TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 152, December 1970

METABELIAN p-GROUPS OF MAXIMAL CLASS[1]

BY
R. J. MIECH

Abstract. This paper deals with the classification of the metabelian p-groups of maximal class and order p^n where p is odd and, roughly, $n \geqq 2p$.

This paper deals with the classification of the metabelian p-groups of maximal class and order p^n where p is an odd prime and, roughly, $n \geqq 2p$. It also contains a result on the order of the automorphism groups of these groups. Some descriptive material must be developed before the main results, Theorems 4 to 8 below, can be stated.

To begin let G be a group, $G_2 = [G, G]$ be the commutator subgroup of G, and $G_{i+1} = [G_i, G]$ for $i \geqq 2$. Then, by definition, G is metabelian if G_2 is abelian. The group G, of order p^n, is of maximal class if $G > G_2 > \cdots > G_n = 1$ where $|G:G_2| = p^2$ and $|G_i:G_{i+1}| = p$ for $i = 2, 3, \ldots, n-1$. If G is of maximal class the subgroup G_1 is defined by: G_1 is the largest subgroup of G such that $[G_1, G_2] \leqq G_4$. The general theory of p-groups of maximal class can be found in [2, p. 361].

Most of the known results on the classification of metabelian p-groups have been derived under the assumption that G or G_2 is of exponent p [4]. The starting point of this paper is the following result of Blackburn:

THEOREM 1. *Let G be a metabelian p-group of maximal class and order p^n where $n \geqq p+1$. Then*

$$[G_1, G_i] \leqq G_{n-p+i}, \qquad i = 1, 2, \ldots, p.$$

This follows from Theorem 3.10 of [1] and the fact that G/G_2 is elementary abelian.

If we take $i=2$ in Theorem 1 we get $[G_1, G_2] \leqq G_{n-p+2}$. Thus, by the general theory, there is an integer k with $0 \leqq k \leqq p-2$ such that $[G_1, G_2] = G_{n-k}$, and this integer k is an invariant of the group G. The structure of the groups in question can be described in terms of this invariant k. We have

THEOREM 2. *Let G be a metabelian p-group of maximal class and order p^n where $n \geqq p+1$, and suppose that $[G_1, G_2] = G_{n-k}$ where $0 \leqq k \leqq p-2$. Let s be an element of G not in G_1, s_1 be an element of G_1 not in G_2, and $s_i = [s_{i-1}, s]$ for $i = 2, 3, \ldots, n$.*

Received by the editors October 30, 1969.

AMS subject classifications. Primary 2027, 2040.

Key words and phrases. Metabelian p-groups, p-groups of maximal class.

[1] The preparation of this paper was supported in part by the NSF Grant #GP-13164.

Copyright © 1970, American Mathematical Society

Then:

(1) $G=\langle s, G_1\rangle$ *and* $G_i=\langle s_i, G_{i+1}\rangle$ *for* $i=1, 2, \ldots, n$;

(2) *there are integers* $a(n-k), \ldots, a(n-1)$ *with* $a(n-k)\not\equiv 0 \bmod p$ *such that*

$$[s_1, s_2] = s_{n-k}^{a(n-k)} s_{n-k+1}^{a(n-k+1)} \cdots s_{n-1}^{a(n-1)};$$

(3) *there are integers* w *and* z *such that*

$$s^p = s_{n-1}^w \quad \textit{and} \quad s_1^{\binom{p}{1}} s_2^{\binom{p}{2}} \cdots s_p^{\binom{p}{p}} = s_{n-1}^z;$$

(4) *for* $i=2, 3, \ldots, n-1$,

$$s_i^{\binom{p}{1}} s_{i+1}^{\binom{p}{2}} \cdots s_{i+p-1}^{\binom{p}{p}} = 1.$$

The first part of the conclusion is contained in the general theory. The other three parts are not difficult to establish and this will be done later. The main point of this theorem is that our groups can be described in terms of a set of parameters

$$(a(n-k), a(n-k+1), \ldots, a(n-1), w, z).$$

Conversely, given any set of such parameters one can usually prove that there is a metabelian p-group of maximal class and order p^n having the stated parameters.

The main problem that arises at this point is the one of determining the distinct, nonisomorphic groups in this collection. It is solvable for the case $n \geqq 2k+3$, and this paper deals with the solution. The case $(p+1) \leqq n < 2k+3$ is still open.

We have one invariant, k; several others arise. Among these are a positive integer s and an s-tuple of integers $(j_1, \ldots, j_s)$ having the properties

(1) $j_s \geqq 0$,

(2) if $s>1$ then $j_i \geqq 2$ for $i=1, 2, \ldots, s-1$,

(3) $j_1+j_2+\cdots+j_s \leqq k-1$.

A discussion of the origin of the $(j_1, \ldots, j_s)$ will be given in the next few paragraphs. Next, if $0 \leqq k \leqq p-3$ we have the invariants (λ, τ) where $(\lambda, \tau)=(0, 0)$, $(0, 1)$, or $(1, 0)$. These are related to the parameters z and w of Theorem 2 and refer to the values assumed by the corresponding parameters, $\bar{z}$ and $\bar{w}$, of any isomorphic image of G. When $(\lambda, \tau)=(0, 0)$ we have $z \equiv w \equiv 0 \bmod p$ and must have $\bar{z} \equiv \bar{w} \equiv 0$; when $(\lambda, \tau)=(0, 1)$ we have $z \equiv 0$, $w \not\equiv 0$ and must have $\bar{z} \equiv 0$, $\bar{w} \not\equiv 0$; when $(\lambda, \tau)=(1, 0)$ we have $z \not\equiv 0$, w unspecified, must have $\bar{z} \not\equiv 0$, and may take $\bar{w} \equiv 0$. Finally, if $k=p-2$ we have the invariant Δ, where $\Delta=0$ or 1. It refers to the parameters $a(n-k)$, z, w. When $\Delta=0$ we have $z^2-4a(n-k)w \equiv 0$ and this congruence must hold for all isomorphic images of G. When $\Delta=1$ we have $z^2-4a(n-k)w \not\equiv 0$ and this congruence must hold for all isomorphic images of G. These invariants

$$(k, j_1, \ldots, j_s, \lambda, \tau) \quad \text{for } 1 \leqq k \leqq p-3,$$
$$(k, j_1, \ldots, j_s, \Delta) \quad \text{for } k = p-2,$$

are the basic ones we shall use in the classification of our groups.

