} (i < n), xb_n^{-1}x^{-1}b^{\nu_{n1}} \cdots b_n^{\nu_{nn}}, \\ [b_i, b_j] (i > j, (i, j) \neq (n, 1)), b_1^{-1}b_n^{-1}b_1^m b_n\}$$

*where* $m_i = p^{\beta_i}$, $w_i(p) \in \langle b_{i+1}^p, \cdots, b_n^p \rangle$, $k = p^{\delta}$, $\pi_1 = p^{\delta_1}$, $\pi_i = p^{\nu_i}$ $(i > 1)$, $\{\nu_{ij}\}$ *is some set of integers satisfying* $\nu_{ij} \equiv 0 \pmod p$ *if* $i \neq j$, $\nu_{ii} \equiv 1 \pmod p$, *and* $m = 1 + \lambda p^{\mu}$, *where* $\lambda$ *is an integer, and* $p^{\mu}$ *is the exponent of G.*

PROOF. We may suppose $\delta_1 \leqq \delta_i$ for all $i$; set $\lambda_1' = k_ip^{\delta_i - \delta_1}$ and $\pi_1 = p^{\delta_1}$. Then $x^k = a_1^{\lambda_1} \cdots a_n^{\lambda_n} = (a_1^{\lambda_1'} \cdots a_n^{\lambda_n'})^{\pi_1} = b_1^{\pi_1}$. As $\lambda_1' \not\equiv 0 \pmod p$, $\{b_1, a_2, \cdots, a_n, x\}$ is a generating set, $b_1^{m_1} \in \langle a_2^p, \cdots, a_n^p \rangle$ and $[b_1, a_i] = 1$ for all $i$.

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

$$xb_ix^{-1} = b_1^{\nu_{i1}} \cdots b_i^{\nu_{ii}}(a_{i+1}^{\alpha'_{ii+1}} \cdots a_n^{\alpha'_{in}}) = b_1^{\nu_{i1}} \cdots b_i^{\nu_{ii}}(a_{i+1}^{\alpha''_{ii+1}} \cdots a_n^{\alpha''_{in}})^{\pi_{i+1}}$$

as in the first step, where $\alpha''_{ii+1} \not\equiv 0 \pmod p$, $\pi_{i+1} = p^{\nu_{i+1}}$. Let $b_{i+1}$ be the term inside the brackets. Then $\{b_1, \cdots, b_{i+1}, a_{i+2}, \cdots, a_n, x\}$ is a generating set, $b_{i+1}^{m_{i+1}} \in \langle a_{i+2}^p, \cdots, a_n^p \rangle$ (if $i < n-1$, otherwise $b_n^{m_n} = 1$), $xb_ix^{-1} = b_1^{\nu_{i1}} \cdots b_i^{\nu_{ii}}b_{i+1}^{\pi_{i+1}}$, $[b_{i+1}, a_j] = 1$ for all $j$, and all the congruences on the $\{\nu_{ij}\}$ 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 $b_1, \cdots, b_n$ satisfying the required relations. The process terminates at $b_n$, and we still have $xb_nx^{-1}=b_1^{\nu_{n1}} \cdots b_n^{\nu_{nn}}$. At this step we may go through the argument again, replacing each occurrence of $\langle a_j^p, \cdots, a_n^p\rangle$ by $\langle b_j^p, \cdots, b_n^p\rangle$. Clearly the order of each $b_j$ is a power of $p$, because $b_j^{m_j}\in\langle b_{j+1}^p, \cdots, b_n^p\rangle$, $b_{j+1}^{m_{j+1}}\in\langle b_{j+2}^p, \cdots, b_n^p\rangle$, $\cdots$ etc., and $b_n^{m_n}=1$, each $m_i$ being a power of $p$. Also, if the exponent of $G$ is $p^\mu$, we may replace the defining relation $[b_n, b_1]=1$ by $b_nb_1=b_1^mb_n$, where $m=1+\lambda p^\mu$ for some positive integer $\lambda$. This completes the proof.

*Note.* In the above proof, $\nu_{ij}$ may be replaced by $\nu_{ij}+sp^\mu$ 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 $\kappa\in K$ 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 $A_1(t), \cdots, A_r(t)$. For each $i$, $1\leqq i\leqq r$, there are four possibilities:

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

(ii) $A_i(t)|B(t)$ and $A_i(t)\nmid C(t)$—then there is at most one $\lambda$ such that $A_i(t)|D(t)$, since if $\lambda_1$ and $\lambda_2$ have this property:

$$A_i(t) \mid \kappa_1B(t) + \lambda_1C(t) + \mu \quad \text{and} \quad A_i(t) \mid \kappa_2B(t) + \lambda_2C(t) + \mu,$$

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

$$A_i(t) \mid \kappa B(t) + \lambda_1C(t) + \mu \quad \text{and} \quad A_i(t) \mid \kappa B(t) + \lambda_2C(t) + \mu,$$

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 $\lambda\in L'$, $A_i(t)\nmid D(t)$ 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

$$A_i(t) \nmid \kappa B(t) + \lambda C(t) + \mu \quad \text{for each } i = 1, \cdots, r.$$

Hence $A(t)$ and $\kappa B(t)+\lambda C(t)+\mu$ are coprime.

