BULL. AUSTRAL. MATH. SOC. 20D15, 20F05
VOL. 8 (1973), 103-131.

# Presentations of metacyclic groups

Bruce W. King

Each metacyclic $p$-group has a natural canonical presentation which is easily derived from the usual presentation. Parameters in the canonical presentation measure how far the group is from splitting, and from being either commutative or dihedral. The structure of the groups is discussed.

## 1. Introduction

A metacyclic $p$-group is usually given by a presentation

$$a^{p^m} = 1 \ , \quad b^{p^n} = a^k \ , \quad a^b = a^r$$

where $m, n \geq 0$ , $0 < r, k \leq p^m$ , $p^m | k(r-1)$ and $p^m \Big| r^{p^n} - 1$ . Different values of the parameters $m, n, r, k$ do not necessarily correspond to non-isomorphic groups. In order to study metacyclic $p$-groups it is desirable to restrict the possible values of the parameters so that two different sets of parameters do correspond to non-isomorphic groups. Partial solutions to this problem exist. For fixed $m, n$ with $n = 1$ the result is well-known, and for fixed $m, n$ with $n = 2$ there is a solution in Burnside [3]. An arithmetic solution for arbitrary fixed $m, n$ appears in [1], but the main theorem is incorrect as stated, and certain points are obscure, rendering the use of [1] difficult. Furthermore, as is shown below the same group can occur with different values of the parameters $m, n$ .

The explicit solution offered here is: every non-cyclic metacyclic $p$-group has a unique presentation of the form

Received 26 September 1972. The author is indebted to Dr L.G. Kovács and Dr M.F. Newman for suggested improvements.

$$a^{p^m} = 1 \ , \quad b^{p^n} = a^{p^{m-s}} \ , \quad a^b = \begin{cases} a^{1+p^{m-c}} \\ \\ a^{-1+p^{m-c}} \end{cases} ,$$

where the second alternative occurs only for $p = 2$, and the parameters satisfy simple inequalities listed in Theorem 3.2. It is claimed that this is a natural presentation for the following reasons. The parameter $s$ measures how far the group is from splitting, for every metacyclic $p$-group $G$ has a unique minimal normal subgroup $S$ in its derived group such that $G/S$ splits and the order of $S$ is $p^s$ (Theorem 4.6).

In a splitting metacyclic group the order of the cyclic normal subgroup and of its cyclic complement are fixed (Theorem 4.4); in the above presentation these orders are $p^m$, $p^n$ respectively. For the first alternative above the parameter $c$ measures how far the group is from being commutative, and the derived group has order $p^c$. For the second alternative $c$ measures how far the group is from being dihedral (see Theorem 4.9).

Solutions related to this one have recently been obtained in [2] and [7], the former based on cohomology methods, the latter based on an extensive treatment of the subgroup lattice of a metacyclic group in two preceding papers [5], [6].

In the present paper the methods are a combination of presentation-theoretic and group-theoretic arguments. An advantage of the methods used here is that with them it is comparatively simple to derive certain properties of metacyclic groups. A number of properties can be read off directly from the presentations (Proposition 4.10 and §5). These properties are needed in the proof of Theorem 5.4 which justifies the claim that different presentations lead to non-isomorphic groups. The method of getting from an initial presentation to the canonical one (Theorems 3.1, 3.2) is constructive (4.2, 4.3), and makes the transformation to canonical form a simple matter.

The results obtained on group structure are of interest in themselves, as only a little is yet known either about non-split metacyclic $p$-groups,

or about the metacyclic 2-groups whose presentations are as in the second alternative above. In the latter case particular groups such as the dihedral, semi-dihedral and quaternion groups are well-known and a class of groups $\tilde{P}_n$ has been discussed in [8]. The cyclic and abelian structure of split metacyclic $p$-groups has been dealt with in [5], [6] by Lindenberg, but the non-split groups are mentioned only briefly in [7].

## 2. Notation and preliminaries

Unless otherwise stated, the groups occurring are finite $p$-groups. $p$ always denotes the prime under consideration.

Generally, notation is standard. In particular, note the following usage;

$$p^k \| \omega \quad \text{means} \quad p^k | \omega \quad \text{and} \quad p^{k+1} \nmid \omega \ .$$

$G$, $\gamma_2(G)$, ..., $\gamma_i(G)$, ... is the descending central series of a group $G$. $G$, $\Phi(G)$, $\Phi^2(G) = \Phi\big(\Phi(G)\big)$, ... defines a descending Frattini series.

If $n$ is a non-negative integer then $G^n = \langle g^n;\ g \in G \rangle$ denotes the subgroup generated by the $n$th powers of elements of $G$.

$D = D(2^g)$, $S = S(2^g)$ and $Q = Q(2^g)$ denote respectively the dihedral, semi-dihedral and generalized quaternion groups of order $2^g$.

Next, some special notation is introduced, relating to metacyclic groups. Let $m$, $n$, $s$, $r$, $c$ and $k$ be integers.

$\langle a.b \rangle$ and likewise $\langle a|b \rangle$ and $\langle a\|b \rangle$, denotes a metacyclic group which is the extension of a cyclic normal subgroup $\langle a \rangle$ by $\langle b \rangle$.

In particular $\langle a.b \rangle$ refers to the presentation

$$a^{p^m} = 1 \ , \quad b^{p^n} = a^{p^{m-s}} \ , \quad a^b = a^r$$

with $m \geq s \geq 0$, $n > 0$, $p^s | r-1$ and $p^m \Big| r^{p^n} - 1$.

For $\langle a|b \rangle$ and $\langle a\|b \rangle$, refer to Theorems 3.1 and 3.2.

If necessary the parameters of interest are included in the notation,

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

as for example, $\langle a.b;\ m,\ n,\ s,\ c,\ \pm\rangle$ .

From now on, the following simplifying assumptions are made.

(i) $\langle a.b\rangle$ is not cyclic, and so $m > s \geq 0$ , $n > 0$ .

(ii) $r$ is an integer, $1 < r \leq 1+p^m$ , representing an element in the group of units of $Z(p^m)$ . This is legitimate since $|a| = p^m$ and by (i), $p|r-1$ . Hence $r = 1 + hp^{m-c}$ , $p \nmid h$ , $m > c \geq 0$ if $p \geq 3$ , but $r = \pm 1 + h2^{m-c}$ , $2 \nmid h$, $m > c \geq 0$ if $p = 2$ . Further, if $p = 2$ and $m \geq 3$ then $m-1 > c \geq 0$ .

These formulae for $r$ correspond to the fact that the group of units of $Z(p^m)$ has generator $1 + p$ except if $p = 2$ and $m \geq 3$ , when it has generators $1 + 2^2$ , $-1 + 2^2$ . For fixed $c$ , as $h$ varies $r$ represents all the elements of order $p^c$ . Hence $c \leq n$ .

$q(x, u)$ denotes the (integer) quotient $\frac{x^u-1}{x-1}$ if $x$, $u$ are integers, $u \geq 0$ and $x \neq 1$ . If $x = 1$ put $q(1, u) = u$ .

$R$ is the least positive integer such that $R \equiv r^{p^n-1} \bmod p^m$ . Thus $b^{-1}ab = a^r$ and $bab^{-1} = a^R$ . Note that the same parameter $c$ is associated with $R$ as with $r$ .

To complete the preliminaries it remains to observe two important but elementary facts in connection with the arithmetic of the parameters.

The first of these facts is the nature of the $p$-power divisors of the integers $q = q(\pm r, u)$ . For example $q(r, u)$ arises naturally in taking powers of products.

Thus

$$(ab)^{p^k} = ab.ab. \ \ldots\ .ab = a(bab^{-1})(b^2ab^{-2}) \ \ldots\ \left(b^{p^k-1}ab^{-(p^k-1)}\right)b^{p^k}$$
$$= a^{1+R+\ldots}\, b^{p^k} = a^{q(R,p^k)}b^{p^k} .$$

**PROPOSITION 2.1.** *Let $k$ be an integer, $k \geq 0$ .*

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

*(a)* ([1], [5]). $p^k \| u$ *implies that* $p^k \| q(r, u)$ *except if* $p = 2$ *and* $4 | r+1$ .

$2^k \| u$ , $k \neq 0$ , *implies that* $2^{k+m-c-1} \| q(r, u)$ *if* $p = 2$ *and* $4 | r+1$ .

*Under either condition above,* $p^{k+m-c} \| r^u - 1$ .

*(b)* $2^k \| u$ *implies that* $2^k \| q(-r, u)$ *if* $p = 2$ *and* $4 | r+1$ .