We need a set of functions to characterize the $(j_1, \ldots, j_s)$. To this end let S_n^m be a Stirling number of the first kind. These numbers are defined by

$$(x)_n = x(x-1)\cdots(x-n+1) = \sum_{m=1}^{n} S_n^m x^m.$$

Let $\mathcal{S}_n^m$ be a Stirling number of the second kind. These are defined by

$$x^n = \sum_{m=1}^{n} \mathcal{S}_n^m (x)_m.$$

It is known that [3, pp. 146, 176]

$$(-1)^{n-m}\frac{m!}{n!}\mathcal{S}_n^m = \sum{}^* \frac{1}{v_1\cdots v_m},$$

$$\frac{m!}{n!}\mathcal{S}_n^m = \sum{}^* \frac{1}{v_1!\cdots v_m!},$$

where the * on the summation symbols means that the summation is extended over all those m-tuples of integers $(v_1, \cdots, v_m)$ such that $v_i \geqq 1$ for $i=1, 2, \ldots, m$ and $v_1+\cdots+v_m=n$.

To continue, let

$$g(n, t) = \sum{}^* \frac{1}{r_1\cdots r_t}$$

where the * on the summation symbol means that the summation is extended over all those integral t-tuples $(r_1, \ldots, r_t)$ such that $r_i \geqq 2$ for $i=1, 2, \ldots, t$ and $r_1+\cdots+r_t=n+t$. Next, let

$$e(0) = 1, \qquad e(n) = \sum_{t=1}^{n} (-1)^t g(n, t) \quad \text{for } n \geqq 1.$$

These numbers, the $e(n)$, are, except for sign, the coefficients of the Bernoulli polynomial of the second kind. It is known that

$$\sum_{m=0}^{n-1} \frac{e(m)}{n-m} = 0 \quad \text{for } n > 1 \text{ [3, p. 266].}$$

Next define a function $D(M, l)$ for integral M and l by

$$D(M, l) = (-1)^l \sum_{v=0}^{l} e(l-v)(-1)^v \frac{M!}{(M+v)!} S_{M+v}^M.$$

Note for later purposes that $D(M, 0)=1$ for any positive integer.

Incidentally, although $D(M, l)$ is defined as a rational number we will wish to consider it as an element of $GF(p)$, the finite field with p elements. Since, in our applications, we will have $0 \leqq l \leqq k-1$ it is easy to check that $D(M, l)$ is well defined in $GF(p)$. The Stirling number component of the sum defining $D(M, l)$ is

$$(-1)^v \frac{M!}{(M+v)!} S_{M+v}^M = \sum_{v_1+\cdots+v_M=M+v;\, v_i\geqq 1} \frac{1}{v_1\cdots v_M}.$$

Since $\nu_i \geqq 1$ and $\nu_1 + \cdots + \nu_M = M + \nu$, the maximum value any ν_i can attain is $\nu + 1 \leqq l + 1 \leqq k \leqq p - 2$, so this sum is well defined in $GF(p)$. Similar considerations, starting from the definition of the numbers $g(n, t)$, lead to the conclusion that $e(l-\nu)$, hence $D(M, l)$, is well defined in $GF(p)$.

We can now describe how the invariants $(j_1, \ldots, j_s)$ arise. Let $a(n-k)$, $a(n-k+1), \ldots, a(n-1)$ be a set of numbers in $GF(p)$ with $a(n-k) \neq 0$. (We are now working in $GF(p)$ and all the equations that follow are equations in this field.) Define a new sequence $a_1(l)$ for $l = 0, 1, \ldots, k-1$ by

$$a(n-k+l)/a(n-k) = D(M, l) + a_1(l)$$

where $M = n-k-1$. If $a_1(l) = 0$ for all l, take $s = 1, j_s = j_1 = 0$, and stop. If there are positive integers l for which $a_1(l) \neq 0$, let j_1 be the smallest of them. If $j_1 = 1$ or $j_1 = k-1$, take $s = 1$ and stop. If not, i.e. $1 < j_1 < k-1$, continue.

In order to continue let

$$\begin{aligned} \omega(i) &= 0 && \text{if } i = 0 \\ &= j_1 + \cdots + j_i && \text{if } i \geqq 1. \end{aligned}$$

Then, at the dth step we have a sequence of integers $j_1, \ldots, j_d$ with $1 < j_i < k-1-\omega(i)$ for $i = 1, \ldots, d$, and a set of numbers $a_d(l)$ for $l = 0, \ldots$ $k-1-\omega(d-1)$ such that

$$a_d(0) = a_d(1) = \cdots a_d(j_d - 1) = 0, a_d(j_d) \neq 0.$$

We continue by defining $a_{d+1}(l)$ by

$$(1) \qquad a_d(j_d + l)/a_d(j_d) = D(M + \omega(d), l) + a_{d+1}(l)$$

for $l = 0, 1, \ldots, k-1-\omega(d)$. If all the numbers $a_{d+1}(l)$ are 0 we take j_{d+1} to be 0. If there are positive integers l such that $a_{d+1}(l) \neq 0$ we take j_{d+1} to be the smallest of them.

The process stops at the sth step when $d+1 = s$ in (1) and all the numbers $a_s(l)$ are 0 or j_s, the smallest integer l such that $a_s(l) \neq 0$, does exist and is equal to 1 or $k-1-\omega(s-1)$.

In sum, given n, k, and the sequence $a(n-k), \ldots, a(n-1)$ we get a unique sequence

$$a(n-k), a_1(j_1), \ldots, a_s(j_s), a_s(j_s+1), \ldots, a_s(k-1-\omega(s-1))$$

by this scheme. Conversely any given sequence of this last type determines a unique sequence of the first type. If we let $a(n-k) = a_0(j_0)$, $P(t) = a_0(j_0) \cdots a_t(j_t)$, $j_0 = 0$, and $\omega(t) = j_0 + j_1 + \cdots + j_t$ the specific equations are

$$a(n-k+\omega(t)+l) = \sum_{\nu=0}^{t} P(\nu) D(M+\omega(\nu), \omega(t) - \omega(\nu) + l)$$

for $t = 0, 1, \ldots, s-1$ and $l = 0, 1, \ldots, j_{t+1} - 1$, and

$$a(n-k+\omega(s-1)+l)) = \sum_{\nu=0}^{s-1} P(\nu) D(M+\omega(\nu), \omega(s-1) - \omega(\nu) + l)) + P(s-1) a_s(l)$$

for $l = j_s, \ldots, k-1-\omega(s-1)$.