LEMMA 5. *Let $p, q_1, \cdots, q_r$ be distinct primes, then it is possible to find an integer $k$ such that, for $n>0$,*

$$(1+kp^\alpha)^n - 1 \not\equiv 0 \pmod{q_1, \cdots, q_r}.$$

PROOF. $p^\alpha$ is prime to $q_1 \cdots q_r$ so by the division algorithm there exists an integer $k$ such that $kp^\alpha \equiv -1 \pmod{q_1 \cdots q_r}$. Then

$$(1+kp^\alpha)^n - 1 \equiv -1 \pmod{q_1 \cdots q_r}$$

so

$$(1+kp^\alpha)^n - 1 \equiv -1 \pmod{q_1, \cdots, q_r}.$$

## 3. The main theorem.

THEOREM 3. *Let*

$$G = \{a_1, \cdots, a_n, x \mid a_i^{m_i}, x^{-k}a_1^{\lambda_1} \cdots a_n^{\lambda_n}, xa_i^{-1}x^{-1}a_1^{\alpha_{i1}} \cdots a_n^{\alpha_{in}} \\ (i=1, \cdots, n); [a_i, a_j](i>j)\}$$

*where $m_i = p^{\beta i}$, $k=p^\delta$, $\lambda_i = k_i p^{\delta_i}$, $k_i \not\equiv 0 \pmod p$, $\alpha_{ij} \equiv 0 \pmod p$ 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 $G \in \mathcal{G}_p$.*

PROOF. By Lemma 3, $G$ has a presentation

$$G = \{b_1, \cdots, b_n, x \mid x^{-k}b_1^{\pi_1}; xb_i^{-1}x^{-1}b_1^{\nu_{i1}} \cdots b_i^{\nu_{ii}}b_{i+1}^{\pi_{i+1}} (i<n), \\ xb_n^{-1}x^{-1}b_1^{\nu_{n1}} \cdots b_n^{\nu_{nn}}; [b_i, b_j] (i>j, (i,j) \neq (n,1)), \\ b_1^{-1}b_n^{-1}b_1^m b_n; b_i^{m_i}w_i(p) (i<n), b_n^{m_n}\}$$

where $k=p^\delta$, $\pi_1 = p^{\delta_1}$, $\pi_i = p^{\nu_i}$ $(i>1)$, $\nu_{ij} \equiv 0 \pmod p$ if $i \neq j$, $\nu_{ii} \equiv 1 \pmod p$, $m = 1+\lambda p^\mu$, $m_i = p^{\beta_i}$, $w_i(p) \in \langle b_{i+1}^p, \cdots, b_n^p \rangle$. We abbreviate this presentation to

$$G = \{b_1, \cdots, b_n, x \mid R_1, \cdots, R_t, b_i^{m_i}w_i(p) (i<n), b_n^{m_n}\}.$$

With this notation we define

$$K = \{b_1, \cdots, b_n, x \mid R_1, \cdots, R_t\},$$

and

$$H = \{b_1, \cdots, b_n, x \mid R_1, \cdots, R_t, b_i^{m_i}w_i(p) (i<n), b_n^{m_n}; \\ b_j^p (j=1, \cdots, n)\}.$$

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 $t = 1+n+C_2^n = \frac{1}{2}(n+1) \times (n+2)-n$, so $H$ has a minimal presentation

$$H = \{b_1, \cdots, b_n, x \mid R_1, \cdots, R_t, b_j^p (j=1, \cdots, n)\},$$

and $H \in \mathcal{G}_p$. Thus $R_1, \cdots, R_t$ are linearly independent, and to apply

Theorem 1 and thereby prove the theorem, it remains only to show that for a suitable choice of $\nu_{ij}$ and $\lambda$, $H$ is a $p$-group.

