J. Austral. Math. Soc. **20** (Series A) (1975), 178–198.

ON p-GROUPS WITH A CYCLIC COMMUTATOR SUBGROUP

R. J. MIECH

(Received 17 October 1972; revised 19 October 1973)

Communicated by G. Szekeres

This paper contains the complete classification of the finite p-groups G where p is an odd prime, G is generated by two elements, and the commutator subgroup of G is cyclic.

These groups are a special kind of two-generator metabelian group, a class that has been studied by Szekeres (1965). He determined the defining relations of such groups but, as he noted, a "residual isomorphism problem" remains. The cyclic commutator groups are simple when considered from this first point of view; they have a short, easily derived set of defining relations. However, the isomorphism problem is a bit complicated for the defining relations contain nine parameters and each of these parameters might and can be an invariant of the group.

One particular type of cyclic commutator group, the metacyclic, has been classified. This was done by Basmaji (1969).

I am indebted to Professor Szekeres for his helpful comments, criticisms, and suggestions on this paper.

The following notation will be used throughout this paper: (a, b, c, m, n, r, s) will denote nonnegative integers; capitals (R, S, M, N) will denote positive integers that are relatively prime to p; p is an odd prime, $p(r) = p^r$ and $p(x_1, \cdots, x_n) = p^m$ where m is the minimum of $x_1, \cdots, x_n$.

We need the defining relations of our groups to get under way. They are given by:

THEOREM 1. *Let p be an odd prime. Let G be a finite nonabelian p-group generated by two elements and suppose that the commutator subgroup of G is cyclic. Then G has a pair of generators $\{x, y\}$ such that the defining relations of the group are*

$$[y,x] = z, \quad x^{p(a)} = z^{Rp(r)}, \quad y^{p(b)} = z^{Sp(s)}$$
$$z^{p(c)} = 1, \quad [z,x] = z^{Mp(m)}, \quad [z,y] = z^{Np(n)}$$

where a, b, c, r, s, m, n and R, S, M, N are integers that satisfy the conditions

$$a \geqq b, \quad a \geqq c, \quad r + m \geqq c, \quad r + n \geqq c, \quad s + n \geqq c,$$

$$1 \leqq m, \quad n \leqq c, \quad 0 \leqq r, \quad s \leqq c, \quad p(b) - MSp(m + s) \equiv 0 \bmod p(c).$$

Conversely given any set of parameters $\{a, b, c, r, s, m, n, R, S, M, N\}$ that satisfies these conditions there is a group defined by these relations.

The defining relations stated in Theorem 1 are easy to derive: Let G_2 be the commutator subgroup of G and suppose that $G/G_2 = \langle G_2x\rangle \otimes \langle G_2y\rangle$ where $\langle G_2x\rangle$ is of order $p(a)$, $\langle G_2y\rangle$ is of order $p(b)$ and $a \geqq b$. Then set $z = [y, x]$ and assume that $G_2 = \langle z\rangle$ is of order $p(c)$ to get the power relations. Finally once we suppose that

$$[z, x] = z^{Mp(m)} \quad \text{and} \quad [z, y] = z^{Np(n)}$$

the higher order commutators are determined. We have, for example,

$$[z, x, x] = [z^{Mp(m)}, x] = z^{A}$$

where $A = (Mp(m))^2$. Note incidentally that a, b, and c are invariants of the group, G is of order $p(a + b + c)$ and if q is the smallest integer such that

$$(q - 1)\min\{m, n\} \geqq c$$

then G is of class q.

The inequalities and congruence given at the end of Theorem 1 will be derived later.

The notation arising in Theorem 1 can be abbreviated. The parameters a, b, and c will be considered fixed in what follows so the groups described there have essentially four defining relations:

$$x^{p(a)} = z^{Rp(r)}, \quad y^{p(b)} = z^{Sp(s)}, \quad [z, x] = z^{Mp(m)}, \quad [z, x] = z^{Np(n)}.$$

We shall call this group "the group defined by $[Rp^r, Sp^s, Mp^m, Np^n]$". Furthermore in our classification scheme we shall be dealing with a number of groups where one of the parameters r, s, m, or n is equal to c; that is, a power or commutator is equal to 1. To make these cases more conspicuous the corresponding p^c of the bracket notation will be replaced by 0. Thus the group defined by $[0, Sp^s, p^m, 0]$ is that group whose defining relations are

$$x^{p(a)} = 1, \quad y^{p(b)} = z^{Sp(s)}, \quad [z, x] = z^{p(m)}, \quad [z, y] = 1.$$

Finally, z will always denote the commutator of y and x; $z = [y, x]$.

As for the isomorphism problem, our groups have four defining relations and we get a system of four congruences that govern isomorphism between two such groups. The congruences are derived in section 1. Section 2 deals with the analysis of these congruences. The argument there splits into several cases for one has to make assumptions about the relative sizes of r and s and m and n to carry out the

analysis. Once this is done one can write out the different isomorphism types; there is quite a number of them.

The main factors that are employed in the presentation of the types in what follows are: (1) The size of b relative to c, i.e., $b \geqq c$ or $b < c$. (2) The relative sizes of a, b, and c, i.e., $a - b > c$, $1 \leqq a - b \leqq c$, or $a = b$. (3) The number of parameters among r, s, m, n, R, and S that appear as invariants in the defining relations. The simplest case occurs when a, b, and c are spread apart. We then have:

THEOREM 2. *If $a - b > c$ and $b \geqq c$ the distinct (non-isomorphic) groups of Theorem 1 having the parameters a, b, and c are given by:*

(a) $[Rp^r, 0, 0, p^n]$ $\quad 1 \leqq n \leqq c, \quad c - n \leqq r \leqq c, \quad R \leqq p(c - n, c - r).$

(b) $[Rp^r, 0, p^m, p^n]$ $\quad 1 \leqq m < n \leqq c, \quad c - m \leqq r \leqq c,$
$R \leqq p(c - n, c - r).$

(c) $[Rp^r, p^s, 0, p^n]$ $\quad 1 \leqq n \leqq c, \quad c - n \leqq s < r \leqq c,$
$R \leqq p(c - n, \quad c - r).$

(d) $[Rp^r, Sp^s, p^m, p^n]$ $\quad 1 \leqq s \leqq c - 1, \quad c - s \leqq m \leqq c - 1,$
$s + 1 \leqq r \leqq c, \quad m + 1 \leqq n \leqq c,$
$R \leqq p(c - n, c - r), \quad S \leqq p(r - s, n - m).$

The following conventions will be used in the rest of this paper: $\max\{q, t\} \leqq u$ will be abbreviated to $\{q, t\} \leqq u$; similarly $u \leqq \{q, t\}$ means that $u \leqq \min\{q, t\}$. In addition the "obvious" conditions, $1 \leqq m, n \leqq c$ and $0 \leqq s, r \leqq c$ will always be assumed but they will not always be mentioned.

THEOREM 3. *Suppose that $b \geqq c$ and $a - n = c - k$ where $0 \leqq k \leqq c - 1$. Then the distinct groups associated with a, b, and c and which are defined in terms of most four parameters are given by*

(a) $[p^r, 0, p^m, 0]$ $\quad 1 \leqq m \leqq k, \quad \{c - m, c - k + m\} \leqq r \leqq c.$

(b) $[0, p^s, 0, p^n]$ $\quad k/2 \leqq s \leqq k, \quad c - s \leqq n \leqq c - k + s.$

(c) $[Rp^r, 0, 0, p^n]$ $\quad 1 \leqq n \leqq c, \quad c - n \leqq r \leqq c, \; R \leqq p(c - n, c - r).$

(d) $[0, Sp^s, p^m, 0]$ $\quad c - k \leqq s \leqq k, \quad c - s \leqq m \leqq k,$
$S \leqq p(c - m, c - s).$

(e) $[Rp^r, 0, p^m, p^n]$ $\quad 1 \leqq r \leqq c, \quad c - r \leqq m \leqq c - 1,$
$m + 1 \leqq n \leqq 2c + m - k - r - 1,$
$R \leqq p(c - n, c - r, \quad 2c + m - k - r - n).$

(f) $[Rp^r, p^s, 0, p^n]$ $\quad 1 \leqq n \leqq c, \quad 0 \leqq s \leqq c - 1,$
$s + 1 \leqq r \leqq c - k - 1 + s, \quad R \leqq p(c - r, c - n).$