The proofs amount to expanding $(\pm 1 + hp^{m-c})^u - 1$ (or in *(b)*, $(-1+h2^{m-c})^u + 1$ if $2 \nmid u$ ) in powers of $p$ and then cancelling powers of $p$ from numerator and denominator of $q = q(\pm r, u)$ .

The second fact is that the generators $a, b$ in $\langle a.b \rangle$ may be chosen so as to make $h = 1$ in the formulae for $r$ . The point to note is that this can be done without disturbing the form of the relation $b^{p^n} = a^{p^{m-s}}$ .

It is necessary first to prove the following lemma.

**LEMMA 2.2.** *Let* $r$ *be defined as above and let* $u, t$ *be positive integers with* $t \leq m$ *and* $p \nmid u$ .

*The map* $u \mapsto q(r, u)$ *determines a bijection of the group of units of* $Z(p^t)$ *except if* $p = 2$ *and* $4 | r+1$ .

*The map* $u \mapsto q(-r, u)$ *determines a bijection of the group of units of* $Z(p^t)$ *if* $p = 2$ *and* $4 | r+1$ .

Proof. The method of proof used for $p \geq 3$ or for $p = 2$ and $4 | r-1$ also works for $p = 2$ and $4 | r+1$ after + signs are replaced by - signs as appropriate.

Let $U$ be the group of units of $Z(p^t)$ . By Proposition 2.1, if $p \nmid u$ then $p \nmid q(r, u)$ so that it can be assumed that $q \in U$ . Suppose that $0 < u_1 \leq u_2 < p^t$ for two values $u_1, u_2$ of $u$ . Now

$$q(r, u_2) - q(r, u_1) = (1 + \ldots + r^{u_2-1}) - (1 + \ldots + r^{u_1-1})$$

$$= r^{u_1} q(r, u_2 - u_1) .$$

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

Hence if $q(r, u_2) \equiv q(r, u_1) \bmod p^t$ then $p^t | q(r, u_2-u_1)$ .

By Proposition 2.1 again it follows that $p^t | u_2-u_1$ and so $u_1 = u_2$ . Thus $u \mapsto q$ is injective, whence it is bijective as $U$ is finite.

Thus the proof is complete. It may be remarked that $u \mapsto q$ is even an automorphism of $U$ if $t \leq m-c$ . This is so since

$$q(r, u_1u_2) = q\left(r^{u_1}, u_2\right)q(r, u_1)$$

with $q\left(r^{u_1}, u_2\right) \equiv q(r, u_2) \bmod p^{m-c}$ .

Now the second fact can be proven.

**PROPOSITION 2.3.** *Let $G = \langle a.b \rangle$ be a non-cyclic metacyclic p-group with parameters $m, n, s, c, r$ .*

*$G$ also has a presentation $\langle a^*.b^* \rangle$ with parameters $m, n, s, c, r^* = \pm 1 + p^{m-c}$ such that $\langle a^* \rangle = \langle a \rangle$ and $\langle b^* \rangle = \langle b \rangle$ .*

Proof. Let $r$ be as described in assumption (ii) above, that is $r = \pm 1 + hp^{m-c}$ . Take new generators $a^* = a^u$ , $b^* = b^u$ with $p \nmid u$ . Hence

$$\begin{aligned} a^{*b^*} &= a^{ur^u} = (a^*)^{\pm 1}(a^*)^{r^u \mp 1} \\ &= (a^*)^{\pm 1}(a^*)^{qhp^{m-c}} \end{aligned}$$

where $q = q(\pm r, u)$ .

By Lemma 2.2 it follows that $u$ can be chosen to make $qh \equiv 1 \bmod p^c$ . Hence $a^{*b^*} = (a^*)^{\pm 1+p^{m-c}}$ and $r^*$ may be defined to equal $\pm 1 + p^{m-c}$ . Note that the choice of sign in $r^*$ when $p = 2$ is the same as the choice of sign in $r$ .

REMARK. From this proof it is clear that every group $\langle a.b \rangle$ has a presentation involving only the parameters $m, n, s, c$ and a sign, $\pm$ . $\langle a.b \rangle$ may now be taken to refer to this presentation, whenever necessary.

## 3. Statement of theorems

The first main theorem provides an explicit solution to the problem of isomorphism of extensions of a cyclic normal subgroup $C(p^m)$ by $C(p^n)$.

Each such extension is either cyclic or isomorphic to a metacyclic group $\langle a|b;\ m, n, s, c, \pm\rangle$ whose presentation $\langle a|b\rangle$ is said to be in reduced form.

THEOREM 3.1. *(a) Every group* $G = \langle a.b;\ m, n, s, c, \pm\rangle$ *has exactly one reduced presentation* $\langle a^*|b^*;\ m, n, s^*, c^*, \pm\rangle$ *up to isomorphism. Reduced presentations with different parameters* $s, c$ *represent non-isomorphic groups, for fixed* $m, n$.

*(b) A presentation is reduced if and only if its parameters satisfy one of six sets of conditions below, where* $r = \pm 1 + p^{m-c}$.

*For* $p \geq 3$, *or for* $p = 2$, $4|r-1$ *and* $c < m-1$ *if* $m \geq 2$:

*(i)* $0 = s \leq c < \min\{n+1, m\}$;

*(ii)* $\max\{1, m-n+1\} \leq s < \min\{c, m-c+1\}$;

*(iii)* $\max\{c, m-n+1\} \leq s < m-c < m$.

*For* $p = 2$, $4|r+1$ *and* $c < m-1$:

*(i)* $0 = s \leq c < \min\{n+1, m-1\}$;

*(ii)* $1 = s$, $\max\{1, m-n+1\} \leq c < \min\{n, m-1\}$, *or* $1 = s$, $c = 0$, $1 = n < m$, *(generalized quaternion);*

*(iii)* $1 = s$, $c = 0$, $2 = m \leq n$.

In the lists above, the type *(i)* groups have $s = 0$ so split as given. Groups of types *(ii)* and *(iii)* have been separately classified, as the type *(iii)* groups can also be represented as split extensions $\langle a^*|b^*;\ m^*, n^*\rangle$ with $m^* \neq m$, $n^* \neq n$ whereas type *(ii)* groups are never split extensions (Theorem 3.2). If groups of type *(iii)* are dropped from the list then the groups remaining have presentations $\langle a\|b\rangle$ said to be in uniquely reduced form. Every metacyclic $p$-group has a presentation $\langle a\|b\rangle$ as the next theorem, Theorem 3.2, shows.

Thus Theorem 3.2 provides a solution to the problem of associating a unique presentation with each metacyclic $p$-group. There are four basic

types of uniquely reduced presentations.

First, a metacyclic group either splits or never splits. Correspondingly, its uniquely reduced presentation has either $s = 0$ (splitting) or $s > 0$ (non-split).

Secondly, either $p \geq 3$ or $p = 2$ and then two kinds of group arise. One kind has $p = 2$, $4|r-1$ and consists of what may be called ordinary metacyclic groups, along with their analogues, the metacyclic $p$-groups with $p \geq 3$. The other kind of metacyclic 2-group has $4|r+1$ and is called exceptional.

Notice that a presentation of the form $\langle a.b; + \rangle$ always defines an ordinary metacyclic group, but that it may be necessary to uniquely reduce a presentation $\langle a.b; - \rangle$ to determine whether the group so defined is exceptional.

It is shown in Theorem 4.9 that ordinary and exceptional metacyclic 2-groups may be distinguished by certain group-theoretic properties.

THEOREM 3.2. *Every metacyclic $p$-group has up to isomorphism exactly one uniquely reduced presentation $\langle a\|b; m, n, s, c, \pm \rangle$, for some set of parameters $m, n, s, c, \pm$. A presentation is uniquely reduced if and only if the parameters satisfy the following conditions, where $r = \pm 1 + p^{m-c}$.*

Ordinary metacyclic groups. $p \geq 3$ *or* $p = 2$, $4|r-1$ *and* $c < m-1$ *if* $m \geq 2$.

*(i)* Split: $0 = s \leq c < \min\{n+1, m\}$;

*(ii)* Non-split: $\max\{1, m-n+1\} \leq s < \min\{c, m-c+1\}$.

Exceptional metacyclic groups. $p = 2$, $4|r+1$ *and* $c < m-1$.

*(i)* Split: $0 = s \leq c < \min\{n+1, m-1\}$;

*(ii)* Non-split: $1 = s$, $\max\{1, m-n+1\} \leq c < \min\{n, m-1\}$ *or* $1 = s$, $c = 0$, $1 = n < m$ *(generalized quaternion).*

The proof of Theorems 3.1, 3.2 are by manipulation of the basic presentation in Theorem 2.3. In order to establish that the groups listed in the theorems are not isomorphic, one relates the parameters to group invariants under isomorphism. The theorem which achieves this is Theorem

5.4, which is stated here in a simplified formulation.