These equations can be established by a simple computation. Their chief value is that they permit us to speak of the group defined in terms of the parameters $a(n-k), \ldots, a(n-1), w, z$, as in Theorem 2, as the group defined in terms of the parameters $a(n-k), a_1(j_1), \ldots, a_{s-1}(j_{s-1}), a_s(j_s), a_s(j_s+1), \ldots, a_s(k-1-\omega(s-1))$, w, z.

In short, we shall see that the metabelian p-groups of maximal class and order p^n with $n \geqq \max\{p+1, 2k+3\}$ can be classified, first, by the invariants

$$\begin{aligned} (0, \lambda, \tau) &\quad \text{if } [G_1, G_2] = G_n = 1, \\ (k, j_1, \ldots, j_s, \lambda, \tau) &\quad \text{if } [G_1, G_2] = G_{n-k}, 1 \leqq k \leqq p-3, \\ (k, j_1, \ldots, j_s, \Delta) &\quad \text{if } [G_1, G_2] = G_{n-k}, k = p-2, \end{aligned}$$

where $(\lambda, \tau) = (0, 0), (0, 1)$, or $(1, 0)$, $\Delta = 0$ or 1, and $(j_1, \ldots, j_s)$ is any set of integers such that $j_s \geqq 0, j_i \geqq 2$ for $i = 1, 2, \ldots, s-1$ if $s > 1$, $j_1 + \cdots + j_s \leqq k-1$. The distinct groups having these invariants will then be given by a set of parameters $(a(n-k), a_1(j_1) \cdots, w, z)$.

For the sake of brevity, $\mathscr{M}$ will denote the set of metabelian p-groups of maximal class and order p^n with $n \geqq \max\{p+1, 2k+3\}$. We shall also assume that the conditions on $(j_1, \ldots, j_s)$, (λ, τ) and Δ given above also hold whenever these numbers are mentioned in the sequel. Finally, we shall always assume that $n \geqq p+1$.

The following result is known:

THEOREM 3. *Let* $(\lambda, \tau) = (0, 0), (0, 1)$, *or* $(1, 0)$. *Then the set of distinct groups in* $\mathscr{M}$ *having the invariants* $(0, \lambda, \tau)$ *are given by the set of parameters* (z, w) *where*

$$z = \lambda \cdot g^l, \quad l = 0, 1, \ldots, d-1, \qquad w = \tau;$$

g is a primitive root modulo p and $d = (n-2, p-1)$. *The number of such groups is equal to* $2 + (n-2, p-2)$.

A variant of this theorem is in Blackburn [1, p. 88]; it will also be proved here.

The next four theorems are the main results of this paper. The four cases arise from the considerations: $1 \leqq k \leqq p-3$ or $k = p-2$; $j_s = 1$ or $j_s \neq 1$.

THEOREM 4. *Let* $(k, j_1, \ldots, j_s, \lambda, \tau)$ *be a set of integers with* $1 \leqq k \leqq p-3$ *and* $j_s = 1$. *Let* $\omega = 0$ *if* $s = 1$ *and* $\omega = j_1 + \cdots + j_{s-1}$ *if* $s \geqq 2$. *Then the distinct groups in* $\mathscr{M}$ *having the invariants* $(k, j_1, \ldots, j_s, \lambda, \tau)$ *are given by the set of parameters*

$$\{(a(n-k), a_1(j_1), \ldots, a_s(1), a_s(2), \ldots, a_s(k-1-\omega), w, z)\}$$

where

$$\begin{aligned} a(n-k) &= 1, && \\ a_t(j_t) &= \alpha_t, & \alpha_t &= 1, \ldots, p-1, & t &= 1, 2, \ldots, s-1, \\ a_s(1) &= 1, && \\ a_s(l) &= \beta_l, & \beta_l &= 0, 1, \ldots, p-1, & l &= 2, \ldots, k-1-\omega, \\ z &= \lambda \cdot \gamma, & \gamma &= 1, \ldots, p-1, && \\ w &= \tau \cdot \delta, & \delta &= 1, \ldots, p-1. && \end{aligned}$$

In addition, the number of distinct groups in $\mathcal{M}$ having the invariants $(k, j_1, \ldots, j_s, \lambda, \tau)$ is equal to $(p-1)^{s-1+\lambda+\tau} \cdot p^J$ where $J = j_1 + \cdots + j_s$.

THEOREM 5. *Let $(k, j_1, \ldots, j_s, \lambda, \tau)$ be a set of integers with $1 \leqq k \leqq p-3$ and $j_s \neq 1$. Let*

$$\begin{aligned} \varepsilon &= 0 \quad \text{if } j_s = 0, \\ &= 1 \quad \text{if } j_s \geqq 2; \end{aligned}$$

$$j_{s+1} = \lambda(n-2), \qquad j_{s+2} = \tau(2n-k-5).$$

Let g be a primitive root modulo p. Let $(k_1, \ldots, k_{s+2})$ be the set of integral $(s+2)$-tuples defined by

$$0 \leqq k_1 < (p-1, j_1),$$

$$0 \leqq k_i < ((p-1)j_i/(p-1, j_1, \ldots, j_{i-1}), p-1), \qquad i = 2, \ldots, s+2.$$

Then the distinct groups in $\mathcal{M}$ having the invariants $(k, j_1, \ldots, j_s, \lambda, \tau)$ are given by the set of parameters

$$\{(a(n-k), a_1(j_1), \ldots, a_s(j_s), w, z)\}$$

where

$$\begin{aligned} a(n-k) &\equiv 1, \\ a_t(j_t) &\equiv g^{k_t}, \qquad t = 1, 2, \ldots, s-1, \\ a_s(j_s) &= \varepsilon g^{k_s}, \\ z &= \lambda \cdot g^{k_{s+1}}, \\ w &= \tau \cdot g^{k_{s+2}}. \end{aligned}$$