(g) $[p^r, Sp^s, p^m, 0]$ $\quad 0 \leqq s \leqq c - 1, \quad s + 1 \leqq r \leqq c - 1 + s - k,$
$c - r \leqq m \leqq k, \quad S \leqq p(c - s, r + k - m - s).$

(h) $[0, Sp^s, p^m, p^n]$ $\quad 0 \leqq s \leqq k, \quad c - s \leqq m \leqq c$
$\{c - s, s - k + m + 1\} \leqq n \leqq c - k + m - 1.$
$S \geqq p(n + k - s - m, \quad c - m)$

THEOREM 4. *Suppose that* $b \geqq c$ *and* $a - b = c - k$ *where* $1 \leqq k \leqq c-2$. *Let* $\mathscr{A}$ *be the set of* (r, s, m, n) *such that*

$$1 \leqq s \leqq c-1 \qquad c - s \leqq m \leqq c-1$$

$$s+1 \leqq r \leqq c-1-k+s \qquad m+1 \leqq n \leqq c-1-k+m, \qquad r, n \leqq c$$

Let $\mathscr{B}_1$ *be the subset of* $\mathscr{A}$ *where*

$$s \geqq k, \ m < k, \ \text{and} \ n > m + r - k.$$

Let $\mathscr{B}_2$ *be the subset of* $\mathscr{A}$ *where*

$$s < k, \ m \geqq k, \ \text{and} \ n < k - s + r.$$

Let $\mathscr{B}_3$ *be the subset of* $\mathscr{A}$ *where*

$$s < k \ \text{and} \ m < k.$$

Let $\mathscr{B}$ *denote the union of all the* $\mathscr{B}_i$. *Then the distinct six parameter groups of Theorem* 1 *associated with* a, b, *and* c *are given by* $[Rp, Sp^s, p^m, p^n]$ *where* (r, s, m, n) *is in* $\mathscr{A}$,

$$R \leqq p(c-r, c-r+s-k, c-n, c-n+m-k).$$

and

$$S \leqq p(r-s, n-m) \ \text{for} \ (r, s, m, n) \in \mathscr{A} - \mathscr{B},$$

$$S \leqq p(r-s+k-m, n-m+k-s) \ \text{for} \ (r, s, m, n) \in \mathscr{B}.$$

Theorems 2, 3, and 4 deal with the case where $b \geqq c$ and $a - b \geqq 1$. The case $a = b$ stands alone, which is not too surprising, for then there is a certain symmetry present in the defining relations. We have:

THEOREM 5. *If* $a = b$ *then the distinct groups of Theorem* 1 *having parameters* a, a, *and* c *are given by*

(a)	$[0, p^s, 0, p^n]$	$c/2 \leqq s \leqq c-1, \quad c-s \leqq n \leqq s.$
(b)	$[0, Sp^s, p^m, 0]$	$0 \leqq s \leqq c, \quad c-s \leqq m \leqq c. \quad S \leqq p(c-m, c-s)$
(c)	$[0, Sp^s, p^m, p^n]$	$1 \leqq s \leqq c-1, \quad c-s \leqq m \leqq c$ $\{c-s, m+s-c+1\} \leqq n \leqq m-1$

The next three theorems deal with the case $b < c$. These results could be ncorporated into Theorems 2 through 4, but when one does this the inequalities on the parameters become obscure.

THEOREM 6. *Suppose* $b > c$ *and* $a - b > c$. *Then the distinct groups of Theorem* 1 *associated with the parameters* a, b, *and* c *are given by* $[Rp^r, Sp^s, p^{b-s}, p^n]$ *where:*

$$0 \leqq s \leqq b-1, \quad c-b+s \leqq r \leqq c, \quad c-s \leqq n \leqq c,$$

$$R \leqq p(c-n, c-r),\ S \leqq p(r-s, b-s, n-b+s),\ S \equiv 1 \bmod p(c-b).$$

THEOREM 7. *Suppose that $b < c$ and $a - b = c - k$ where $0 \leqq k \leqq b$. Then the distinct groups associated with a, b, and c which are defined in terms of at most three parameters are given by*:

(a) $[0, Sp^s, p^{b-s}, 0]$ $\quad b-k \leqq s \leqq \{k, b-1\},\ S \equiv 1 \bmod p(c-b)$
$S \leqq p(c-b+s, b-s)$.

(b) $[p^r, Sp^s, p^{b-s}, 0]$ $\quad b-k \leqq s \leqq b-1,\ c-b+s \leqq r \leqq c-k-1+s,$
$S \equiv 1 \bmod p(c-b),\ S \leqq p(b-s, r+k-b)$.

(c) $[0, Sp^s, p^{b-s}, p^n]$ $\quad b-k \leqq s \leqq k,\ \{c-s, b-k+1\} \leqq n \leqq c-s$
$+ b-k-1,\ S \equiv 1 \bmod p(c-b)$
$S \leqq p(k+n-b, c+s-b, b-s)$.

THEOREM 8. *Suppose that $b < c$ and $a - b = c - k$ where $2 \leqq k \leqq b$. Let $\mathscr{A}$ denote the set of (r, s, n) such that*

$$0 \leqq s \leqq b-1, \quad c-b+s \leqq r \leqq c-k-1+s$$

$$c-s \leqq n \leqq c-s+b-1-k, \quad r, n \leqq c.$$

Let $\mathscr{B}_1$ be the subset of $\mathscr{A}$ where

$$s \geqq \{k, b-k+1\}, \quad r < b, \quad \text{and} \quad n > b-k+r-s.$$

Let $\mathscr{B}_2$ be the subset of $\mathscr{A}$ where

$$s \leqq \{k-1, b-k\} \text{ and } n < \{k-s+r, 2b-2s\}.$$

Let $\mathscr{B}_3$ be the subset of $\mathscr{A}$ where

$$b-k < s < k \text{ and } r < b \text{ or } n < 2b-2s.$$

Let $\mathscr{B}$ denote the union of all the $\mathscr{B}_i$. Then the distinct five parameter groups of Theorem 1 associated with a, b, and c are given by $[Rp^r, Sp^s, p^{b-s}, p^n]$ where (r, s, n) is in $\mathfrak{U}$, $S \equiv 1 \bmod p(c-b)$,

$$R \leqq p(c-r, c-r+s-k, c-n, c-n+b-s-k)$$

and

$$S \leqq p(r-s, n-b+s, b-s) \text{ for } (r, s, n) \in \mathscr{A} - \mathscr{B},$$

$$S \leqq p(r+k-b, n+k-b, b-s) \text{ for } (r, s, n) \in \mathscr{B}.$$

This completes the tabulation of the groups of Theorem 1. Any such group is isomorphic to one of the groups of Theorems 2 through 8. Furthermore any two classes listed in any one of these theorems are disjoint.

1. The isomorphism congruences

Set

$$\mu = 1 + Mp^m, \qquad \nu = 1 + Np^n.$$

Note that μ is a function of M and m; ν depends on N and n. Next, let

$$M(\alpha) = \sum_{i=0}^{\alpha-1} \mu^i, \qquad N(\alpha) = \sum_{i=0}^{\alpha-1} \nu^i.$$

We then have

THEOREM 9. *Let* $G = \langle x, y\rangle$ *be defined by* $[Rp^r, Sp^s, Mp^m, Np^n]$ *and* $\bar{G} = \langle \bar{x}, \bar{y}\rangle$ *be defined by* $[\bar{R}p^{\bar{r}}, \bar{S}p^{\bar{s}}, \bar{M}p^{\bar{m}}, \bar{N}p^{\bar{n}}]$. *Suppose* θ *is the mapping from* $\bar{G}$ *to* G *defined by*

$$\bar{x}^\theta = x^\alpha y^\beta z^\pi, \qquad \bar{y}^\theta = x^\gamma y^\delta z^\rho.$$

Let $\Delta = \alpha\delta - \beta\gamma$. *Then* θ *is an isomorphism if and only if* $(\Delta, p) = 1$, $\gamma = \gamma' p^{a-b}$ *and*

$$\begin{aligned} \alpha Rp^r + \beta Sp^{s+a-b} &\equiv \varepsilon \bar{R}p^{\bar{r}} \bmod p^c \\ \gamma' Rp^r + \delta p^s &\equiv \varepsilon \bar{S}p^{\bar{s}} + \rho p^b \bmod p^c \\ \mu^\alpha \nu^\beta &\equiv \bar{\mu} \bmod p^c \\ \mu^\gamma \nu^\delta &\equiv \bar{\nu} \bmod p^c \end{aligned}$$

where

$$\varepsilon = M(\alpha)N(\delta)\nu^\beta - M(\gamma)N(\beta)\nu^\delta.$$

The number ε appearing in Theorem 9 is prime to p: We have $\mu \equiv \nu \equiv 1 \bmod p$, hence $M(\alpha) \equiv \alpha$, $N(\delta) \equiv \delta, \cdots$, and $\varepsilon \equiv \Delta \bmod p$.