THEOREM 3.3. *If there exists a metacyclic p-group $G$ of order $p^g$, with derived factor of type $(p^h, p^k)$ and centre of type $(p^{h'}, p^{k'})$, then either*

*(i) $G$ is unique (up to isomorphism) in having this derived factor and centre, or*

*(ii) $G/G'$ is of type $(2^n, 2)$ and $Z(G)$ is of type $(2^{n-1}, 2)$.*

*If $n > 1$ then $G \cong \langle a\|b; m, n, 0, 0, -\rangle$ or $G \cong \langle a\|b; m, n, 0, 1, -\rangle$. If $n = 1$ then $G \cong D, S$ or $Q$.*

## 4. Group properties of metacyclic $p$-groups

The section begins with the computational aspects of the proofs of the first two of the main theorems.

In this section some routine calculations in metacyclic $p$-groups are carried out. These results will be used to find the centre, Frattini subgroup and derived factor of a metacyclic group. An important by-product is a group-theoretic method for distinguishing the exceptional metacyclic groups from others.

Recall the definition of the quotients $q(r, u)$ and the facts concerning divisibility (Proposition 2.1).

LEMMA 4.1. *If $G = \langle a.b \rangle$ is a non-abelian metacyclic p-group, then for integers $\alpha, \beta, \lambda, k$ with $k \geq 1$,*

$$(a^\alpha b^\beta)^{p^k} = a^{\alpha p^k} b^{\beta p^k} [a^\alpha, b^\beta]^{\lambda p^{k-1}} .$$

*Also $p|\lambda$ if and only if $p \geq 3$.*

Proof. It may be assumed that $\alpha = \beta = 1$ as $\langle a^\alpha, b^\beta \rangle$ is also metacyclic. Let $q = q(R, p^k)$. Thus

$$(ab)^{p^k} = a^q b^{p^k} = a^{p^k} b^{p^k} a^{(q-p^k)r p^k} .$$

But from the binomial expansion of $(1+(R-1))^{p^k}$ one has

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

$q - p^k = \binom{p^k}{2}(R-1) + \ldots$ and so $(R-1)p^k | q-p^k$ if $p \geq 3$, but only $(R-1)2^{k-1} | q-2^k$ if $p = 2$.

As $[a, b^{-1}] = a^{R-1}$ and $[a, b] = a^{r-1}$ and both generate the cyclic group $G'$, the result follows.

From the lemma it is seen that if $\langle a.b \rangle$ is a metacyclic $p$-group then $G' \leq \langle a^p \rangle$, whence $\Phi(G) = G^p = \langle a^p.b^p \rangle$. The formula $\Phi(G) = \langle a^2.b^2 \rangle$ is particularly useful in dealing with 2-groups, as is shown in Lemma 4.7.

Lemma 4.1 and Proposition 2.1 are now to be used to show that presentations of metacyclic $p$-groups may be reduced to the forms in Theorems 3.1, 3.2. The proof of these theorems is completed by using Theorem 3.3, which shows that the uniquely reduced presentations listed in Theorem 3.2 define non-isomorphic groups. Due to the method for obtaining Theorem 3.2 from Theorem 3.1 the reduced presentations listed in Theorem 3.1 also define non-isomorphic groups.

4.2 Proof of Theorem 3.1. From the discussion in §1 concerning the parameters $c$ and $r$, it follows that $0 \leq c < \min\{m, n+1\}$ and even $c < m-1$ if $p = 2$ and $4 | r+1$.

From the basic defining relations for $\langle a.b \rangle$ as in Proposition 2.3 it is seen that $p^s | r-1$ and so $0 \leq s \leq m-c$ except if $p = 2$ and $4 | r+1$ when $0 \leq s \leq 1$ since $2 \| r-1$.

However, for some values of $s$, $c$ it is possible to obtain a splitting presentation by replacing $b$ by a new generator $b^*$, as is now shown.

For if $0 < s \leq m-n$, and $4 | r-1$ when $p = 2$, put $b^* = ba^{-p^{m-n-s}}$. Therefore by Lemma 4.1,

$$b^{*p^n} = b^{p^n} a^{-p^{m-s}} \left[a^{-p^{m-n-s}}, b\right]^{\lambda p^{n-1}}$$

(with $p | \lambda$ if and only if $p \geq 3$). Thus $b^{*p^n} = a^{-\lambda p^{2m-c-s-1}}$. If

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

$s^* = c + s - m + 1$ then $s^* \leq 1$ if $p \geq 3$ and certainly $s^* < s$ when $p = 2$ since $c \leq m-2$ .

If $p \geq 3$ then $p|\lambda$ and so $b^{*p^n} = 1$ . If $p = 2$ and $s^* < s$ then, by repeating the process, eventually $s^* = 0$ is obtained. Then $G = \langle a.b^*; m, n, 0, c, + \rangle$ and this is a splitting extension.

On the other hand, if $p = 2$ and $4|r+1$ , suppose that $c = n$ when $s = 1$ . Put $b^* = ba$ , and so $b^{*2^n} = b^{2^n} a^q$ with $q = q(r, 2^n)$ . Hence by Proposition 2.1,

$$b^{*2^n} = b^{2^n} a^{2^{m-c+n-1}} = b^{2^n} a^{2^{m-1}} = 1 .$$

Then $G = \langle a.b^*; m, n, 0, n, - \rangle$ and this is a splitting extension.

Second, it is shown that if $m \geq 3$ , $n \geq 2$ , $s = 1$ , $c = 0$ when $p = 2$ and $4|r+1$ then one can choose a new generator $a^*$ and parameter $c^* = 1$ . For, put $a^* = ab^{2^{n-1}}$ , $n \geq 2$ , so that $a^{*2} = a^2 b^{2^n} = a^{2(1+2^{m-2})}$ . Hence

$$a^2 = a^{*2(1+2^{m-2}+2^{2m-4})} = (a^*)^{2-2^{m-1}}$$

since $m \geq 3$ . Thus

$$[a^*, b] = [a, b] = a^{-2} = (a^*)^{-2+2^{m-1}}$$

and

$$b^{2^n} = a^{2^{m-1}} = \left((a^*)^{2-2^{m-1}}\right)^{2^{m-2}} = (a^*)^{2^{m-1}} .$$

Thus $G = \langle a^*, b; m, n, 1, 1, - \rangle$ .

Finally, it is easily verified that with the restrictions on parameters derived above, the groups can be listed as in Theorem 3.1.

4.3 Proof of Theorem 3.2. It suffices to assume that $G$ has a reduced presentation $\langle a|b; m, n, s, c, \pm \rangle$ of type *(iii)* in Theorem 3.1. It is shown that such a group also has a splitting reduced presentation of the form $\langle b|a^*; n+s, m-s, 0, c^*, + \rangle$ .

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

First let $G = \langle a|b;\ + \rangle$ and put $a^* = b^{p^{n+s-m}} a^{-1}$ so that $G = \langle a^*, b \rangle$. Now

$$a^{*p^{m-s}} = b^{p^n} a^{-p^{m-s}} \left[a^{-1}, b^{p^{n+s-m}}\right]^{\lambda p^{m-s-1}}$$

by Lemma 4.1. Hence (by Proposition 2.1), $a^{*p^{m-s}} = a^{\tau p^{n+m-c-1}}$ where $\tau p^{n+m-c-1} = -\left(r^{p^{n+s-m}} - 1\right)\lambda p^{m-s-1}$. Thus $a^{*p^{m-s}} = 1$ since $n + m - c - 1 > m - 1$ as $G$ is of type *(iii)* in Theorem 3.1.

Also $a^{p^{m-c}} = \left(a^{p^{m-s}}\right)^{p^{s-c}} = \left(b^{p^n}\right)^{p^{s-c}} \in \langle b \rangle$ and thus $G' \leq \langle b \rangle$, $\langle b \rangle \trianglelefteq G$.

But $|b| = p^{n+s}$ and $|a^*| \leq p^{m-s}$ whence $G$ is actually a split extension of $\langle b \rangle$ by $\langle a^* \rangle$ and $|a^*| = p^{m-s}$.

Second, let $G = \langle a|b;\ - \rangle$ again of type *(iii)* in Theorem 3.1. Rewrite the defining relations so that

$$G = \left\langle b,\ a;\ b^{2^{n+1}} = 1,\ a^2 = b^{2^n},\ [b, a] = b^{2^n} \right\rangle.$$

Next put $a^* = ab^{-2^{n+1}}$, and thence $G = \langle b|a^*;\ n+1,\ 1,\ 0,\ n,\ + \rangle$. Thus, the result required is proven.