In addition, the number of distinct groups in $\mathcal{M}$ having the invariants $(k, j_1, \ldots, j_s, \lambda, \tau)$ is equal to $dp^{s-2+\varepsilon+\lambda+\tau}$ where

$$d = (j_1, \ldots, j_s, \lambda(n-2), \tau(2n-k-5), p-1).$$

THEOREM 6. *Let $(k, j_1, \ldots, j_s, \Delta)$ be a set of integers with $k = p-2$ and $j_s = 1$. Let $\omega = 0$ if $s = 1$ and $\omega = j_1 + \cdots + j_{s-1}$ if $s \geqq 2$. Then the distinct groups in $\mathcal{M}$ having the invariants $(k, j_1, \ldots, j_s, \Delta)$ are given by the set of parameters*

$$\{(a(n-k), a_1(j_1), \ldots, a_s(1), a_s(2), \ldots, a_s(k-1-\omega), w, z)\}$$

where

$$\begin{aligned} a(n-k) &= 1, \\ a_t(j_t) &= \alpha_t, \qquad \alpha_t = 1, \ldots, p-1, \qquad t = 1, 2, \ldots, s-1, \\ a_s(1) &= 1, \\ a_s(l) &= \beta_l, \qquad \beta_l = 0, 1, \ldots, p-1, \qquad l = 2, \ldots, k-1-\omega, \\ z &= 0, \\ w &= \Delta \cdot \delta, \qquad \delta = 1, 2, \ldots, p-1. \end{aligned}$$

In addition, the number of groups in $\mathcal{M}$ having the invariants $(k, j_1, \ldots, j_s, \Delta)$ is equal to $(p-1)^{s-1+\Delta} p^J$ where $J = j_1 + \cdots + j_s$.

THEOREM 7. *Let $(k, j_1, \ldots, j_s, \Delta)$ be a set of integers with $k=p-2$ and $j_s \neq 1$. Let*

$$\begin{aligned} \varepsilon &= 0 \quad \text{if } j_s = 0, \\ &= 1 \quad \text{if } j_s \geqq 2; \\ j_{s+1} &= \Delta(2n-4). \end{aligned}$$

Let g be a primitive root modulo p. Let $(k_1, \ldots, k_{s+1})$ be the set of integral $(s+1)$-tuples defined by

$$0 \leqq k_1 < (p-1, s_1)$$
$$0 \leqq k_i < ((p-1)j_i/(p-1, j_1, \ldots, j_{i-1}), p-1), \qquad i = 2, \ldots, s+1.$$

Then the distinct groups in $\mathscr{M}$ having the invariants $(k, j_1, \ldots, j_s, \Delta)$ are given by the set of parameters

$$\{(a(n-k), a_1(j_1), \ldots, a_s(j_s), w, z)\}$$

where

$$\begin{aligned} a(n-k) &\equiv 1, \\ a_t(j_t) &\equiv g^{k_t} \qquad t = 1, 2, \ldots, s-1, \\ a_s(j_s) &\equiv \varepsilon \cdot g^{k_s}, \\ z &\equiv 0, \\ w &\equiv \Delta \cdot g^{k_{s+1}}. \end{aligned}$$

In addition the number of distinct groups in $\mathscr{M}$ having the invariants $(k, j_1, \ldots, j_s, \Delta)$ is equal to $d(p-1)^{s-2+\varepsilon+\Delta}$ where $d=(j_1, \ldots, j_s, \Delta(2n-4), p-1)$.

The methods employed in this work also enable one to evaluate the order of the automorphism group of the type of group under consideration. We have

THEOREM 8. *Let $|\mathrm{Aut}\, G|$ denote the order of the automorphism group of the group G, and suppose that G is in $\mathscr{M}$. We then have*:

(1) *If G has the invariants $(0, \lambda, \tau)$, then*

$$|\mathrm{Aut}\, G| = (p-1, \lambda(n-2))^{1-\tau}(p-1)p^{2(n-2)+1-\lambda}.$$

(2) *If G has the invariants $(k, j_1, \ldots, j_s, \lambda, \tau)$, then*

$$|\mathrm{Aut}\, G| = dp^{2(n-2)+1-\lambda}$$

where $d=(j_1, \ldots, j_s, \lambda(n-2), \tau(2n-k-5), p-1)$.

(3) *If G has the invariants $(k, j_1, \ldots, j_s, \Delta)$, then*

$$|\mathrm{Aut}\, G| = dp^{2n-2}$$

where $d=(j_1, \ldots, j_s, \Delta(2n-4), p-1)$.

Loosely, most of the groups under consideration will have an automorphism group of prime power order since for most $(j_1, \ldots, j_s)$ we will have $(j_1, \ldots, j_s, p-1)=1$. However there will be groups of order p^n whose automorphism group is of order $dp^{2(n-2)+1}$ where d is any divisor of $p-1$. To get $d=p-1$, for example, take $\lambda=\tau=0$, $s=1$ and $j_1=0$ in (2) or take $\lambda=0$ and $\tau=1$ in (1). To get a $d<p-1$ (for $p\geqq 5$) take $\lambda=\tau=0$, $k=p-3$, $s=1$ and $j_1=d$ in (2). There are other possibilities.

Note also that in Hall's theorem, the order of the automorphism group is a divisor of $p^{2(n-2)+1}(p-1)^2(p+1)$ for these groups, overstates the case by a factor of $p+1$. There is a group, however, where we get $p^{2(n-2)+1}(p-1)^2$; take $\lambda=\tau=0$ in (1).

This paper has one central result, Lemma 37. Nearly everything that precedes it is connected in one way or another with its proof. Because of this a brief description of the organization of the paper might be helpful. §1 contains a collection of simple and useful results on commutators and pth powers of products, $(xy)^p$; it also contains a proof of Theorem 2. In §2 we assume two groups are isomorphic, derive some congruences on this assumption, and then bring these congruences to a point where the problem begins. The third section contains various results on binomial sums and Stirling numbers, most of which have no obvious purpose until §4. Lemma 37 is then proved in the fourth section. Once it is established the theorems follow quite quickly.