We need several results on commutators to prove Theorem 9. The first is:

LEMMA 1. *Let* G *be defined as in Theorem* 1. *Let* μ *and* $M(\alpha)$ *be defined as above and set* $z(\alpha) = z^\alpha$. *Then*

$$\begin{aligned} [y^\beta, x^\alpha] &= z(M(\alpha)N(\beta)) \\ [z^\gamma, x^\alpha y^\beta] &= z(\gamma(\mu^\alpha \nu^\beta - 1)). \end{aligned}$$

PROOF. These results are easy consequences of the usual commutator relations for a metabelian group.

The inequalities stated in Theorem 1 can be derived at this point: By the defining relations there,

$$1 = [y^{p(b)}, y] = [z^{Sp(s)}, y] = z^{SNp(s+n)}.$$

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

Consequently, $s + n \geqq c$. Next

$$1 = [z, y^{p(b)}] = z^A$$

where, by Lemma 1,

$$A = (1 + Np^n)^{p(b)} - 1 = Bp^{b+n}$$

and $(B, p) = 1$. Thus $b + n \geqq c$. Similar arguments with the power $x^{p(a)}$ yield $r + m \geqq c$ and $a + m \geqq c$.

To continue, by Lemma 1 and the inequality $a + m \geqq c$, $[y, x^{p(a)}] = z^A$ where $A \equiv p^a \bmod p^c$. But we also have

$$[y, x^{p(a)}] = [y, z^{Rp(r)}] = z^{-NRp(n+r)}.$$

Consequently

$$p(a) + NRp(n + r) \equiv 0 \bmod p(c). \tag{1}$$

A similar congruence

$$p(b) - NSp(m + s) \equiv 0 \bmod p(c) \tag{2}$$

can be obtained by expanding $[x, y^{p(b)}]$ in two ways. These two congruences imply that $a \geqq c$ and $r + n \geqq c$: Suppose that $a < c$. Then by (1), $a = n + r$. Furthermore since $b \leqq a < c$ we have by (2), $b = m + s$. Thus we have

$$a + b = (n + r) + (m + s) = (s + n) + (m + r) \geqq c + c,$$

a contradiction. So, $a \geqq c$ and $r + n \geqq c$.

Finally we must have $m \geqq 1$ and $n \geqq 1$. If for example $n = 0$ then $[y, x]^M = [y, x, x]$ so $G_2 \leqq G_3 = [G, G_2]$.

The converse to Theorem 1 can be proved in the conventional way.

LEMMA 2. *Let G be defined as in Theorem 1. Then for any x, y in G and any positive integer q*

$$(xy)^q = x^q y^q z^{G(q)}$$

where

$$G(q) = \sum_{0 \leqq i < j < q} \mu^i \nu^j.$$

This result can be proved by induction on q.

Incidentally, it is known that if p is odd and G has a cyclic commutator subgroup then G is regular Huppert ((1967; page 322)). Thus if $q = p(b)$ in Lemma 2 then $G(p(b))$ is a multiple of $p(b)$.

The next result is about changing generators in the group.

LEMMA 3. *Let G be defined as in Theorem 1. Suppose that*

$$u = x^\alpha y^\beta z^\pi, \quad v = x^\gamma y^\delta z^\rho.$$

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

Set

$$\begin{aligned}\varepsilon &= M(\alpha)N(\delta)v^{\beta} - M(\gamma)N(\beta)v^{\delta}\\ \lambda &= (\mu^{\alpha}v^{\beta} - 1)\rho - (\mu^{\gamma}v^{\delta} - 1)\pi\\ \tau &= \varepsilon + \lambda.\end{aligned}$$

Then, with $z(\alpha) = z^{\alpha}$,

$$\begin{aligned}w = [v,u] &= z(\tau),\\ [w,u] &= z(\tau[\mu^{\alpha}v^{\beta} - 1]),\\ [w,v] &= z(\tau[\mu^{\gamma}v^{\delta} - 1]).\end{aligned}$$

PROOF. This follows from Lemma 1.

We are now in a position to prove Theorem 9. We adopt the notation of Theorem 2 and suppose that θ, defined by

$$\bar{x}^{\theta} = u = x^{\alpha}y^{\beta}x^{\pi}, \quad \bar{y}^{\theta} = v = x^{\gamma}y^{\delta}z^{\rho},$$

is an isomorphism from $\bar{G}$ to G in what follows.

Going to the first defining relation of $\bar{G}$ and applying Lemma 3 we have

$$(\bar{x}^{p(a)})^{\theta} = [v,u]^{\bar{R}p(\bar{r})} = z^{\tau\bar{R}p(\bar{r})}.$$

Then, since G is regular and $p(a) \geqq p(c)$, we have

$$(\bar{x}^{\theta})^{p(a)} = (x^{\alpha}y^{\beta})^{p(a)} = z^{A}$$

where $A = \alpha Rp(r) + \beta Sp(s + a - b)$. Thus

$$\alpha Rp(r) + \beta Sp(s + a - b) \equiv \tau\bar{R}p(\bar{r}) \bmod p(c) \tag{3}$$

Later on we shall show that this reduces to the first congruence of Theorem 2.

Complications appear in the congruence from the second defining relation since we might have $b < c$. Going one way

$$(\bar{y}^{p(b)})^{\theta} = [v,u]^{\bar{S}p(\bar{s})} = z^{\tau\bar{S}p(\bar{s})}.$$

Going the other, and applying Lemma 2 several times along the route, we have

$$(\bar{y}^{\theta})^{p(b)} = (x^{\gamma}y^{\delta}z^{\rho})^{p(b)} = x^{\gamma p(b)}y^{\delta p(b)}z^{B}$$

where

$$B = [M(\gamma)N(\delta) + \rho(\mu^{\gamma}v^{\delta} - 1)]G(p(b)).$$

The last two sets of equations imply that $x^{\gamma p(b)}$ is in G_2; consequently $\gamma = \gamma' p(a - b)$. Bringing these results together we have

$$\gamma' Rp(r) + \delta Sp(s) + B \equiv \tau\bar{S}p(\bar{s}) \bmod p(c). \tag{4}$$

To continue we have

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

$$[\bar{y}, \bar{x}, \bar{x}]^{\theta} = [v, u]^{\bar{M}p(\bar{m})} = z(\tau \bar{M}\, p(\bar{m})),$$

and

$$[\bar{y}, \bar{x}, \bar{x}]^{\theta} = [v, u, u] = z(\tau[\mu^{\alpha}v^{\beta} - 1]).$$

Since $(\tau, p) = 1$ it follows that

$$\mu^{\alpha}v^{\beta} - 1 \equiv \bar{M}\, p(\bar{m}) \bmod p(c). \tag{5}$$

Similarly working with $[\bar{y}, \bar{x}, \bar{y}]$ we get

$$\mu^{\gamma}v^{\delta} - 1 \equiv \bar{N} p(\bar{n}) \bmod p(c). \tag{6}$$

Relations (5) and (6) are the last two congruences of Theorem 2; in addition they can be used to simplify (3) and (4). Consider the right hand side of (3):

$$\tau p(\bar{r}) = [\varepsilon + (\mu^{\alpha}v^{\beta} - 1)\rho - (\mu^{\gamma}v^{\delta} - 1)\pi]p(\bar{r}).$$

By (5) and (6),

$$(\mu^{\alpha}v^{\beta} - 1)p(\bar{r}) \equiv \bar{M}\, p(\bar{r} + \bar{m}) \bmod p(c)$$

$$(\mu^{\gamma}v^{\delta} - 1)p(\bar{r}) \equiv \bar{N} p(\bar{n} + \bar{r}) \bmod p(c).$$

Then by the inequalities on the parameters for $\bar{G}$, $\bar{r} + \bar{m} \geqq c$ and $\bar{r} + \bar{n} \geqq c$. Thus (3) reduces to the first congruence of Theorem 2.