Observe that a splitting presentation $\langle a.b \rangle$ for a metacyclic $p$-group is not further reduced by the operations in Theorems 3.1, 3.2. That is to say, for a splitting presentation, $\langle a.b \rangle = \langle a\|b \rangle$. This observation shows that Theorem 3.2 implies the following theorem.

**THEOREM 4.4.** *In a splitting metacyclic $p$-group the order of a cyclic normal subgroup and of its cyclic complement is fixed.*

The derivation of Theorem 4.4 given here relies on the isomorphism aspect of Theorem 3.2, but the result can also be proved directly. It is not used in the sequel in any case.

**LEMMA 4.5.** *Let $\langle a\|b \rangle$ be a uniquely reduced presentation of a*

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

*metacyclic p-group $G$, and let $N$ be a normal subgroup of $G$ properly contained in the cyclic normal subgroup $\langle a \rangle$.*

*The factor group $G/N$ has a uniquely reduced presentation $\langle aN \| bN \rangle$.*

**Proof.** Clearly it is sufficient to consider the case in which $|N| = p$, $N \lhd G$, $N < \langle a \rangle$. Hence $N = \left\langle a^{p^{m-1}} \right\rangle$. If $G = \langle a \| b;\ m, n, s, c, \pm \rangle$ and $0 \le s \le 1$ then $G/N$ splits, whence $\langle aN \| bN \rangle$ is in uniquely reduced form. Thus the only case remaining to be proved is that of the ordinary non-split groups $\langle a \| b;\ + \rangle$ in which if $p \ge 3$ then $\max\{1, m-n+1\} \le s < c < \min\{m-s+1, m\}$, $s \ge 2$.

But $G/N = \langle aN.bN;\ m-1, n, s-1, c-1, + \rangle$ and so

$$\max\{1, m-n\} \le s-1 < c-1 < \min\{m-s, m-1\}.$$

Hence $G/N = \langle aN \| bN \rangle$ as required. (The case for $p = 2$ is identical except for the last term in the inequalities.)

Now that Lemma 4.5 is proved, it is possible to establish the nature of the parameter $s$ in a uniquely reduced presentation. The magnitude of $s$ measures how far $G$ is from splitting. By Theorem 3.2 this result does not necessarily hold for presentations that merely are reduced.

**THEOREM 4.6.** *Let $G$ be a metacyclic p-group and $S$ be its unique minimal normal subgroup contained in the derived subgroup, such that $G/S$ splits.*

*If $G = \langle a \| b;\ m, n, s, c, \pm \rangle$ then $S$ has order $p^s$.*

**Proof.** $S$ exists since $G/G'$ splits. The result is obviously true if $G$ has small order; so for induction it can be supposed true in $G/N$ where $N \le S$ and $|N| = p$.

By Lemma 4.5, $G/N = \langle aN \| bN;\ m-1, s-1, c, \pm \rangle$ for some parameter $\bar{c}$, where by induction $|S/N| = p^{s-1}$. Hence $|S| = p^s$ as required.

It will be seen that the parameter $c$ is not quite as simply related to the presentation as $s$ is. The following lemma is fundamental in the study of this question.

**LEMMA 4.7.** *Let $G = \langle a.b \rangle$ be a metacyclic p-group, and let $x, y$ be generators of $G$.*

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

*(a)* $\Phi(G) = G^p = \langle x^p, y^p \rangle$, *except in case (b) below.*

*(b) If* $G$ *has reduced relations* $\langle a|b; - \rangle$ *and* $\langle x \rangle = \langle ab^\beta \rangle$, $\langle y \rangle = \langle a^\rho b \rangle$ *with* $\beta, \rho$ *integers such that* $\beta$ *is even or zero and* $\rho$ *is odd then* $\langle x^2, y^2 \rangle = \left\langle a^{2^{m-c}}, b^2 \right\rangle$. *Furthermore* $\langle x^2, y^2 \rangle$ *is normal in* $G$ *and its factor group* $G/\langle x^2, y^2 \rangle$ *is the epimorphic image of a dihedral group of order* $2^{m-c+1}$.

Proof. (i) As noted before, Lemma 4.1 implies the result if $\langle x \rangle = \langle a \rangle$, $\langle y \rangle = \langle b \rangle$.

Let $G = \langle x, y \rangle$ with $x = a^\alpha b^\beta$, $y = a^\rho b^\sigma$ for some integers $\alpha, \beta, \rho, \sigma$. From working in the vector space $G/\Phi(G)$ it is seen that $\alpha\sigma \not\equiv \beta\rho \bmod p$.

By Lemma 4.1, $x^p = a^{\alpha p} b^{\beta p} [a^\alpha, b^\beta]^\lambda$ where $p|\lambda$ if $p \geq 3$ and a similar result holds for $y^p$.

Suppose first that $G$ is abelian or $p \geq 3$; therefore

$$x^p \equiv a^{\alpha p} b^{\beta p}, \quad y^p \equiv a^{\rho p} b^{\sigma p} \text{ modulo } \Phi^2(G).$$

Eliminating $b^p$ from these congruences gives $a^{p(\beta\rho - \alpha\sigma)} \equiv x^{-\sigma p} y^{\beta p}$ and thus $a^p \in \langle x^p, y^p \rangle \Phi^2(G)$. Hence $\Phi(G) = \langle a^p, b^p \rangle \leq \langle x^p, y^p \rangle \Phi^2(G)$ whence $\langle a^p, b^p \rangle = \langle x^p, y^p \rangle$.

Suppose next that $p = 2$ and $4|r-1$. In this case $G' \leq \langle a^4 \rangle \leq \langle a^4, b^4 \rangle \leq \Phi^2(G)$ and so $G/\Phi^2(G)$ is abelian. By the case already dealt with above, therefore $\langle a^2, b^2 \rangle \equiv \langle x^2, y^2 \rangle \bmod \Phi^2(G)$ and so $\langle a^2, b^2 \rangle = \langle x^2, y^2 \rangle$.

(ii) Consider now the case in which $p = 2$ and $4|r+1$.

By symmetry one may take $\alpha, \sigma$ to be odd, and so assume $\alpha = \sigma = 1$ by choice of generators. There are then two typical cases; first $2|\beta$ and $\rho$ arbitrary and second $2|\rho$ but $2 \nmid \beta$ (since $1 \not\equiv \beta\rho \bmod 2$).

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

In the first of these two cases, $\beta = 0$ gives $x = a$, $y = a^{\rho}b$ and so $G = \langle x.y \rangle$, the case handled before. So $\beta \neq 0$ and then

$$x^2 = a^{q(R^{\beta},2)}b^{2\beta} \quad \text{and} \quad y^{2\beta} = a^{\rho q(R,2\beta)}b^{2\beta} .$$

From this it follows that

$$x^2y^{-2\beta} = a^{q(R^{\beta},2)-\rho q(R,2\beta)}$$

Let $2^{\nu}\|\beta$, for some positive integer $\nu$. By Proposition 2.1 it follows that $2\|q(R^{\beta}, 2)$ and $2^{m-c+\nu}|q(R, 2\beta)$, with $m-c+\nu \geq 3$. Thus $x^2y^{-2\beta} = a^{2j}$, $j$ odd, showing that $a^2 \in \langle x^2, y^2 \rangle$. Since $y^2 = a^{\rho q(R,2)}b^2$ it follows that $b^2 \in \langle x^2, y^2 \rangle$. Hence $\langle a^2, b^2 \rangle = \langle x^2, y^2 \rangle$.

It remains to consider the second of these two cases. As $\beta$ is odd, one has that

$$2^{m-c}\|q(R^{\beta}, 2) \quad \text{and} \quad 2^{m-c}\|q(R, 2\beta) .$$

As $2|\rho$ therefore $a^{2^{m-c}} \in \langle x^2, y^2 \rangle$ and $b^2 \in \left\langle a^{2^{m-c}}, y^2 \right\rangle$ so that $\left\langle a^{2^{m-c}}, b^2 \right\rangle \leq \langle x^2, y^2 \rangle \leq \left\langle a^{2^{m-c}}, b^2 \right\rangle$ and therefore equality holds.

This proves most of the lemma. Finally it is necessary to look at the factor group $G/\langle x^2, y^2 \rangle$.

First, $\langle x^2, y^2 \rangle \trianglelefteq G$. For $[a, b^2] = a^{h2^{m-c+1}}$ so that

$$a^{-1}b^{-2}a = a^{h2^{m-c+1}}b^{-2} \in \left\langle a^{2^{m-c}}, b^2 \right\rangle .$$

This yields $(b^2)^g \in \left\langle a^{2^{m-c}}, b^2 \right\rangle$ for any $g \in \langle a.b \rangle$. But $\langle a \rangle \trianglelefteq G$ and therefore $\left\langle a^{2^{m-c}}, b^2 \right\rangle \trianglelefteq G$.