1. As mentioned, we are concerned mostly with the calculus of commutators here.

LEMMA 1. *Let G be a metabelian group, g and h be elements of G, and k and m be positive integers. Then*

$$[g^k, h^m] = \prod_{\nu=1}^{k}\prod_{j=1}^{m}\Big[g, h, \overset{\nu-1}{\overline{g,\dots,g}}, \overset{j-1}{\overline{h,\dots,h}}\Big]^{\binom{k}{\nu}\binom{m}{j}}.$$

Proof. First, if x is in $G_2=[G, G]$ and y is in G then since G_2 is abelian, x commutes with $[x, y]$ and $[x^k, y]=[x, y]^k$. Thus, by induction on k,

$$h^{-1}g^kh = g^k\prod_{\nu=1}^{k}\Big[g, h, \overset{\nu-1}{\overline{g,\dots,g}}\Big]^{\binom{k}{\nu}}.$$

To complete the proof compute $g^{-k}h^mg^k$ by induction on m.

From this point on we shall assume that G is a metabelian p-group of maximal class and order p^n, s is an element of G not in G_1, s_1 is an element of G_1 not in G_2, and $s_i=[s_{i-1}, s]$ for $i=2, 3, \dots, n-1$.

LEMMA 2.

$$[s_1^k, s^m] = s_2^{\binom{m}{1}k}\cdots s_{m+1}^{\binom{m}{m}k}\prod_{\nu=2}^{k}\prod_{j=1}^{m}\Big[s_2, \overset{\nu-1}{\overline{s_1,\dots,s_1}}, \overset{j-1}{\overline{s,\dots,s}}\Big]^{\binom{k}{\nu}\binom{m}{j}},$$

$$[s_i^k, s^m] = s_{i+1}^{\binom{m}{1}k}\cdots s_{i+m}^{\binom{m}{m}k}\quad \textit{for } i\geqq 2,$$

$$[s_i^k, s_1^m] = \prod_{j=1}^{m}\Big[s_i, \overset{j}{\overline{s_1,\dots,s_1}}\Big]^{\binom{m}{j}k}.$$

These equations are special cases of Lemma 1; they will be used frequently in the sequel.

LEMMA 3. *Suppose that* $[s_1, s_2]=s_{n-k}^{a(n-k)}\cdots s_{n-1}^{a(n-1)}$. *Then for* $r\geqq 2$,

$$[s_1, s_r] = s_{n-k+r-2}^{a(n-k)}\cdots s_{n-1}^{a(n-r+1)}.$$

Proof. Suppose the result is true for r. Then, by the commutativity of G_2, we have

$$\begin{aligned}[s_1, s_{r+1}]s_{r+1}^{-1} &= s_1^{-1}s_{r+1}^{-1}s_1 = s_{r+1}^{-s_1} = [s_r, s]^{-s_1}\\ &= [s, s_r]^{s_1} = [s^{s_1}, s_r^{s_1}] = [s[s, s_1], s_r[s_r, s_1]]\\ &= [ss_2^{-1}, s_r[s_r, s_1]] = [s, s_r[s_r, s_1]] = [s, [s_r, s_1]][s, s_r]\\ &= [s, s_{n-k+r-2}^{-a(n-k)}\cdots s_{n-1}^{-a(n-r+1)}]s_{r+1}^{-1}.\end{aligned}$$

That is,

$$\begin{aligned}[s_1, s_{r+1}] &= [s, s_{n-k+r-2}]^{-a(n-k)}\cdots[s, s_{n-2}]^{-a(n-r)}\\ &= s_{n-k+r-1}^{a(n-k)}\cdots s_{n-1}^{a(n-r)}.\end{aligned}$$

LEMMA 4. *Let G be a metabelian p-group of maximal class and order p^n. Then*

$$s_i^{\binom{p}{1}}s_{i+1}^{\binom{p}{2}}\cdots s_{i+p-1}^{\binom{p}{p}} = 1$$

for $i=2, 3, \ldots, n-1$. *In addition,* G_ν *is a group of exponent* p *for* $\nu=n-(p-1)$, $n-(p-2), \ldots, n-1$.

Proof. Since s^p is in the center of G [2, Theorem 14.13, p. 368] the first assertion follows from Lemma 2; take $k=1$ and $m=p$ in the first two equations of Lemma 2. The second assertion is a consequence of the first.

The next sequence of lemmas deals with the evaluation of pth powers of projects. There is a result in Blackburn [1, Theorem 1.6] on the subject but it does not contain the information we need for the case $k=p-2$.

LEMMA 5. *Let G be a metabelian p-group and x and y be elements of G. Set* $\sigma_1=y$, $\sigma_2=[y, x], \ldots, \sigma_i=[\sigma_{i-1}, x]$ *and*

$$h(r) = \prod_{\nu=1}^{r}\sigma_{\nu+1}^{\binom{r}{\nu}}\left[\sigma_{\nu+1}^{\binom{r}{\nu}}, \sigma_1^r\right]$$

for $r\geqq 1$. *Then* $(xy)^p=x^p\cdot y^p h(1)\cdots h(p-1)$.

Proof. First, by induction on m,

$$(xy)^m = x^m\prod_{q=1}^{m}\prod_{\nu=0}^{m-q}\sigma_{\nu+1}^{\binom{m-q}{\nu}}.$$

Secondly, by collecting the σ_1, $(xy)^m=x^m y^m h(1)h(2)\cdots h(m-1)$. Finally, take $m=p$.

Lemma 6. *Let G be a metabelian p-group. Then*

$$(xy)^p = x^p y^p \sigma_2^{\binom{p}{2}} \cdots \sigma_p^{\binom{p}{p}} h$$

where

$$h = \prod_{\nu=1}^{p-1} \prod_{j=1}^{p-1} \Big[\sigma_{\nu+1}, \overset{j}{\overline{\sigma_1, \ldots, \sigma_1}}\Big]^{C(\nu,j)}$$

and

$$C(\nu,j) = \sum_{r=1}^{p-1} \binom{r}{\nu}\binom{r}{j}.$$

Proof. We need to evaluate $h(1)\cdots h(p-1)$ of Lemma 5. Since G_2 is abelian we have upon rearranging

$$h(1)\cdots h(p-1) = \sigma_2^{\binom{p}{2}} \cdots \sigma_p^{\binom{p}{p}} h$$

where

$$h = \prod_{r=1}^{p-1} \prod_{\nu=1}^{r} [\sigma_{\nu+1}, \sigma_1^r]^{\binom{r}{\nu}}.$$

By Lemma 1,

$$[\sigma_{\nu+1}, \sigma_1^r] = \prod_{j=1}^{r} \Big[\sigma_{\nu+1}, \overset{j}{\overline{\sigma_1, \ldots, \sigma_1}}\Big]^{\binom{r}{j}}.$$

If we combine these last two equations and rearrange we get Lemma 6.