To reduce (4) begin with

$$B = [M(\gamma)N(\delta) + \rho(\mu^{\gamma}v^{\delta} - 1)]G(p(b)).$$

Recall that since G is regular we have $G(p(b)) = ip(b)$ for some integer i. Then by (6) and the fact that $b + \bar{n} \geqq c$ we have

$$(\mu^{\gamma}v^{\delta} - 1)G(p(b)) \equiv i\bar{N} p(b + \bar{n}) \equiv 0 \bmod p(c).$$

Furthermore since $\gamma = \gamma' p(a - b)$ we have $M(\gamma)G(p(b)) \equiv 0 \bmod p(c)$. Thus $B \equiv 0 \bmod p(c)$. As for the right hand side of (4):

$$\tau \bar{S} p(\bar{s}) = [\varepsilon + (\mu^{\alpha}v^{\beta} - 1)\rho - (\mu^{\alpha}v^{\delta} - 1)\pi]\bar{S} p(\bar{s}).$$

By (6) and the fact that $\bar{n} + \bar{s} \geqq c$, $(\mu^{\gamma}v^{\delta} - 1)p(\bar{s}) \equiv 0 \bmod p(c)$. Then by (5) and the congruence appearing in the defining conditions for $\bar{G}$,

$$(\mu^{\alpha}v^{\beta} - 1)\bar{S} p(\bar{s}) \equiv \bar{M}\, \bar{S} p(\bar{m} + \bar{s}) \equiv p(b) \bmod p(b).$$

Thus

$$\tau \bar{S} p(\bar{s}) \equiv \varepsilon \bar{S} p(\bar{s}) + \rho p(b) \bmod p(c),$$

and (4) reduces to the second congruence of Theorem 2.

This completes the proof of Theorem 9.

Incidentally, the last two congruences of Theorem 2,

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

$$(1 + Mp^m)^\alpha(1 + Np^n)^\beta = (1 + \bar{M}p^{\bar{m}}) \bmod p(c)$$

$$(1 + Mp^m)^\gamma(1 + Np^n)^\delta = (1 + \bar{N}p^{\bar{n}}) \bmod p(c),$$

are not difficult to analyze. For let K be the cyclic group of reduced residues modulo p^c and K_m be the subgroup of elements congruent to 1 modulo p^m. Then any integer of the form $1 + Mp^m$ where $(M, p) = 1$ generates K_m as the two congruences above form a simple system of equations in a cyclic group. This fact will be used frequently, without further mention, in what follows.

We shall close this section with a list of three elementary transformations that will be useful in the sequel. But first we need

LEMMA 4. *Let G be defined as in Theorem 1, ε as in Lemma 3, and $\Delta = \alpha\delta - \beta\gamma$. Set*

$$t(\alpha) = M \sum_{v=2}^{\alpha} \binom{\alpha}{v} (Mp^m)^{v-2}.$$

Then

$$\varepsilon p(r) \equiv \Delta p(r) \bmod p(c)$$

$$\varepsilon p(s) \equiv \Delta p(s) + \delta t(\alpha) p(b) \bmod p(c).$$

To prove this write out the sums involved and use the conditions: $r + n \geqq c$, $r + m \geqq c$, $s + n \geqq c$, $m + s = b$ if $b < c$.

LEMMA 5. *$G = \langle x, y \rangle$ be defined by $[Rp^r, Sp^s, Mp^m, Np^n]$. Then:*

(a) *If $u = x^\alpha$ and $v = y^\delta$ and $(\alpha\delta, p) = 1$ then $G = \langle u, v \rangle$ and is defined by*

$$[\delta' Rp(r),\ \alpha' Sp(s),\ \mu^\alpha - 1,\ v^\delta - 1]$$

where $\delta'\delta \equiv 1 \bmod p(c - r)$, $\alpha\alpha' \equiv 1 \bmod p(c - s)$ if $b \geqq c$ and $(\alpha', p) = 1$ if $b < c$.

(b) *If $u = x$ and $v = x^\gamma y$ where $\gamma = \gamma' p(a - b)$ then $G = \langle u, v \rangle$ and is defined by*

$$[Rp(r),\ \gamma' Rp(r) + Sp(s),\ Mp(m),\ \mu^\gamma v - 1].$$

(c) *If $u = xy^\beta$ and $v = y$ then $G = \langle u, v \rangle$ and is defined by*

$$[Rp(r) + \beta Sp(s + a - b),\ Sp(s),\ \mu v^\beta - 1,\ Np(n)]\ .$$

The results stated here are special cases of Theorem 2 for we can start with G defined by $[Rp^r, Sp^s, Mp^m, Np^n]$ and consider $\bar{G}$ as the group defined by the congruences. For example to obtain (a) set $\beta = \gamma = \pi = \rho = 0$ in Theorem 2. The first congruence is then

$$\alpha Rp(r) \equiv \varepsilon \bar{R}\, p(\bar{r}) \bmod p(c).$$

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

Thus $\bar{r} = r$ and, by Lemma 4

$$\alpha R p(r) \equiv \alpha\delta \bar{R} p(r) \bmod p(c).$$

So, $\bar{R} = \delta' R$. Similarly, in the second congruence of Theorem 2 we have $\bar{s} = s$ and, by Lemma 4,

$$\delta S p(s) \equiv \bar{S}[\alpha\delta p(s) + \delta t(\alpha) p(b)] \bmod p(c).$$

Consequently, $\bar{S} = \alpha' S$ where α' is the inverse of $(\alpha + t(\alpha)p(b-s))$ modulo $p(c-s)$. Continuing this way, we get Lemma 5.

Note finally that if G is defined as in Theorem 1 then we may (and shall) assume that $M = N = 1$. This follows from Lemma 5 (a) for there are integers α and δ with $(\alpha\delta, p) = 1$ such that

$$(1 + Mp^m)^\alpha - 1 \equiv p^m, \quad (1 + Np^n)^\delta - 1 \equiv p^n \bmod p^c.$$

2. Point of the classification theorems

We shall assume that $a > b$ throughout most of this sections; the case $a = b$ will be treated separately at the end. Note that if $a < b$ then, in the notation of Theorem 9, α and δ are prime to p for $\gamma = \gamma' p^{a-b}$, $\Delta = \alpha\delta - \beta\gamma$, and $(\Delta, p) = 1$.

Next, we shall split the groups of Theorem 1 into three classes by means of the following inequalities on r and s:

$$r \leqq s, \quad s < r < s + a - b, \quad s + a - b \leqq r \leqq c.$$

Let $\mathscr{F}$ be that class where $r \leqq s$. Then $b \geqq c$, we may assume $s = c$, and r is an invariant of the group. For if $b < c$ then, by the conditions of Theorem 1, $b = m + s \geqq m + r \geqq c$. Consequently the second congruence of Theorem 9 is

$$p^r(\gamma' R + \delta p^{s-r}) \equiv \varepsilon \bar{S} p^{\bar{s}} \bmod p^c,$$

and given δ we can choose γ' so that the left hand side here is 0 modulo $p(c)$. But this means we can find an isomorphic image of G where $\bar{s} = c$, i.e., we may assume $s = c$. Finally, by the first congruence of Theorem 9, r is an invariant of the group.

We shall first prove

THEOREM 10. *Let $\mathscr{F}$ be those groups in Theorem 1 where $r \leqq s$ and $a > b$. Then $b \geqq c$ and the distinct elements of $\mathscr{F}$ are given by*:

(a) $[Rp^r, 0, 0, p^n]$ $\quad r + n \geqq c,\ R \leqq p(c-n, c-r).$

(b) $[Rp^r, 0, p^m, p^n]$ $\quad r + m \geqq c,\ m < n \leqq q - 1$
$\quad q = c - r + m + a - b,\ R \leqq p(c-r, c-n, q-n).$

(c) $[p^r, 0, p^m, 0]$ $\quad r + m\ \ c,\ a \geqq -b \leqq r - m.$

The correspondence between this result and the theorems of the introduction

is this: First assume that $a - b > c$. Then parts (a) and (b) of Theorem 10 yield parts (a) and (b) of Theorem 2. When $a - b = c - k$ where $0 \leqq k \leqq c - 1$ then 10.a corresponds to 3.c, 10.b to 3.e, and 10.c to 3.a.