Also $a^{2^{m-c}} \equiv b^2 \equiv 1$, $[a, b] \equiv a^{-2}$ modulo $\left\langle a^{2^{m-c}}, b^2 \right\rangle$ whence the

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

factor group is the epimorphic image of a dihedral group of order at most $2^{m-c+1}$ . This completes the proof of the lemma and also of the next corollary.

COROLLARY 4.8. *If $G$ is a metacyclic p-group then $\Phi(G)$ is an ordinary metacyclic group.*

Consider in more detail the subgroup $\left\langle a^{2^{m-c}}, b^2 \right\rangle$ in a group $\langle a|b; - \rangle$ . It is usually the case that $\left\langle a^{2^{m-c}}, b^2 \right\rangle < \Phi(G) = \langle a^2, b^2 \rangle$ . Suppose first of all that this inequality holds. If $G$ splits, or if $c > 0$ when $G$ does not split then $\left|\left\langle a^{2^{m-c}}, b^2 \right\rangle\right| = 2^{n+c-1}$ . Hence in these cases it follows that $G \Big/ \left\langle a^{2^{m-c}}, b^2 \right\rangle$ is dihedral of order $2^{m-c+1}$ . For the case remaining in which $c = 0$ one has $G = Q(2^{m+1})$ , $m \geq 3$ , and $\left\langle a^{2^{m-c}}, b^2 \right\rangle = \langle b^2 \rangle$ has order 2 .

Therefore, suppose instead that $\left\langle a^{2^{m-c}}, b^2 \right\rangle = \Phi(G)$ . Since $\left\langle a^{2^{m-c}}, b^2 \right\rangle \Big/ \Phi^2(G)$ is cyclic therefore $\Phi(G)$ is cyclic. Hence either $1 \neq b^2 \in \langle a^2 \rangle$ and so $n = 1$ , or $a^2 \in \langle b^2 \rangle$ and $n > 1$ . The first of these alternatives shows that $G \tilde{=} Q(8)$ , whilst the second shows that $m = 2$ and that the reduced relations for $G$ are of type *(iii)* in Theorem 3.1. In the latter case therefore $G$ is not exceptional.

This argument leads to the next theorem.

THEOREM 4.9. *Let $G = \langle a.b; c, - \rangle$ be some presentation of an exceptional metacyclic 2-group $\langle a^* \| b^*; c^*, - \rangle$ .*

*$G_D = \left\langle a^{2^{m-c}}, b^2 \right\rangle = \left\langle a^{*2^{m-c^*}}, b^{*2} \right\rangle$ is independent of the choice of presentation $\langle a.b \rangle$ .*

*Furthermore $G_D$ is a characteristic subgroup of $G$ which is the intersection of all normal subgroups of $G$ which give dihedral factor*

*groups, and* $G/G_D$ *is the largest dihedral factor group of* $G$ .

*Either* $G/G_D$ *has order* $2^{m-c+1}$ *or* $G = Q(2^{m+1})$ *and* $G/G_D$ *has order* $2^m$ .

Proof. By Lemma 4.7, $G_D = \langle x^2, y^2 \rangle$ which is unique. Further it is obviously still unique modulo $N$ if $N \trianglelefteq G$ and so if $G/N$ is dihedral then $N \geq G_D$ .

Hence $G_D$ is a characteristic subgroup of $G$ , which (according to the discussion preceeding this theorem) does give a dihedral group $G/G_D$ of the desired order via a reduced presentation of $G$ . Note, that since $G$ is by hypothesis an exceptional 2-group, there is only one case in which $G_D = \Phi(G)$ , namely when $G \tilde{=} Q(8)$ . In this case therefore $G/G_D$ is (abelian) dihedral of order 4 .

Finally this section is completed by a list of further group properties in relation to group parameters.

PROPOSITION 4.10. *Let* $G = \langle a|b;\ m, n, s, c, \pm \rangle$ *be a reduced presentation of a metacyclic p-group.*

*(i) Let* $G$ *have nilpotent class* $\nu$ . *If* $G = \langle a|b;\ + \rangle$ *then* $\nu(m-c) \geq m > (\nu-1)(m-c)$ . *If* $G = \langle a|b;\ - \rangle$ *then* $\nu = m$ .

*(ii) Let* $Z(G) = \left\langle a^{p^u}, b^{p^u} \right\rangle < G$ . *If* $G = \langle a|b;\ + \rangle$ *then* $u = v = c$ . *If* $G = \langle a|b;\ - \rangle$ *then* $u = m - 1$ , $v = \max\{1, c\}$ .

*Thus if* $G$ *is exceptional then either* $Z(G)$ *is cyclic or else* $G$ *splits and* $Z(G)$ *is of type* $(2^t, 2)$ , $t \geq 1$ .

*(iii) Let* $G$ *have class at least* 3 . *If* $G = \langle a|b;\ + \rangle$ *then* $C_G(G') = \left\langle a, b^{p^c} \right\rangle$ . *If* $G = \langle a|b;\ - \rangle$ *then* $C_G(G') = \left\langle a, b^{p^{\max\{1, c-1\}}} \right\rangle$ .

*(iv) The exponent* $p^\omega$ *of* $G$ *is* $\max\{|a|, |b|\}$ *and so* $\omega = \max\{n+s, m\}$ .

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

*(v) The derived factor group is of type* $(p^{m-c}, p^n)$ *if* $G = \langle a|b; + \rangle$, *or of type* $(2^n, 2)$ *if* $G = \langle a|b; - \rangle$.

Proofs. *(i)* $G' = \left\langle a^{p^{m-c}} \right\rangle$ or $G' = \langle a^2 \rangle$ respectively.

*(ii)* $\left(a^{p^u}\right)^b = a^{p^u(r-1)}a^{p^u} = a^{p^u}$ if and only if $c \leq u$ when $G = \langle a|b; + \rangle$ or if and only if $c \leq 1$ when $G = \langle a|b; - \rangle$.

Similarly $\left(b^{p^v}\right)^a = a^{-1}\left(b^{p^v}ab^{-p^v}\right) = b^{p^v}$, if and only if both $v \geq 1$ (as $G$ is non-abelian) and also $p^m | R^{p^v} - 1$, that is, $v \geq c$.

*(iii)* Similar to *(ii)* with $a$ replaced by $a^{p^{m-c}}$ and $p^m$ replaced by $p^c$ if $G = \langle a|b; + \rangle$ or with $a$ replaced by $a^2$ and $2^m$ replaced by $2^{m-1}$ if $G = \langle a|b; - \rangle$.

*(iv)* This follows from the fact that by Corollary 4.8, $\Phi(G) = \langle a^p|b^p \rangle$ is an ordinary metacyclic group, containing $\langle x^p, y^p \rangle$ for any pair of generators.

By induction $\Phi(G)$ has exponent equal to $\max\{|a^p|, |b^p|\}$, and so $|x^p| \leq \max\{|a^p|, |b^p|\}$. Therefore $|x| \leq \max\{|a|, |b|\}$.

*(v)* Modulo $G'$ one has $a^{p^{m-c}} \equiv 1$, $b^{p^n} \equiv a^{p^{m-s}}$, $[a, b] \equiv 1$, if $G = \langle a|b; + \rangle$ and this factor group is therefore abelian of type $(p^{m-c}, p^n)$. If $G = \langle a|b; - \rangle$ then modulo $G'$,

$$a^2 \equiv b^{2^n} \equiv 1, \quad [a, b] \equiv 1$$

and so the factor group is abelian of type $(2^n, 2)$.

This section is concluded with the following remarks. It is well known that for odd primes $p$, metacyclic $p$-groups are regular. This may be proved by application of Lemma 4.1, or by the general theory of regular $p$-groups ([4], Satz 10.13, p. 332). From this follows the

odd-prime case of Proposition 4.10 *(iv)*. Regularity is not found particularly useful in problems of the kind dealt with here.

Finally there are group-theoretic tests which verify whether a metacyclic 2-group suspected of being exceptional is exceptional. The simplest is the following:

If $G = \langle x, y \rangle$ then one considers whether $\langle x^2, y^2 \rangle$, $\langle (xy)^2, y^2 \rangle$, $\langle (xy)^2, x^2 \rangle$ are equal. By Lemma 4.7 they are equal if and only if the group $G$ is either an ordinary metacyclic 2-group or is isomorphic to $Q(8)$. In case $G$ is exceptional this test also determines values for the parameter $c$.