Lemma 7. *Let G be a metabelian p-group of maximal class and order p^n. Suppose that x is in G and y is in G_1. Then*

$$(xy)^p = x^p y^p \sigma_2^{\binom{p}{2}} \cdots \sigma_p^{\binom{p}{p}} [\sigma_1, \sigma_{p-1}].$$

Proof. Since

$$\sigma_{\nu+1} = \Big[y, \overset{\nu}{\overline{x, \ldots, x}}\Big] \in G_{\nu+1}$$

we have, by Theorem 1,

$$[\sigma_{\nu+1}, \sigma_1] \in [G_{\nu+1}, G_1] \leqq G_{n-p+\nu+1}.$$

By Lemma 4, $G_{n-p+\nu+1}$ is a group of exponent p. Consequently, the only terms of the product h of Lemma 6 that are of interest are those where $C(\nu, j)$ is not a multiple of p. These exponents have been computed at another point in this paper (§3, Lemmas 19 and 20) and we have

$$C(\nu,j) = \sum_{t=0}^{j} \frac{(-1)^{t+j}}{t!\,\nu!} \binom{j}{t} \frac{(p+t)\cdots(p-\nu)}{(\nu+t+1)} \quad \text{if } j \leqq \nu,$$

and

$$C(\nu,j) = \sum_{t=0}^{\nu} \frac{(-1)^{t+\nu}}{t!\,j!} \binom{\nu}{t} \frac{(p+t)\ldots(p-j)}{(j+t+1)} \quad \text{if } \nu \leqq j.$$

Since $1 \leqq j, \nu \leqq p-1$ it follows that $C(\nu, j)$ is a multiple of p except for the cases: $t \leqq j \leqq \nu$ and $\nu+t+1=p$ or $t \leqq \nu \leqq j$ and $(j+t+1)=p$.

We proceed by examining that part of the product in question where j is fixed and ν varies.

If $j=1$ we have $t \leqq j=1 \leqq \nu$ for all ν and the only solutions of $\nu+t+1=p$ are $t=0$, $\nu=p-1$ and $t=1$, $\nu=p-2$. If $t=0$, $\nu=p-1$ the corresponding term in the product is $[\sigma_p, \sigma_1]$. But, by Theorem 1, $[\sigma_p, \sigma_1] \in [G_p, G_1] \in G_{n-p+p}=G_n=1$. If $t=1$ and $\nu=p-2$ the corresponding term is $[\sigma_{p-1}, \sigma_1] \in [G_{p-1}, G_1] \leqq G_{n-1}$. The corresponding exponent is

$$C(p-2, 1) \equiv (-1)^{1+1}\binom{1}{1}\frac{1}{1!(p-2)!}(p+1)(p-1)(p-2)\cdots 2 \equiv -1 \mod p.$$

Thus

$$[\sigma_{p-1}, \sigma_1]^{C(p-2,1)} = [\sigma_{p-1}, \sigma_1]^{-1} = [\sigma_1, \sigma_p].$$

Suppose next that j is fixed and $2 \leqq j \leqq p-1$. Consider first those ν and t where $t \leqq j \leqq \nu$ and $\nu+t+1=p$. The corresponding term of the product, for fixed ν and j, is

$$\begin{aligned}\Big[\sigma_{\nu+1}, \overset{j}{\overline{\sigma_1, \dots, \sigma_1}}\Big] &= \Big[[\sigma_{\nu+1}, \sigma_1], \overset{j-1}{\overline{\sigma_1, \dots, \sigma_1}}\Big] \\ &\leqq \Big[G_{n-p+\nu+1}, G_1, \overset{j-2}{\overline{G, \dots, G}}\Big] \leqq \Big[G_{n-p+\nu+3}, \overset{j-2}{\overline{G, \dots, G}}\Big] \\ &\leqq G_{n-p+\nu+3+j-2} \leqq G_n = 1,\end{aligned}$$

the last inequality following from

$$n-p+\nu+j+1 \geqq n-p+\nu+t+1 = n-p+p = n.$$

Since a similar argument gives the same conclusion for $\nu \leqq j$, this completes the proof of Lemma 7.

If we apply Lemma 7 with $x=s$ and $y=s_1^\zeta$ we get

Lemma 8. *Let G be a metabelian p-group of maximal class and order p^n. Suppose that $[G_1, G_2]=G_{n-k}$ and $[s_1, s_2]=s_{n-k}^{a(n-k)}\cdots s_{n-1}^{a(n-1)}$ then*

$$(ss_1^\zeta)^p = s^p\Big(s_1^{\binom{p}{1}}\cdots s_p^{\binom{p}{p}}\Big)^\zeta s_{n-1}^{\psi\zeta^2}$$

where

$$\begin{aligned}\psi = \psi(k) &= a(n-k) \quad \textit{if } k = p-2, \\ &= 0 \qquad\qquad \textit{if } k \leqq p-3.\end{aligned}$$

Proof. We need to compute σ_ν, where

$$\sigma_\nu = \Big[s_1^\zeta, \overset{\nu-1}{\overline{s, \dots, s}}\Big].$$

By Lemma 2,

$$\sigma_2 = [s_1^\zeta, s] = s_2^\zeta \prod_{\nu=2}^{\zeta} \Big[s_2, \overset{\nu-1}{\overline{s_1, \dots, s_1}}\Big]^{\binom{\zeta}{\nu}} = s_2^\zeta t_2$$

where $t_2 \in G_{n-p+2}$. By induction, $\sigma_\nu = s_\nu^\zeta t_\nu$, $t_\nu \in G_{n-p+\nu}$, thus

$$\sigma_\nu^{\binom{p}{\nu}} = s_\nu^{\zeta\binom{p}{\nu}}, \qquad \nu = 2, \ldots, p-1, p,$$

since for $\nu \leqq p-1$, t_ν is in a group of exponent p, while for $\nu = p$, $t_p \in G_{n-p+p} = 1$. Next, since t_{p-1} is in the center of G, $[\sigma_1, \sigma_{p-1}] = [s_1^\zeta, s_{p-1}^\zeta t_{p-1}] = [s_1^\zeta, s_{p-1}]^\zeta$. By Lemma 2,

$$[s_{p-1}, s_1^\zeta] = \prod_{j=1}^{\zeta} \Big[s_{p-1}, \overbrace{s_1, \ldots, s_1}^{j}\Big]^{\binom{\zeta}{j}} = [s_{p-1}, s_1]^\zeta.$$

Consequently, by Lemma 3,

$$[\sigma_1, \sigma_{p-1}] = [s_1, s_{p-1}]^{\zeta^2} = s_{n-k+p-1-2}^{a(n-k)\zeta^2} = s_{n-1}^{\psi\zeta^2}.$$

Lemma 8 follows from these results.