PROOF OF THEOREM 10. As mentioned we can assume $s = c$ and r is an invariant of the group, so $\mathscr{F}$ is included in the set of groups G defined by $[Rp^r, 0, p^m, p^n]$. Suppose $\bar{G}$, defined by $[\bar{R}p^r, 0, p^{\bar{m}}, p^{\bar{n}}]$ is isomorphic to G. Applying Lemma 4 to the first two congruences of Theorem 9 we get

$$\alpha Rp(r) \equiv \Delta\bar{R}p(r) \bmod p(c), \quad \gamma' Rp(r) \equiv 0 \bmod p(c).$$

Since $\gamma = \gamma' p(a - b)$ and, by the second congruence here, $\gamma' = \gamma'' p(c - r)$, we have $\Delta p(r) = (\alpha\delta - \beta\gamma)p(r) \equiv \alpha\delta p(r) \bmod p(c)$. Consequently the isomorphism congruences of Theorem 9 reduce to

$$\begin{aligned} R &\equiv \delta\bar{R} \bmod p(c - r), & \gamma' &\equiv 0 \bmod p(c - r) \\ \mu^\alpha \nu^\beta &\equiv \bar{\mu} \bmod p(c), & \mu^\gamma \nu^\delta &\equiv \bar{\nu} \bmod p(c) \end{aligned} \tag{1}$$

where $\mu = 1 + p^m$, $\nu = 1 + p^n$, $\bar{\mu} = 1 + p^{\bar{m}}$, and $\bar{\nu} = 1 + p^{\bar{n}}$.

We shall now split $\mathscr{F}$ into three parts: Let $\mathscr{F}_1$ be the subset of $\mathscr{F}$ where $n \leqq m$, $\mathscr{F}_2$ be the subset of $\mathscr{F}$ where $m < n < m + a - b + c - r$, and $\mathscr{F}_3$ be the subset where $m + a - b + c - r \leqq n \leqq c$.

If $n \leqq m$ we may assume, by Lemma 5.c, that $m = c$ in the defining relations. Thus $\mathscr{F}_1$ is included in the set of groups G defined by $[Rp^r, 0, 0, p^n]$. Furthermore if $\bar{G}$, defined by $[Rp^r, 0, 0, p^{\bar{n}}]$, is isomorphic to G then, by the last congruence in (1), $n = \bar{n}$. The isomorphism congruences for this case are then:

$$\begin{aligned} R &\equiv \delta\bar{R} \bmod p(c - r), & \gamma' &\equiv 0 \bmod p(c - r) \\ \nu^\beta &\equiv 1 \bmod p(c), & \nu^\delta &\equiv \nu \bmod p(c). \end{aligned} \tag{2}$$

That last congruence of (2) implies that $\delta \equiv 1 \bmod p(c - n)$. Placing $\delta = 1 + \omega p(c - n)$ in the first congruence we get

$$R - \bar{R} \equiv \omega\bar{R}p(c - n) \bmod p(c - r).$$

Thus if G and $\bar{G}$ are isomorphic then $R \equiv \bar{R} \bmod p(c - n, c - r)$. Conversely if R and $\bar{R}$ are so related the congruences in (2) are solvable. In sum the distinct members of $\mathscr{F}_1$ are given by $[Rp^r, 0, 0, p^n]$ where $r + n \mathscr{B} c$ and $R \leqq p(c-n, c-r)$.

Let us go on to $\mathscr{F}_2$, those groups where $m < n < m + a - b + c - r$. Since $(\alpha\delta, p) = 1$ and $\gamma = \gamma'' p(a - b + c - r)$ it follows, from (1), that m and n are invariants for these groups. The isomorphism congruences are:

$$\begin{aligned} R &\equiv \delta\bar{R} \bmod p(c - r), & \gamma' &\equiv 0 \bmod p(c - r) \\ \mu^{\alpha-1} &\equiv \nu^{-\beta} \bmod p(c), & \nu^{\delta-1} &\equiv \mu^{-\gamma} \bmod p(c). \end{aligned} \tag{3}$$

Define $f(m, n)$ modulo $p(c - n)$ by

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

$$\mu^{p(n-m)} \equiv \nu^{f(m,n)} \bmod p(c).$$

Then since $\gamma = \gamma'' p(a - b + c - r)$ the last congruence of (3) is equivalent to

$$\delta - 1 \equiv -\gamma'' f(m,n)p(q - n) \bmod p(c - n)$$

where $q = m + a - b + c - r$. Placing this in the first congruence of (3) we have

$$R - \bar{R} \equiv (-\gamma'' f(m,n)p(q - n) + \omega p(c - n))\bar{R} \bmod p(c - r).$$

Thus if the groups are isomorphic then $R \equiv \bar{R} \bmod p(q - n, c - n, q - r)$. Since the converse also holds the distinct members of $\mathscr{F}_2$ are given by $[Rp^r, 0, p^m, p^n]$ where r, m, n, and R satisfy the conditions stated in Theorem 10.b.

The family $\mathscr{F}_3$, those groups where $m + a - b + c - r \leqq n \leqq c$ reduces to the groups defined by $[p^r, 0, p^m, 0]$. To see this first apply Lemma 5.b to get $n = c$; then apply 5.a to get $R = 1$.

The classes $\mathscr{F}_i$ are disjoint. Suppose first that $\mathscr{F}_3$ is not empty. That is $a - b \leqq r - m$, a case that occurs when $a - b \leqq c - 1$. Then the groups of Theorem 10.b are distinct from those of 10.a or 10.c: For if $n < c$ the members of 10.b have generators that lie outside the centralizer of the commutator subgroup; the members of 10.a or 10.c have a generator that commutes with the commutator subgroup. If $n = c$ the group from 10.b appears similar to the one from 10.c. However the condition $c = n \leqq q - 1$ from 10.b implies that $r - m < a - b$; in 10.c we have $r - m \geqq a - b$. So, $\mathscr{F}_2$ is disjoint from $\mathscr{F}_1$ and $\mathscr{F}_3$. The last two congruences of (1) show that $\mathscr{F}_1$ and $\mathscr{F}_3$ are disjoint, for suppose the group in $\mathscr{F}_1$ defined by $[Rp^r, 0, 0, p^n]$ is isomorphic to $[p^r, 0, p^m, 0]$ from $\mathscr{F}_3$. Then, by (1)

$$(1 + p^n)^\beta \equiv (1 + p^m) \bmod p^c, \quad (1 + p^n)^\delta \equiv 1 \bmod p^c.$$

Since $(\delta, p) = 1$ the last congruence implies that $n = c$. But then $m = c$. However, by the conditions given for $\mathscr{F}_3$ in Theorem 10.c, $m \leqq r - (a - b)$. Since $r \leqq c$ and $a - b \geqq 1$ we have a contradiction. Thus $\mathscr{F}_1$ and $\mathscr{F}_3$ are disjoint.

If $\mathscr{F}_3$ is empty we have to show $\mathscr{F}_1$ and $\mathscr{F}_2$ are disjoint but this is an easy consequence of (1) and the conditions given in Theorem 10.

This completes the proof of Theorem 10.

Let $\mathscr{H}$ denote the set of groups in Theorem 1 where $s < r < s + a - b$. Note that the first two congruences of Theorem 9 imply that r and s are invariant for these groups.

This case includes a particularly complicated subcase, the one that occurs when $m < n < m + a - b$, so we shall introduce some notation for it. Let $a - b = c - k$. If $b \geqq c$ set

$$\mathscr{A} = \{(r, s, m, n) : s + m \geqq c, 0 < r - s < c - k, 0 < n - m < c - k\}.$$

If $b < c$ set

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

$$\mathscr{A} = \{(r,s,m,n) : c-b \leqq r-s < c-k,\ c-s \leqq n < b+c-k-s,\ m = b-s\}.$$

Next let

$$\mathscr{B}_1 = \{(r,s,m,n) : m < k \leqq s,\ r-n+m < k,\ r < b\},$$

$$\mathscr{B}_2 = \{(r,s,m,n) : s < k \leqq m,\ n-r+s < k,\ n-m < b-s\},$$

and

$$\mathscr{B}_3 = \{(r,s,m,n) : m, s < k,\ \min\{r-s, n-m\} < b-s\},$$

with the understanding that the last inequality for each of the $\mathscr{B}_i$ is to be suppressed if $b \geqq c$, and $m = b-s$ if $b < c$. Let $\mathscr{B}$ denote the union of all the $\mathscr{B}_i$. Note for later reference that each $\mathscr{B}_i$ is empty when $k \leqq 0$.