## 5. Invariants of metacyclic $p$-groups

The purpose of this section is to relate the parameters of a metacyclic group $G = \langle a \| b; m, n, s, c, \pm \rangle$ to isomorphism invariants such as order, exponent and the abelian types of the derived factor and centre.

By this means one is able to choose metacyclic groups which satisfy given conditions on their group structure. Various possibilities will be obvious from the text. In particular, one fairly simple set of conditions in Theorem 5.4 is enough to specify metacyclic $p$-groups uniquely up to isomorphism. It follows that distinct uniquely reduced presentations determine non-isomorphic metacyclic groups, thus completing the proofs of the main theorems.

Throughout this section, the following notation will be used. $g$, $\omega$, $z$, $\kappa$, $\gamma$, $\alpha$, $\varepsilon$ are non-negative integers such that $|G| = p^g$, $|Z(G)| = p^z$, $\exp G = p^\omega$, $\exp Z(G) = p^\kappa$ and $|G'| = p^\gamma$.

It remains to define $\alpha$ and $\varepsilon$. A group element not contained in the Frattini-subgroup of the group is said to be a non-Frattini element. $\alpha$ is defined so that $p^\alpha$ is equal to the minimum of the orders of the non-Frattini elements of the group.

$\varepsilon$ is defined to equal zero if $G$ is an ordinary metacyclic group, and to equal $m - c - 1$ if $G$ is exceptional. By use of $\varepsilon$ some repetition of arguments in the ordinary and exceptional cases is avoided.

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

The first lemma relates $\alpha$, $\omega$ and $g$.

**LEMMA 5.1.** *Let* $G = \langle a\|b; m, n, s, c, \pm\rangle$ *be a non-cyclic metacyclic p-group of order* $p^g$, *exponent* $p^\omega$, *in which* $p^\alpha$ *is the minimum of the orders of the non-Frattini elements of* $G$. $n + s = \alpha$ *if and only if* $m - s \geq n$ *and* $m - s = \alpha$ *if* $m - s < n$.

*Further* $\alpha + \omega = g$ *except if* $G$ *is a non-split exceptional 2-group with* $m - 1 \geq n$, *in which case* $\alpha + \omega = g + 1$.

Proof. (i) Let $u$, $v$ be integers. $a^u b^v$ is a non-Frattini element of $G$ if and only if $p$ divides at most one of $u$ and $v$. Putting $u = u'p^x$, $v = v'p^y$ with $p \nmid u'$, $p \nmid v'$ makes it possible to restate this condition as:

$a^u b^v$ is a non-Frattini element of $G$ if and only if either $0 = y \leq x \leq m$ or $0 = x < y \leq n$.

Let $\beta$ be a non-negative integer such that $(a^u b^v)^{p^\beta} = a^{uq} b^{vp^\beta} = 1$, where $q = q(R^v, p^\beta)$ as in §1.

There are two cases; first, that $|a| = p^m | uq$, or equivalently that $|b| = p^{n+s} | vp^\beta$; second that $G$ does not split and $uq \equiv kp^{m-s}$ and $vp^\beta \equiv -kp^n$ modulo $p^m$ for some integer $k$.

Case 1. $p^m | uq$.

If $0 = y \leq x \leq m$ then $R^v$ is of the form $\pm 1 + hp^{m-c}$ by Proposition 2.1. Hence $|a| \Big| uq$ and $|b| \Big| vp^\beta$ if and only if $p^m | p^{x+\beta+\varepsilon}$ (by Proposition 2.1) and $p^{n+s} | p^\beta$, that is,

$$\beta \geq \max\{m-x-\varepsilon,\ n+s\}.$$

By choosing $x \geq 0$ such that $m-x-\varepsilon \leq n+s$ one therefore attains a minimal value of $\beta$, namely $\beta_1 = n + s$.

Next consider the other inequality $0 = x < y \leq n$. By Proposition 2.1, $p^{y+m-c} \| R^v - 1$ where $y+m-c \geq 2$. Hence by Proposition 2.1,

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

$p^{\beta} \| uq\,(R^{v}, p^{\beta})$ and so $p^{m} | p^{\beta}$ if $|a| \Big| uq$ . Also $p^{n+s} | p^{\beta+y}$ as $|b| \Big| vp^{\beta}$ .

Hence $\beta \geq \max\{m, n+s-y\}$ so that if $y$ is chosen large enough then $n+s-y \leq m$ and plainly $\beta_2 = m$ is a minimal value for $\beta$ .

Case 2. $uq \equiv kp^{m-s}$ and $vp^{\beta} \equiv -kp^{n} \bmod p^{m}$ .

It suffices to assume that $p^{m} \nmid kp^{m-s}$ else Case 1 applies. If $y = 0$ , then equating $p$-power divisors of $k$ gives

$$p^{m}/p^{m-s} > p^{x+\beta+\varepsilon}/p^{m-s} = p^{\beta}/p^{n} ,$$

the quotients being integers. Hence

$$m - x - s - \varepsilon = n \leq \beta < m - x - \varepsilon = n + s .$$

Thus $n \leq m-s$ and also $n \leq \beta < n+s$ so that $s \neq 0$ .

By Theorem 3.2 these two facts imply that $G$ is exceptional and so $s = 1$ . Therefore $n = m - 1 - x - \varepsilon = c - x$ so that $c \neq 0$ and $n \leq c$ . But Theorem 3.2 implies that $c < n$ , a contradiction. Thus instead it must be that $x = 0 < y \leq n$ . Proceeding as above gives

$$p^{m}/p^{m-s} > p^{\beta}/p^{m-s} = p^{y+\beta}/p^{n}$$

whence $m - s = n - y \leq \beta < m$ . In particular $m - s < n$ as $y > 0$ .

Now $q = h'p^{\beta}$ , $p \nmid h'$ , whence from the two expressions involving $k$ , it is the case that $u'h' \equiv -v' \bmod p^{m+n-\beta}$ .

Conversely $q$ (and hence $h'$ ) is determined by $v'$ and $\beta$ . From $h'$ and $v'$ one may determine $u' = u$ by solving the congruence. Hence, provided $\beta$ satisfies the inequality $m - s = n - y \leq \beta < m$ therefore $uq \equiv kp^{m-s}$ and $vp^{\beta} \equiv -kp^{n}$ modulo $p^{m}$ , with $p^{m} \nmid uq$ . Thus $\beta$ attains its lower bound $m - s < n$ whence a minimal value for it is $\beta_3 = m - s$ .

(ii) Let $\alpha = \min\{\beta_i\}$ for the $\beta_i$ appropriate to the group considered. By Proposition 4.10, $\omega = \max\{n+s, m\}$ .

First, let $m - s \geq n$ . By Theorem 3.2 either $G$ is split or $G$ is a non-split exceptional group with $s = 1$ .

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

If $G$ splits then $s = 0$ and $\alpha = \min\{\beta_1, \beta_2\} = \min\{n, m\}$, $\omega = \max\{m, n\}$ and therefore $\alpha + \omega = m + n = g$. If $G$ is non-split and $m-1 \geq n$ then $\alpha = \min\{\beta_1, \beta_2\} = \min\{n+1, m\} = n + 1$ and hence $\alpha + \omega = g + 1$.

Second, let $m - s < n$. If $G$ splits then $\alpha + \omega = g$ as above. If $G$ is non-split then $\alpha = \min\{\beta_1, \beta_2, \beta_3\} = \min\{n+s, m-s\} = m - s$ since $m - s \leq n$. But $\omega = \max\{n+s, m\} = n + s$ whence $\alpha + \omega = g$.

This completes the proof of the first lemma. The second lemma deals with relationships between other parameters and group invariants.

**LEMMA 5.2.** *Let* $G = \langle a\|b; m, n, s, c, \pm\rangle$.

*(a) If $G$ is an ordinary metacyclic group then $\gamma = c$, $z = g - 2c$ and $\kappa = \max\{m-c, n+s-c\}$. Also, if $G$ has class greater than 2, then* $|C_G(G')| = p^{g-c}$.

*(b) If $G$ is an exceptional metacyclic group then $\gamma = m - 1$, $z = n + 1 - c$ for $c \neq 0$ and $z = n$ for $c = 0$. $\kappa = z - 1$ if $G$ is split, or $\kappa = z$ if $G$ is not split. Also, if $G$ has class greater than 2, that is if $m \geq 3$, then $|C_G(G')| = 2^{g-c+1}$ if $c \geq 2$, whilst if $c \leq 3$ then $C_G(G')$ is a maximal subgroup of $G$.*

Proof. Suppose first that $G$ is an ordinary metacyclic group, whence $\gamma = c$. By Proposition 4.10,

$$p^z = \left|\left\langle a^{p^c}, b^{p^c}\right\rangle\right| = \left|a^{p^c}\right|\left|b^{p^c}\right| \Big/ |\langle a\rangle \cap \langle b\rangle|$$

since $c < m - s$ and $c \leq n$ by Theorem 3.2.