Theorem 2 can be proved at this point. Since s^p is in the center of G there is an integer w such that $s^p = s_{n-1}^w$. Since $(ss_1)^p$ is in the center of G [2, p. 368], Lemma 8 implies that

$$s_1^{\binom{p}{1}} \cdots s_p^{\binom{p}{p}} = s_{n-1}^z$$

for some integer z. By Lemma 4,

$$s_i^{\binom{p}{1}} \cdots s_{i+p-1}^{\binom{p}{p}} = 1 \quad \text{for } i = 2, \ldots, n-1.$$

Finally, if $[G_1, G_2] = G_{n-k}$ where $0 \leqq k \leqq p-2$ then

$$[s_1, s_2] = a_{n-k}^{a(n-k)} \cdots s_{n-1}^{a(n-1)}$$

where $a(n-k) \not\equiv 0 \bmod p$ since G_{n-k} is of exponent p. Thus if G is a metabelian p-group of maximal class of order p^n and $[G_1, G_2] = G_{n-k}$ we can speak of G being defined in terms of the parameters $(a(n-k), a(n-k+1), \ldots, a(n-1), w, z)$ where $a(n-k) \not\equiv 0 \bmod p$.

Conversely, given any set of integers $(a(n-k), a(n-k+1), \ldots, a(n-1), w, z)$ where $a(n-k) \not\equiv 0 \bmod p$ and $0 \leqq k \leqq p-2$, there is a metabelian p-group G of maximal class and order p^n with $[G_1, G_2] = G_{n-k}$ having the given integers as parameters provided that $n \geqq 2k+2$. The proof is based on

LEMMA 9. *Let H be a group, A be a fixed element of H, and x be a symbol. Define x^p by $x^p = A$. For $0 \leqq a, b \leqq p-1$ and $a+b = kp+l$ where $0 \leqq l \leqq p-1$, define $x^a x^b$ by $x^a x^b = x^l A^k$. Let α be an automorphism of H such that $h^{\alpha^p} = h^A$ for every $h \in H$; $A^\alpha = A$. Let $H' = \{x^a h : 0 \leqq a \leqq p-1, h \in H\}$, and define the product for pairs of elements in H' by $(x^a h_1)(x^b h_2) = x^l A^k h_1^{\alpha^b} h_2$. Then H' is a group, H is a normal subgroup of H', and $|H' : H| = p$.*

This result, which is easy to verify directly, is a paraphrase of results in Huppert. See [2, pp. 86–90].

To prove the converse of Theorem 2 for $n \geqq 2k+2$ begin by taking $G_{n-1} = \langle s_{n-1} \rangle$; that is G_{n-1} is the cyclic group of order p generated by s_{n-1}. Then having $G_{i+1}, G_{i+2}, \ldots, G_{n-1}$ in hand construct G_i by taking

$$H = G_{i+1}, \quad x = s_i, \qquad A = \left(s_{i+1}^{\binom{p}{2}} \cdots s_{i+p-1}^{\binom{p}{p}}\right)^{-1},$$

and α to be the identity mapping for $i = n-2, n-3, \ldots, 2$.

To construct G_1 take $H = G_2$, $x = s_1$, and

$$A = \left(s_2^{\binom{p}{2}} \cdots s_p^{\binom{p}{p}}\right)^{-1} s_{n-1}^{z}.$$

Let $[s_1, s_2] = s_{n-k}^{a(n-k)} \cdots s_{n-1}^{a(n-1)}$, $[s_1, s_3] = s_{n-k+1}^{a(n-k)} \cdots s_{n-1}^{a(n-2)}$, etc., and for

$$h = s_2^{C(2)} \cdots s_{n-1}^{C(n-1)}$$

in G_2 define α by

$$h^{\alpha} = s_1^{-1} h s_1 = h[h, s_1] = h[s_2, s_1]^{C(2)} \cdots [s_{n-1}, s_1]^{C(n-1)}.$$

Then, by the conditions given in Theorem 2, α is an automorphism of G_2 satisfying the conditions of Lemma 9, and we have G_1.

The group G can be constructed from G_1 in a similar fashion. The assumption that $n \geqq 2k+2$ is made to avoid involved computations with commutators.

We close this section with a result that will be needed later.

LEMMA 10. *Let G be a metabelian p-group of maximal class and order p^n with $[G_1, G_2] = G_{n-k}$. Let ξ be an integer such that $(\xi, p) = 1$ and ξ^{-1} be its inverse modulo p. Then*

$$(s^{\xi} s_1^{\xi(1)} s_2^{\xi(2)} \cdots s_{n-1}^{\xi(n-1)})^p = s_{n-1}^{a}$$

where $a = w\xi + z\xi(1) + \psi\xi^2(1)\xi^{-1}$.

Proof. Since

$$s^{\xi} s_1^{\xi(1)} s_2^{\xi(2)} \cdots s_{n-1}^{\xi(n-1)} \equiv (s s_1^{\xi(1)\xi^{-1}})^{\xi} \mod G_2$$

we have [3, p. 368]

$$(s^{\xi} s_1^{\xi(1)} s_2^{\xi(2)} \cdots s_{n-1}^{\xi(n-1)})^p = (s s_1^{\xi(1)\xi^{-1}})^{p\xi}.$$

Lemma 10 now follows from Lemma 8 and Theorem 2.

2. At this stage we have a set of groups defined in terms of the parameters $(a(n-k), \ldots, a(n-1), w, z)$ and wish to determine the distinct groups in the set. We proceed by supposing that

$$\bar{G} = \langle t, t_1, \ldots, t_{n-1} : t_i = [t_{i-1}, t], i \geqq 2 \rangle$$

is defined in terms of the parameters $(b(n-k), \ldots, b(n-1), \bar{w}, \bar{z})$ where $b(n-k) \not\equiv 0$,

$$G = \langle s, s_1, \ldots, s_{n-1} : s_i = [s_{i-1}, s], i \geqq 2 \rangle$$

is defined in terms of the parameters $(a(n-k),\dots,a(n-1),w,z)$ where $a(n-k)\not\equiv 0$, and θ is an isomorphism from $\bar{G}$ onto G.