We can now state:

THEOREM 11. *Let $\mathscr{H}$ denote the set of groups in Theorem 1 where $s < r < s + a - b$. Set $m(n) = m - n + a - b$ and $s(r) = s - r + a - b$. Then the distinct elements of $\mathscr{H}$ are given by:*

(a) $[Rp^r, p^s, 0, p^n]$ $\quad s+n \geqq c,\ 0 < r-s < a-b,\ b \geqq c$
$R \leqq p(c-r, c-n)$

(b) $[Rp^r, Sp^s, p^m, p^n]$ $\quad (r,s,m,n) \in \mathscr{A},\ R \leqq p(c-r, c-n, m(n), s(r)),$
$S \leqq p(r-s, n-m, b-s)$ on $\mathscr{A} - \mathscr{B}$
$S \leqq p(c-m-s(r), c-s-m(n), b-s)$ on $\mathscr{B}$,
$Sp(m+s) \equiv p(b) \bmod p(c)$

(c) $[p^r, Sp^s, p^m, 0]$ $\quad r+m \geqq c,\ 0 < r-s < a-b,\ m \leqq c-a+b,$
$Sp(m+s) \equiv p(b) \bmod p(c),$
$S \leqq p(c-s, c-m-s(r), b-s).$

The correspondence between this result and the results stated earlier is this: If $b \geqq c$ and $a-b > c$ then Theorem 11.a corresponds to Theorem 2.6, 11.b to 2.d, and 11.c is empty. If $b \geqq c$ and $a-b = c-k$ where $0 \leqq k \leqq c-1$ then 11.a corresponds to 3.f, 11.b to Theorem 4, and 11.c to 3g. If $b < c$ and $a-b > c$ then 11.b corresponds to Theorem 6. If $b < c$ and $a-b = c-k$ where $0 \leqq k \leqq c-1$ the 11.b corresponds to Theorem 8 and 11.c to 7.b.

The proof of Theorem 11 is based on:

LEMMA 6. *Suppose that $0 < r-s < a-b$, G is defined by $[Rp^r, Sp^s, p^m, p^n]$, $\bar{G}$ is defined by $[\bar{R}p^r, \bar{S}p^s, p^{\bar{m}}, p^{\bar{n}}]$, and G is isomorphic to $\bar{G}$. Then the congruences of Theorem 9 are equivalent to the system:*

$$R \equiv \delta\bar{R} - \beta\bar{S}p(s+a-b-r) \bmod p(c-r)$$

$$S \equiv -\gamma'\bar{R}p(r-s) + \alpha\bar{S} + (t'+\rho)p(b-s) \bmod p(c-s)$$

$$\mu^\alpha\nu^\beta \equiv \bar{\mu} \bmod p(c), \quad \mu^\gamma\nu^\delta \equiv \bar{\nu} \bmod p(c),$$

where t' is an integer that depends on $\bar{S}$ and α.

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

PROOF. First replace ρ in Theorem 9 by $\delta\rho$. Then, applying Lemma 4 to the first two congruences of Theorem 9 we get

$$\begin{aligned} \alpha Rp(r) + \beta Sp(s + a - b) &\equiv \Delta \bar{R}p(r) \bmod p(c) \\ \gamma' Rp(r) + \delta Sp(s) &\equiv \Delta \bar{S}p(s) + \delta(t' + \rho)p(b) \bmod p(c), \end{aligned} \tag{4}$$

when $t' = t(\alpha)\bar{S}$. Eliminating $Rp(r)$ from the system one gets the congruence for S stated above. Then, placing this value of S in the first congruence of (4), we get the congruence for R. Conversely if R and S are given by Lemma 6 then the relations in (4) hold.

We begin the proof of Theorem 11 by considering $\mathscr{H}_1$, that subset of $\mathscr{H}$ where $n \leqq m$. Note that since $c \leqq n + s \leqq m + s$ we must have $b \geqq c$ for this subcase. Suppose then that G is in $\mathscr{H}_1$ and is defined by $[Rp^r, Sp^s, p^m, p^n]$. Since $n \leqq m$ we may assume, by Lemma 5.c, that $m = c$. Next, when $b > c$ the number α' is the inverse of α so we can take $S = 1$. In short, the defining relations of a group in $\mathscr{H}_1$ may be assumed to be of the form $[Rp^r, p^s, 0, p^n]$. By Lemma 6 the distinct members of the family are obtained (for fixed r, s, and n) by letting R run through the reduced residues from 1 to $p(c - n, c - r)$.

The above argument yields the groups of part (a) of Theorem 11. We shall skip part (b) for the moment and go on to the last part. Let $\mathscr{H}_3$ be the subset of $\mathscr{H}$ where $m + a - b \leqq n \leqq c$ starting with the usual defining relations we can assume, by Lemma 5.b and then Lemma 5.a that $n = c$ and $R = 1$. Thus G in $\mathscr{H}_3$ has defining relations of the form $[p^r, Sp^s, p^m, 0]$. If $\bar{G}$ defined by $[p^r, \bar{S}p^s, p^{\bar{m}}, 0]$ is isomorphic to G then, by Lemma 6, $\bar{m} = m$ and

$$\begin{aligned} 1 &\equiv \delta - \beta \bar{S}p(s + a - b - r) \bmod p(c - r) \\ S &\equiv \alpha \bar{S} - \gamma' p(r - s) + (t' + \rho)p(b - s) \bmod p(c - s) \\ \mu^{\alpha} &\equiv \mu \bmod p(c), \quad \mu^{\gamma} \equiv 1 \bmod p(c). \end{aligned}$$

The third and fourth congruence here are equivalent to

$$\alpha = 1 + \tau p(c - m), \quad \gamma' = \gamma'' p(c - (a - b + m)).$$

Thus the second congruence is equivalent to

$$S - \bar{S} \equiv \tau \bar{S}p(c - m) - \gamma'' p(c - m - s(r)) + (t' + \rho)p(b - s) \bmod p(c - s)$$

This shows that if G and $\bar{G}$ are isomorphic then, necessarily,

$$S \equiv \bar{S} \bmod p(c - m - s(r), c - s, b - s).$$

Conversely if S and $\bar{S}$ are so related these congruences are solvable and the corresponding groups are isomorphic.

The families $\mathscr{H}_1$ and $\mathscr{H}_3$ are disjoint: First if $\mathscr{H}_3$ is not empty then the defining inequalty $m + a - b \leqq n \leqq c$ is not vacuous; thus $m < c$ for $a > b$.

Second if we assume the group from $\mathscr{H}_1$ corresponding to $[Rp^r, p^s, 0, p^n]$ is somorphic to the one from $\mathscr{H}_3$ defined by $[p^r, Sp^s, p^m, 0]$ then, by the last two congruences of Lemma 6, $m = c$.

We now turn to Theorem 11.b. This part corresponds to the class $\mathscr{H}_2$, those groups where $0 < r - s < a - b$ and $0 < n - m < a - b$. By Lemma 6, m and n are invariant for these groups. Thus if the exponential parameters (r, s, m, and n) are fixed we have two other parameters, R and S, to consider. Generally speaking it is easy to find necessary conditions on R and S for isomorphism; complications arise in the sufficiency question.

We shall need:

LEMMA 7. *Suppose that* $0 < n - m < a - b$. *Let* $h(m, n)$ *and* $f(m, n)$ *be defined modulo* $p(c - n)$ *by*

$$\mu^{\theta(m,n)p(n-m)} \equiv \nu \bmod p(c),$$

$$\mu^{p(n-m)} \equiv \nu^{f(m,n)} \bmod p(c),$$

where $\mu = 1 + p^m$ *and* $\nu = 1 + p^n$. *Let* $H = h(m, n)$ *and*

$$F = h(n, m + a - b)f(m, m + a - b).$$

Then the last two congruences of Lemma 6 *are equivalent to the system*

$$\alpha \equiv 1 - \beta Hp(n - m) \bmod p(c - m),$$

$$\delta \equiv 1 - \gamma' Fp(m + a - b - n) \bmod p(c - n).$$

Furthermore if $m + a - b \leqq c$ *then* $1 - HF \equiv \bmod p(c - m - a + b)$.