We have $x^k = b_1^{\pi_1}$ so $x b_1^{\pi_1} x^{-1} = b_1^{\pi_1}$, which implies $b_1^{(\nu_{11}-1)\pi_1} b_2^{\pi_2\pi_1} = 1$,

$$x b_2^{\pi_2\pi_1} x^{-1} = x b_1^{(1-\nu_{11})\pi_1} x^{-1} = b_1^{(1-\nu_{11})\pi_1} = b_2^{\pi_2\pi_1},$$

which implies $b_1^{\nu_{21}\pi_2\pi_1} b_2^{(\nu_{22}-1)\pi_2\pi_1} b_3^{\pi_3\pi_2\pi_1} = 1$. We continue as in the last step for $b_3, \cdots, b_{n-2}$, obtaining $x b_{n-2}^{\pi_{n-2}\cdots\pi_1} x^{-1} = b_{n-2}^{\pi_{n-2}\cdots\pi_1}$ which implies

$$b_1^{\nu_{n-2\,1}\pi_{n-2}\cdots\pi_1} \cdots b_{n-2}^{(\nu_{n-2\,n-2}-1)\pi_{n-2}\cdots\pi_1} b_{n-1}^{\pi_{n-1}\cdots\pi_1} = 1.$$

For $b_{n-1}$ we recall that $b_n b_1 = b_1^m b_n$ applies, and we derive

(i) $$b_1^{\nu_{n-1\,1}S(m)} b_2^{\nu_{n-1\,2}\pi_{n-1}\cdots\pi_1} \cdots b_{n-1}^{(\nu_{n-1\,n-1}-1)\pi_{n-1}\cdots\pi_1} b_n^{\pi_n\cdots\pi_1} = 1.$$

From this and the preceding equations, $b_n^{\pi_n\cdots\pi_1} \in gp\{b_1\}$, so $b_n^{\pi_n\cdots\pi_1^2} \in gp\{b_1^{\pi_1}\} = gp\{x^k\}$ so that $x b_n^{\pi_n\cdots\pi_1^2} x^{-1} = b_n^{\pi_n\cdots\pi_1^2}$, and

(ii) $$b_1^{\nu_{n1}T(m)} b_2^{\nu_{n2}\pi_n\cdots\pi_1^2} \cdots b_n^{(\nu_{nn}-1)\pi_n\cdots\pi_1^2} = 1$$

where in (i) and (ii), $S(m)$ and $T(m)$ are polynomials in $m$, which are independent of $\nu_{nn}$, $\nu_{n-1\,1}$ and $\nu_{n1}$. From (i) and (ii) and earlier derivations, we may derive

$$b_n^{\pi_n\cdots\pi_1} = b_1^{-c_1-\nu_{n-1\,1}S(m)}, \qquad b_n^{(\nu_{nn}-1)\pi_n\cdots\pi_1^2} = b_1^{-c_2-\nu_{n1}T(m)}$$

where $c_1$ and $c_2$ are nonzero integers independent of $\nu_{nn}$. Thus

$$b_n^{(\nu_{nn}-1)\pi_n\cdots\pi_1^2} = b_1^{-(\nu_{nn}-1)\pi_1\nu_{n-1\,1}S(m)-(\nu_{nn}-1)\pi_1 c_1} = b_1^{-c_2-\nu_{n1}T(m)}.$$

By suitable choice of $\nu_{nn}$ we may ensure that

$$c_3 = (\nu_{nn}-1)\pi_1 c_1 - c_2 \neq 0;$$

then $b_1^{\psi(m)} = 1$, where $\psi(m) = (\nu_{nn}-1)\pi_1\nu_{n-1\,1}S(m) - \nu_{n1}T(m) + c_3$.

Also, from (i): $b_n b_1 b_n^{-1} = b_1^m$, so $b_n^\sigma b_1 b_n^{-\sigma} = b_1^{m^\sigma}$. If we put $\sigma = p^{\pi_n\cdots\pi_1}$, then $b_n^\sigma$ is a power of $b_1$, so $b_n^\sigma b_1 b_n^{-\sigma} = b_1$, and we have

(iii) $$b_1^{m^\sigma - 1} = 1, \qquad b_1^{\psi(m)} = 1,$$

so that $|b_1|$ is the greatest common divisor of $m^\sigma - 1$ and $\psi(m)$. Now $S(m)$ and $T(m)$ are independent of $\nu_{n-1\,1}$ and $\nu_{n1}$, 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 $q_1^{t_1} \cdots q_k^{t_k} p^{t_0}$—but if $|b_1|$ divides $m^\sigma - 1$ and $\psi(m)$, then it must divide this number, whence, since $m = 1 + \lambda p^\mu$, by Lemma 5 it is possible to choose $\lambda$ such that $m^\sigma - 1$ is prime to $q_1, \cdots, q_k$. 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

1. D. Epstein, *Finite presentations of groups and* 3-*manifolds*, Quart. J. Math. Oxford Ser. (2) **12** (1961), 205–212. MR **26** #1867.

2. J.-P. Serre, *Cohomologie galoisienne*, 3rd ed., Lecture Notes in Math., no. 5, Springer-Verlag, Berlin and New York, 1965. MR **34** #1328.

3. J. W. Wamsley, *The deficiency of metacyclic groups*, Proc. Amer. Math. Soc. **24** (1970), 724–726. MR **41** #3576.

School of Mathematics, The Flinders University of South Australia, Bedford Park, South Australia