But $\left|a^{p^c}\right| = p^{m-c}$, $\left|b^{p^c}\right| = p^{n+s-c}$ and $|\langle a\rangle \cap \langle b\rangle| = \left|a^{p^{m-s}}\right| = p^s$ whence $p^z = p^{m+n-2c} = p^{g-2c}$.

It is clear that $Z(G)$ has exponent $p^\kappa$ where $\kappa = \max\{m-c, n+s-c\}$, since $Z(G)$ has generators $a^{p^c}$, $b^{p^c}$ and is abelian.

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

To prove that $|C_G(G')| = p^{g-c}$ one observes that

$C_G(G')/Z(G) = \langle a, b^{p^c} \rangle \Big/ \langle a^{p^c}, b^{p^c} \rangle$ has order $p^c$ .

Next suppose that $G$ is exceptional, whence $\gamma = m - 1$ . By Proposition 4.10, if $c \neq 0$ then

$$2^z = \left|\langle a^{2^{m-1}}, b^{2^c} \rangle\right| = \left|a^{2^{m-1}}\right| \left|b^{2^c}\right| \Big/ \left|\langle a^{2^{b-1}} \rangle \cap \langle b^{2^c} \rangle\right|$$

$$= 2.2^{n+1-c/2} \quad \text{when} \quad s = 1$$

and

$$= 2.2^{n-c} \quad \text{when} \quad s = 0 .$$

Thus $z = n + 1 - c$ if $c \neq 0$ . Similar arguments show that $z = n$ if $c = 0$ .

Clearly $\kappa = z - 1$ if $G$ is split, but if $G$ is not split then $Z(G)$ is cyclic and $\kappa = z$ . Finally suppose $G$ has class $\geq 3$ . By Proposition 4.10, $C_G(G') = \langle a, b^{2^{\max\{1, c-1\}}} \rangle$ . Hence if $c \geq 2$ it is easily seen that $C_G(G')/Z(G)$ has order $2^m$ whence $|C_G(G')| = 2^{n+1-c+m} = 2^{g-c+1}$ .

If $0 \leq c \leq 1$ then $C_G(G')/Z(G) = \langle a, b^2 \rangle \Big/ \langle a^{2^{m-1}}, b^2 \rangle$ and has order $2^{m-1}$ , whence $|C_G(G')| = 2^{g-1}$ . There if $c \leq 3$ , $C_G(G')$ is a maximal subgroup of $G$ .

By combining the preceding two lemmas one obtains some interesting relationships between $\varepsilon$ and various group invariants. The methods used are purely numerical, however, and do not explain the origin of the relationships.

COROLLARY 5.3. *Let $G$ be as in the lemma.*

*(a) If $G$ is an ordinary metacyclic group and $Z(G)$ is of type $(p^{z_1}, p^{z_2})$ with $z_1 = \kappa$ then $g = z + 2\gamma$ , $\omega = \kappa + \gamma$ and*

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

$z_1 - z_2 = \omega - \alpha$ .

*(b) If $G$ is an exceptional metacyclic group then $g + \varepsilon = z + 2\gamma$ if $c \neq 0$ or $g + \varepsilon = z + 2\gamma + 1$ if $c = 0$. Also $\alpha + \varepsilon = \kappa + \gamma$ if $c \neq 0$, $m - s \geq n$, $\alpha + \varepsilon = \kappa + \gamma + 1$ if $c = 0$, $m - s \geq n$, $\omega + \varepsilon = \kappa + \gamma$ if $c \neq 0$, $m - s < n$ and $\omega + \varepsilon = \kappa + \gamma + 1$ if $c = 0$, $m - s < n$.*

Proof of (a). $g = z + 2\gamma$ from Lemma 5.2. As $\omega = \max\{n+s, m\}$ therefore Lemma 5.2 shows that $\omega = \kappa + \gamma$. Finally

$$\begin{aligned} z_1 - z_2 &= 2\kappa - z = 2\kappa + 2\gamma - g \\ &= 2\omega - g \quad (\text{since } \omega = \kappa + \gamma) \\ &= \omega - \alpha \quad \text{by Lemma 5.1.} \end{aligned}$$

Proof of (b).

$$\begin{aligned} g + \varepsilon &= n + 2m - c - 1 \quad \text{by definition of } \varepsilon \\ &= n + 2\gamma - c + 1 \quad \text{since } \gamma = m - 1 \\ &= z + 2\gamma \qquad \text{if } c \neq 0 \text{ by Lemma 5.2} \end{aligned}$$

or

$$= z + 2\gamma + 1 \qquad \text{if } c = 0 \text{ by Lemma 5.2.}$$

Next, consider the expression

$$n + s + \varepsilon = n + s + m - c - 1 .$$

The expression equals $z + m + s - 2$ if $c \neq 0$ by Lemma 5.2, and hence $n + s + \varepsilon = \kappa + m - 1 = \kappa + \gamma$ whether $G$ splits or not, by Lemma 5.2.

On the other hand if $c = 0$ then

$$n + s + \varepsilon = n + s + m - 1 = \kappa + m = \kappa + \gamma + 1$$

by Lemma 5.2 (this is similar to the case for $c \neq 0$ ).

Finally $n + s = \alpha$ if $m - s \geq n$ by Lemma 5.1, whilst $n + s = \omega$ if $m - s < n$. Hence the stated results follow.

Sufficient machinery has now been developed so that the main isomorphism theorem can be proved. (A simplified formulation is given in Theorem 3.3.)

**THEOREM 5.4.** *There exists up to isomorphism at most one metacyclic*

https://doi.org/10.1017/S0004972700045500 Published online by Cambridge University Press

*group* $G$ *of the form* $\langle a\|b;\ m,\ n,\ s,\ \pm\rangle$ *of given order* $p^g$, *with derived factor of given type* $(p^h,\ p^k)$ *and centre of given type* $(p^{h'},\ p^{k'})$, *except if both* $(p^h,\ p^k) = (2^n,\ 2)$ *and* $(p^{h'},\ p^{k'}) = (2^{n-1},\ 2)$.

*If* $G$ *has derived factor of type* $(2^n,\ 2)$ *and centre of type* $(2^{n-1},\ 2)$ *there are two possibilities for* $G$.

*First, if* $n > 1$ *then* $G \cong \langle a\|b;\ m,\ n,\ 0,\ 0,\ -\rangle$ *or* $G \cong \langle a\|b;\ m,\ n,\ 0,\ 1,\ -\rangle$.

*These groups are distinguished by the orders of their greatest dihedral factor groups.*

*Second, if* $n = 1$, $m \geq 2$, *then* $G \cong D(2^{m+1})$, $S(2^{m+1})$ *or* $Q(2^{m+1})$. *These groups are distinguished by the order of their greatest dihedral factor groups together with the minimum of the orders of their non-Frattini elements.*

COROLLARY 5.5. *Distinct presentations in uniquely reduced form define non-isomorphic metacyclic groups.*

The corollary follows since there are at most three possible metacyclic groups of fixed order, having given types of derived factor and centre. However, the theorem shows also that the distinct presentations so obtained define non-isomorphic groups. Thus, to complete all the proofs of this paper, it remains to prove Theorem 5.4.

Proof. (i) Let $G = G_1$ be a given metacyclic group and let $G_2$ be a metacyclic group in which

$$|G_1| = |G_2|\ ,\quad G_1/G_1' \cong G_2/G_2' \quad \text{and} \quad Z(G_1) \cong Z(G_2)\ .$$

Put $G_i = \langle a_i\|b_i;\ m_i,\ n_i,\ s_i,\ c_i,\ \pm\rangle$ with appropriate choice of sign, $i = 1, 2$.

It simplifies details of the proof if the special cases of abelian groups and groups of order $\leq p^3$ are assumed to be trivial.

Now $G_1$ and $G_2$ are either both ordinary metacyclic groups or both exceptional. For by Proposition 4.10 *(v)* if $G_2$ is exceptional then

$G_2/G_2'$ is of type $(2^n, 2)$. Hence by Proposition 4.10 *(v)* if $G_1$ is not exceptional then $n_1 = 1$ since $m_1 - c_1 \geq 2$.