This result is easy to verify, so we omit the proof.

Suppose then G is defined by R and S, $\bar{G}$ is defined by $\bar{R}\,\bar{S}$, and G is isomorphic to $\bar{G}$. Employing Lemmas 6 and 7 and recalling that $m(n) = m + a - b - n$, $s(r) = s + a - b - r$ we have

$$R - \bar{R} \equiv -\gamma' \bar{R} Fp(m(n)) + \omega p(c - n) - \beta \bar{S} p(s(r)) \bmod p(c - r),$$

$$S - \bar{S} \equiv -\gamma' \bar{R} p(r - s) + \tau p(c - m) - \beta H \bar{S} p(n - m) + (t' + \rho)p(b - s) \bmod p(c - s),$$

where ω and τ are integers. Consequently if G is isomorphic to $\bar{G}$ then $R \equiv \bar{R} \bmod p(f)$ and $S \equiv \bar{S} \bmod p(g)$ where

$$f = \min\{m(n), c - n, s(r), c - r\},$$

$$g = \min\{r - s, n - m, b - s\}.$$

However if R, $\bar{R}$ and S, $\bar{S}$ are so related the corresponding groups need not be isomorphic.

To go on to the converse problem suppose that $R - \bar{R} = y(1)p(f)$ and $S - \bar{S} = y(2)p(g)$ where $y(1)$ and $y(2)$ are integers and f and g are defined as above. Then the isomorphism congruences for the groups are

$$(5)\qquad \begin{aligned} y(1)p(f) &\equiv -\gamma'\bar{R}Fp(m(n) + \omega p(c - n) - \beta\bar{S}p(s(r)) \bmod p(c - r) \\ y(2)p(g) &\equiv -\gamma'\bar{R}p(r - s) + \tau p(c - m) - \beta H\bar{S}p(n - m) \\ &\quad + (t' + \rho)p(b - s) \bmod p(c - s). \end{aligned}$$

Now if the groups under consideration were isomorphic then the system (5) would be solvable for arbitrary values of $y(1)$ and $y(s)$, but this does not happen all the time.

We proceed by cases.

CASE 1. $s + a - b \geqq c$ and $m + a - b - n \geqq c - r$: Under these circumstances the first congruence of (5) reduces to

$$y(1)p(c - n, c - r) \equiv \omega p(c - n) \bmod p(c - r),$$

which is solvable for any given value of $y(1)$. The second congruence of (5) is also solvable for any given value of $y(2)$. Suppose for example that

$$g = \min\{n - m, b - s, r - s\} = r - s.$$

Go to the second congruence, choose and fix any τ and β, and then choose γ' so that

$$y(2)p(r - s) \equiv -\gamma'\bar{R}p(r - s) + \tau p(c - m) - \beta H\bar{S}p(n - m) \bmod p(c - s).$$

Finally choose ρ so that

$$(t' + \rho)p(b - s) \equiv 0 \bmod p(c - s).$$

The argument for the other two cases, $g = n - m$ or $g = b - s$, is similar. Thus the conditions $R \equiv \bar{R} \bmod p(f)$ and $S \equiv \bar{S} \bmod p(g)$ are sufficient here.

CASE 2. $s + a - b \geqq c$ and $m + a - b - n < c - r$: If the parameters satisfy these inequalities the first congruence of (5) reduces to

$$y(1)p(m(n), c - n) \equiv -\gamma'\bar{R}Fp(m(n)) + \omega p(c - n) \bmod p(c - r),$$

which is solvable for any given $y(1)$. However the variable one uses to solve it, γ' or ω, depends on the size of $m + a - b$ relative to c. If $m + a - b \geqq c$ the congruences reduce to the forms that appeared on case 1 and, again, the conditions $R \equiv \bar{R} \bmod p(f)$ and $S \equiv \bar{S} \bmod p(g)$ are sufficient.

So suppose that $m + a - b < c$. Then the congruences of (5) take the form

$$(6)\qquad \begin{aligned} y(1) &\equiv -\gamma'\bar{R}F + \omega p(c-(m+a-b)) \bmod p(c-r-m(n)) \\ y(2)p(g) &\equiv -\gamma'\bar{R}p(r-s) + \tau p(c-m) - \beta H\bar{S}p(n-m) \\ &\quad + (t'+\rho)p(b-s) \bmod p(c-s). \end{aligned}$$

Now the inequalities $s+a-b \geqq c$ and $m+a-b-n < c-r$ imply that $r-s < n-m$ so $g = \min\{r-s, b-s\}$. If $g = b-s$ the system (6) is solvable and the conditions on R, $\bar{R}$ and S, $\bar{S}$ are sufficient.

The final subcase of case 2 occurs when $m+a-b < c$ and $r < b$. According to the first congruence of (6) we can take $y(1) = 0$. Doing so and then eliminating γ' from (6) we get

$$\begin{aligned} y(2)F \equiv \tau Fp(c-m-r+s) - \beta FH\bar{S}p(n-m-r+s) + (t'+\rho)Fp(b-r) \\ -\omega p(c-m-a+b) + \lambda p(c-r-m(n)) \bmod p(c-r). \end{aligned}$$

That is $y(2) \equiv 0 \bmod p(h)$ where

$$h = \min\{n-m-r+s, b-r, c-m-a+b, c-r-m(n)\}.$$

Recall that at this stage G is defined by R and S, $\bar{G}$ is defined by $\bar{R}$ and $\bar{S}$, $R \equiv \bar{R} \bmod p(m(n))$ and $S = \bar{S} + y(2)p(r-s)$. Thus if $0 \leqq y(2) < p(h)$ then G and $\bar{G}$ are not isomorphic; if $y(2) \geqq p(h)$ they are. Next if $0 \leqq y(2) < p(h)$ then

$$1 \leqq \bar{S} + y(2)p(r-s) < p(r-s) + (p(h)-1)p(r-s) = p(h+r-s)$$

where

$$h+r-s = \min\{n-m, b-s, c-m-s(r), c-s-m(n)\}.$$

Finally we have

$$s+a-b \geqq c \text{ so } n-m \geqq c-s-(m+a-b-n) = c-s-m(n)$$

and the distinct groups of this subcase are given by the R and S where $R \leqq p(m(n))$ and $S \leqq p(b-s, c-s-m(n), c-m-s(r))$.

Cases 1 and 2 deal with the congruences in (5) when $s+a-b \geqq c$. The one exception to the rule $S \leqq p(r-s, n-m, b-s)$ occurs in the last part of case 2 when $s+a-b \geqq c$, $m+a-b-n < c-r$, $m+a-b < c$ and $r < b$. Recalling that $a-b = c-k$, the exceptional case occurs when

$$s > k, \quad m-n+r < k, \quad m < k \text{ and } r < b\,.$$

This is the set $\mathscr{B}_1$ that was defined in the paragraph preceeding the statement of Theorem 11.

CASE 3. $s+a-b < c$ and $m+a-b \geqq c$: Consider the first congruence in (5). Since $m(n) = m+a-b-n \geqq c-n$ the γ' term there can be combined with the ω term to give a congruence of the form

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

$$y(1)p(c-n, s(r)) \equiv \omega p(c-n) - \beta\bar{S}p(s(r)) \bmod p(c-r).$$

Now if $c-n \leqq s(r)$ then the system consisting of this congruence and the second congruence of (5) is solvable and the necessary conditions are also sufficient.

So suppose that $c-n \geqq s(r)$. Then the congruences of (5) take the form

$$\begin{aligned} y(1) &\equiv \omega p(c-n-s(r)) - \beta\bar{S} \bmod p(c-s-a+b) \\ y(2)p(g) &\equiv -\gamma'\bar{R}p(r-s) + \tau p(c-m) - \beta H\bar{S}p(n-m) \\ &\quad + (t'+\rho)p(b-s) \bmod p(c-s). \end{aligned}$$

Now the conditions $m+a-b \geqq c$ and $c-n > s+a-b-r$ imply that $n-m < r-s$. Thus $g = \min\{n-m, b-s\}$. If $g = b-s$ this system is solvable and the necessary conditions are sufficient. The final subcase of case 3 occurs when $n-m < b-s$. The argument here is similar to the one given for the last part of case 2.

The total set of inequalities governing the exceptional subcase of case 3 is:

$$s+a-b < c,\ m+a-b \geqq c,\ c-n \geqq s+a-b-r,\ n-m < b-s.$$

Setting $a-b = c-k$ this translates to the set $\mathscr{B}_2$ that was defined earlier.

CASE 4. $s+a-b \leqq c$ and $m+a-b < c$: It is obvious that the system (5) is solvable if $g = \min\{n-m, r-s, b-s\} = b-s$. So let us assume that $g \neq b-s$, say $g = r-s$. Then $r-s \leqq n-m$, $m(n) \leqq s(r)$ and (5) is equivalent to

$$\begin{aligned} y(1) &\equiv -\gamma'\bar{R}F + \omega p(c-m-a+b) - \beta\bar{S}p(s-r+n-m) \bmod p(c-r-m(n)) \\ y(2) &\equiv -\gamma'\bar{R} + \tau p(c-m-r+s) - \beta H\bar{S}p(s-r+n-m) \\ &\quad + (t'+\rho)p(b-r) \bmod p(c-r). \end{aligned}$$

According to the first congruence we can assume that $y(1) = 0$. Doing so and then eliminating γ' we get

$$\begin{aligned} y(2)F &\equiv \tau p(c-m-r+s) - \omega p(c-m-a+b) + \beta\bar{S}(1-HF)p(n-m+s-r) \\ &\quad + F(t'+\rho)p(b-r) + \lambda p(c-r-m(n)) \bmod p(c-r). \end{aligned}$$

Examining the exponents of p here we have $c-m-r+s > c-m-a+b$ for we have $r-s < a-b$. Furthermore, by the last part of Lemma 7, $1-HF \equiv 0 \bmod p(c-m-a+b)$. Thus $y(2) \equiv \bmod p(i)$ where

$$i = \min\{c-m-a+b, c-r-m(n), b-r\}.$$

But then, as before, $S = \bar{S} + y(2)p(r-s)$, the underlying groups are not isomorphic if $y(2) < p^i$, and the distinct groups are obtained by letting S run through the reduced residues less than $p(b-s, c-s-m(n), c-m-s(r))$.

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

The argument for the subcase $\min\{n-m, r-s, b-s\} = n-m$ is similar to the one above.

Finally, the class $\mathscr{H}_2$ is disjoint from $\mathscr{H}_1$ and $\mathscr{H}_3$. This follows from the last two congruence of Lemma 6 and the conditions on the parameters.

This completes the proof of Theorem 11.

THEOREM 12. *Suppose $a > b$ and let $\mathscr{L}$ be the groups in Theorem 1 where $s + a - b \leqq r \leqq c$. Then the distinct elements of $\mathscr{L}$ are given by:*

(a)	$[0, p^s, 0, p^n]$	$s + n \geqq c,\ n \leqq s + a - b,\ b \geqq c.$
(b)	$[0, Sp^s, p^m, p^n]$	$s + n \geqq c,\ s + a - b - c < n - m < a - b$
		$Sp(m + s) \equiv p(b) \bmod p(c)$
		$S \leqq p(c - m, b - s, c - s - m - a + b + n)$
(c)	$[0, Sp^s, p^m, 0]$	$m \leqq c - a + b,\ Sp(m + s) \equiv p(b) \bmod p(c)$
		$S \leqq p(c - m, c - s, b - s).$

The correspondence here to earlier theorems is this: If $b \geqq c$ then 12.a corresponds to 3.b, 12.b to 3.h and 12.c to 3.d. If $b < c$ then 12.b corresponds to 7.c and 12.c to 7.a.

To start the proof of Theorem 12 we apply Lemma 5.c and conclude that $\mathscr{L}$ is included in the set of groups defined by $[0, Sp^s, p^m, p^n]$. Furthermore, by Theorem 9 and Lemma 4, the isomorphism congruences are

$$\begin{aligned} &\beta Sp(s + a - b) \equiv 0 \bmod p(c), \\ &\delta Sp(s) \equiv \alpha\delta \bar{S}p(s) + (\delta t(\alpha) + \rho)p(b) \bmod p(c), \\ &\mu^{\alpha}\nu^{\beta} \equiv \bar{\mu} \bmod p(c), \quad \mu^{\gamma}\nu^{\delta} \equiv \bar{\nu} \bmod p(c). \end{aligned} \tag{7}$$

Let $\mathscr{L}_1$ be those groups in $\mathscr{L}$ where $c - (s + a - b) + n \leqq m$. Then, by Lemma 5.c, we may assume that the defining relations for this subclass are $[0, Sp^s, 0, p^n]$. Next we must have $b \geqq c$ for if $b < c$ then $m + s = b$; but $m = c$. Finally since $b \geqq c$ the number α' of Lemma 5.a is the inverse of α modulo p, so we may assume that $\alpha = 1$.

Let $\mathscr{L}_2$ be those groups where $m < c - (s + a - b) + n$ and $n < m + a - b$; i.e., $a - b - (c - s) < n - m < a - b$. The congruences of (7) imply that m and n are invariants and the isomorphism congruences are

$$\begin{aligned} \beta &= \beta' p(c - s - a + b) \\ \delta(S - \alpha\bar{S}) &\equiv (\delta t(\alpha) + \rho)p(b - s) \bmod p(c - s) \\ \mu^{\alpha-1} &\equiv \nu^{-\beta} \bmod p(c), \quad \nu^{\delta-1} \equiv \mu^{-\gamma} \bmod p(c). \end{aligned}$$

Consequently,

$$\alpha - 1 \equiv -\beta' H p(c - s - a + b + n - m) \bmod p(c - m)$$

https://doi.org/10.1017/S1446788700020486 Published online by Cambridge University Press

where H is a number prime to p. So if the groups are isomorphic then $S \equiv \bar{S} \bmod p(i)$ where

$$i = \min\{c - s - a + b + n - m, c - m, b - s\}$$

the converse also holds.

Let $\mathscr{L}_3$ be those groups where $a - b \leqq n - m \leqq c$. Then, by Lemma 5.b, this class is included in the groups defined by $[0, Sp^s, p^m, 0]$ and it is not difficult to verify that the distinct groups correspond to the S where

$$S \leqq p(c - m, c - s, b - s).$$

The usual arguments show that the classes $\mathscr{L}_i$ are disjoint.

Let $\mathscr{K}$ denote the set of groups of Theorem 1 when $a = b$. This case is similar to the one that appeared in Theorem 12; some details of the proof are different but the final results are nearly identical. To begin $\mathscr{K}$ is included in the set of groups defined by $[0, Sp^s, p^m, p^n]$. To prove this start with G defined by $[Rp^r, Sp^s, p^m, p^n]$, apply Lemma 5.c to show that one may assume $r \geqq s$, and then apply it once more to eliminate the p^r term. Furthermore the isomorphism m congruences are the same as those in (7). However the argument branches into two cases: $s < c$ and $s = c$.

If $s < c$ one gets three cases which are analogous to the $\mathscr{L}_i$ of Theorem 12. Furthermore, as long as one adds the condition $s < c$, the final results are the same as those stated in Theorem 12. The cases of Theorem 12 yield those of Theorem 5 for $s < c$.

If $s = c$ one gets a set of groups defined by $[0, 0, p^m, p^n]$. The subset here where $n \leqq m$ can be reduced, by Lemma 5, to the $[0, 0, p^m, 0]$; the subset where $m < n$ to $[0, 0, 0, p^n]$. Then one can show, by switching generators, that the groups of the last two classes are isomorphic when $m = n$. In short the $a = b$, $s = c$ case reduces to the set of groups $[0, 0, p^m, 0]$ where $1 \leqq m \leqq c$. This can be incorporated into our final results by taking $s = c$ in Theorem 5.b.

References

B. G. Basmaji (1969), 'On the isomorphisms of two metacyclic groups', *Proc. Amer. Math. Soc.* **22**, 175–182.

B. Huppert (1967), *Endliche Gruppen* (Die Grundlehren der math. Wissenschaften, Band 134 Springer-Verlag, Berlin and New York, 1967).

G. Szekeres (1965), *Metabelian groups with two generators*, Proc. Inter. Conf. Theory of Groups, Austral. Nat. Univ., Canberra, 1965, 323–346; (Gordon and Breach, New York, 1967).

Department of Mathematics
University of California
Los Angeles, 90024
U. S. A.