Thus by Proposition 4.10 *(ii)*, $Z(G_1) = \Phi(G_1)$, so that $Z(G_2) = \Phi(G_2)$ as $Z(G_2)$ has index 4 in $G_2$ and $G_2/Z(G_2)$ is not cyclic as $G_2$ is not cyclic. This shows that $G_2$ has class 2 and $m_2 = 2$. By Theorem 3.2 it follows that either $G_2 \tilde{=} Q(8)$ (trivial) or $G_2 = \langle a_2 \| b_2;\ 2, n_2, 0, \delta \rangle$. In the latter case $Z(G_2)$ is not cyclic by Proposition 4.10 *(ii)* whereas Proposition 4.10 *(ii)* shows that $Z(G_1)$ is cyclic since $n_1 = 1$, contradicting that $Z(G_1) \tilde{=} Z(G_2)$.

(ii) If $G_1$, $G_2$ are both ordinary metacyclic groups, it is shown that, under the hypotheses of the theorem, $G_1 \tilde{=} G_2$. To do this it is sufficient to show that $m_1 = m_2$, $n_1 = n_2$, $s_1 = s_2$, $c_1 = c_2$.

Observe that by Proposition 4.10 *(v)*, $G_i/G_i'$ has abelian invariants $p^{m_i - c_i}$, $p^{n_i}$ and order $p^{g - c_i}$. Hence by hypothesis

$$\max\{m_1 - c_1, n_1\} = \max\{m_2 - c_2, n_2\} = e \text{ (say) and } c_1 = c_2 = \gamma .$$

One can assume that $\gamma > 0$ as $\gamma = 0$ makes $G_1$, $G_2$ abelian. Also by hypothesis, the exponent of the centre is the same for both $G_1$ and $G_2$, whence by Lemma 5.2, $\kappa = \max\{m_i - c_i, n_i + s_i - c_i\}$, $i = 1, 2$.

The first step is to show that $m_1 - c_1 \geq n_1$ if and only if $m_2 - c_2 \geq n_2$. This is seen as follows.

Suppose on the contrary that $m_1 - c_1 < n_1$ and $m_2 - c_2 \geq n_2$, for example. By Theorem 3.2, $s_i \leq c_i$ whence $m_2 - c_2 \geq n_2 \geq n_2 + s_2 - c_2$ and therefore $\kappa = m_2 - c_2 = e$ by use of $G_2$. Applying this to $G_1$ gives $\kappa = \max\{m_1 - c_1, n_1 + s_1 - c_1\} = e = n_1$ and so $n_1 + s_1 - c_1 = n_1$. Hence $s_1 = c_1$ and (by supposition that $\gamma \neq 0$) this is non-zero. Thus

$G_1$ is non-split and so the defining relations in Theorem 3.2 imply that $s_1 < c_1$ (a contradiction).

For the second step there are therefore two alternatives to consider, namely, $m_i - c_i \geq n_i$ $(i = 1, 2)$ or $m_i - c_i < n_i$ $(i = 1, 2)$.

If $m_i - c_i \geq n_i$, $i = 1, 2$, then $e = m_1 - \gamma = m_2 - \gamma$ whence $m_1 = m_2$ and so $n_1 = n_2$. By Theorem 3.2 the condition $m_i - c_i \geq n_i$ implies that each $G_i$ splits and hence $s_1 = s_2$.

If $m_i - c_i < n_i$, $i = 1, 2$, then $e = n_1 = n_2 = n$ and $m_1 = m_2 = m$. Again it remains to prove that $s_1 = s_2$. If $\kappa = m - \gamma$ then $m - \gamma \geq n + s_i - \gamma$. Hence $m - n \geq s_i$ and so $s_1 = s_2 = 0$ by Theorem 3.2.

If $\kappa \neq m - \gamma$ then $m - \gamma < n + s_1 - \gamma = n + s_2 - \gamma$ and so $s_1 = s_2$.

(iii) Finally suppose that $G_1$ and $G_2$ are exceptional but not of maximal class (by Proposition 4.10 *(i)* and Theorem 3.2, the (metacyclic) 2-groups of maximal class are $D$, $S$ and $Q$). Thus by Proposition 4.10 *(v)*, $G_i/G_i'$ is of type $\left(2^{n_i}, 2\right)$ with $n_i \geq 2$, whence $n_1 = n_2 = n$ and $m_1 = m_2 = m$.

By Proposition 4.10 *(ii)* (since $n \geq 2$) $G_i$ splits if and only if $Z(G_i)$ splits non-trivially (that is, $Z(G_i)$ is not cyclic), whence $s_1 = s_2$.

By Lemma 5.2, $z = n + 1 - c_1 = n + 1 - c_2$ and so $c_1 = c_2$ if $c_1, c_2 \neq 0$, whence there remains to be considered the following case: $z = n + 1 - c_1$, $c_1 \neq 0$, in $G_1$ and $z = n$, $c_2 = 0$ in $G_2$. Thus $c_1 = 1$, $c_2 = 0$. From this it follows that $G_1$ and $G_2$ split, as otherwise $G_2 \cong Q(2^{m+1})$ by Theorem 3.2, contrary to the supposition that

the groups do not have maximal class.

Thus either $G_1 \cong G_2$ or else $G_1 = \langle a_1 \| b_1; m, n, 0, 1, - \rangle$ and $G_2 = \langle a_2 \| b_2; m, n, 0, 0, - \rangle$ with $n > 1$.

Note that in this case $G_1 \ncong G_2$ since (from Theorem 4.9),

$$(G_1)_D = \left\langle a_1^{2^{m-1}}, b_1^2 \right\rangle = Z(G_1) \quad \text{whereas} \quad (G_2)_D = \left\langle b_2^2 \right\rangle < Z(G_2) .$$

Putting $n = 1$, this argument shows $G_1 = S \ncong G_2 = D$ provided that $m \geq 3$. The remaining maximal class group $Q$ is distinguished from $D$ by the fact that $Q_D \neq 1$, and is distinguished from $S$ by having no non-Frattini element of order 2 (by Lemma 5.1).

The paper is concluded with the following remarks.

It may be noted that the proof of Theorem 5.4 involves no essential use of Lemma 5.1 or Corollary 5.3, nor of the order of the centralizer of $G'$ discussed in Lemma 5.2. The facts used about the group exponent in Proposition 4.10 *(iv)* have been derived from Lemma 4.7; by establishing the exponent result directly one could also avoid the use of Lemma 4.7 in the proof of Theorem 5.4.

The hypotheses of Theorem 5.4 can be modified in various ways by the use of Lemma 5.1 and Corollary 5.3. For example, if the group $G$ is known to have class greater than 2, then the order of the centralizer of $G'$ is often sufficient to determine $c$ from Corollary 5.3, particularly if the orders of the centre and derived groups are known. Or, if the group is known to be an ordinary metacyclic group, by Corollary 5.3, one can determine the abelian type of the centre from the orders of the group and its derived group, together with either the group exponent or (by Lemma 5.1) the minimum of the orders of the non-Frattini elements.

It is of interest to know how subgroups and factor groups are related to the type of presentation that the group has. In particular there are criteria (not stated here) which determine whether a group is exceptional by whether certain subgroups or factor groups are exceptional.

In this connection, Lindenberg shows that the ordinary metacyclic $p$-groups together with $Q(8)$ are precisely the metacyclic $p$-groups whose

subgroup lattice is modular; the remaining exceptional 2-groups have a non-modular subgroup lattice ([5], [6], [7]). The latter statement is a direct consequence of Theorem 4.9, since $D(8)$ is not modular.

## References

[1] B.G. Basmaji, "On the isomorphisms of two metacyclic groups", *Proc. Amer. Math. Soc.* 22 (1969), 175-182.

[2] F. Rudolf Beyl, "The classification of metacyclic $p$-groups", *Notices Amer. Math. Soc.* 19 (1972), 696-20-9.

[3] W. Burnside, *Theory of groups of finite order*, 2nd ed. (Cambridge University Press, Cambridge, 1911; reprinted, Dover, New York, 1955).

[4] B. Huppert, *Endliche Gruppen I* (Die Grundlehren der mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[5] Wolfgang Lindenberg, "Über die Struktur zerfallender bizyklischer $p$-Gruppen", *J. reine angew. Math.* 241 (1970), 118-146.

[6] Wolfgang Lindenberg, "Über die Struktur zerfallender nicht-modularer bizyklischer 2-Gruppen", *Ber. Ges. Math. Datenverarbeitung, Bonn* 29 (1970), 1-63.

[7] Wolfgang Lindenberg, "Struktur und Klassifizierung bizyklischer $p$-Gruppen", *Ber. Ges. Math. Datenverarbeitung, Bonn* 40 (1971), 1-36.

[8] D.S. Passman, "Nonnormal subgroups of $p$-groups", *J. Algebra* 15 (1970), 352-370.

School of Applied Sciences,
Riverina College of Advanced Education,
Wagga Wagga,
New South Wales.