In this section we shall derive a set of equations governing the transformation θ and, loosely speaking, bring this set of equations to the point where our problems begin.

Now, if θ is an isomorphism from $\bar{G}$ onto G we have

$$t^{\theta} = s^{\xi}s_1^{\xi(1)}\cdots s_{n-1}^{\xi(n-1)} \quad \text{where } (\xi,p) = 1.$$

Next, since G_i is the only normal subgroup of G for $i=2,\dots,n-1$ [2, p. 361], we have $(\bar{G}_i)^{\theta}=G_i$ for $i\geqq 2$. Since $G_{n-k}=\bar{G}^{\theta}_{n-k}=[\bar{G}_1,\bar{G}_2]^{\theta}=[\bar{G}_1^{\theta},\bar{G}_2^{\theta}]=[\bar{G}_1^{\theta},G_2]$ and, by definition, G_1 is the largest subgroup of G such that $[G_1,G_2]=G_{n-k}$, it follows that $\bar{G}_1^{\theta}\leqq G_1$ and then $\bar{G}_1^{\theta}=G_1$. Consequently

$$t_1^{\theta} = s_1^{\eta(1)}s_2^{\eta(2)}\cdots s_{n-1}^{\eta(n-1)} \quad \text{where } (\eta(1),p) = 1.$$

Finally since $\{t,t_1\}$ is a minimal set of generators for $\bar{G}$, θ is determined by the values it assumes at t and t_1.

In the next sequence of lemmas we shall work out the consequences of the fact that if θ is an isomorphism of $\bar{G}$ to G then $[t_{i-1}^{\theta},t^{\theta}]=[t_{i-1},t]^{\theta}=t_i^{\theta}$. The main result to be otained is

Lemma 11. *Suppose θ is an isomorphism of $\bar{G}$ to G with*

$$t^{\theta} = s^{\xi}s_1^{\xi(1)}\cdots s_{n-1}^{\xi(n-1)}, \qquad (\xi,p) = 1,$$
$$t_1^{\theta} = s_1^{\eta(1)}\cdots s_{n-1}^{\eta(n-1)}, \qquad (\eta(1),p) = 1.$$

Set

$$F(r,x) = \sum{}^{*} \binom{\xi}{\nu_1}\cdots\binom{\xi}{\nu_r}$$

*where * indicates the summation is taken over all integral $(\nu_1,\dots,\nu_r)$ such that $\nu_i\geqq 1$ for $i=1,2,\dots,r$ and $\nu_1+\cdots+\nu_r=x$. Set, for $r=2,3,\dots,n-1$,*

$$m(r,j) = \sum_{x=r-1}^{j-1} \eta(j-x)F(r-1,x), \qquad j = r,r+1,\dots,n-1,$$

and $Q(r)=\prod_{j=r}^{n-1} s_j^{m(r,j)}$. Then $t_r^{\theta}=Q(r)P(r)$, $r=2,3,\dots,n-1$, where $P(2)\in G_{n-k}$ and $P(r)\in G_{n-k+r-3}$ for $r\geqq 3$.

To begin we have

Lemma 12. *Under our assumptions, $t_2^{\theta}=[t_1^{\theta},s^{\xi}]h_2$ where $h_2\in G_{n-k}$.*

Proof. Since $[a,xy]=[a,y][a,x]^y$, $[ab,x]=[a,x]^b[b,x]$, and G_2 is abelian we have

$$\begin{aligned} t_2^{\theta} = [t_1^{\theta},t^{\theta}] &= [t_1^{\theta},s^{\xi}s_1^{\xi(1)}s_2^{\xi(2)}\cdots s_{n-1}^{\xi(n-1)}] \\ &= [t_1^{\theta},s_2^{\xi(2)}\cdots s_{n-1}^{\xi(n-1)}][t_1^{\theta},s^{\xi}s_1^{\xi(1)}]. \end{aligned}$$

Now

$$[t_1^{\theta},s_2^{\xi(2)}\cdot s_{n-1}^{\xi(n-1)}]\in[G_1,G_2] = G_{n-k}.$$

In addition,

$$[t_1^\theta, s^\xi s_1^{\xi(1)}] = [t_1^\theta, s_1^{\xi(1)}][t_1^\theta, s^\xi]^a$$

where $a = s_1^{\xi(1)}$. But

$$\begin{aligned} [t_1^\theta, s_1^{\xi(1)}] &= [s_1^{\eta(1)} s_2^{\eta(2)} \cdots s_{n-1}^{\eta(n-1)}, s_1^{\xi(1)}] = [s_2^{\eta(2)} \ldots s_{n-1}^{\eta(n-1)}, s_1^{\xi(1)}] \in G_{n-k}, \\ [t_1^\theta, s^\xi]^a &= [t_1^\theta, s^\xi][t_1^\theta, s^\xi, s_1^{\xi(1)}], \end{aligned}$$

and

$$[t_1^\theta, s^\xi, s_1^{\xi(1)}] \in [G_2, G_1] = G_{n-k}.$$

If we bring these results together we have $t_2^\theta = [t_1^\theta, s^\xi]h_2$ where $h_2 \in G_{n-k}$.

LEMMA 13. *We have*

$$[t_1^\theta, s^\xi] = h_2' \prod_{j=2}^{n-1} s_j^{m(2,j)}$$

where $h_2' \in G_{n-k}$ *and, for* $j = 2, 3, \ldots, n-1$,

$$m(2,j) = \sum_{x=1}^{j-1} \eta(j-x)\binom{\xi}{x}.$$

Proof. Since $[ab, x] = [a, x]^b[b, x]$ and G_2 is abelian,

$$\begin{aligned} [t_1^\theta, s^\xi] &= [s_1^{\eta(1)} s_2^{\eta(2)} \cdots s_{n-1}^{\eta(n-1)}, s^\xi] \\ &= [s_1^{\eta(1)}, s^\xi][s_2^{\eta(2)} \cdots s_{n-1}^{\eta(n-1)}, s^\xi] = \prod_{i=1}^{n-1} [s_i^{\eta(i)}, s^\xi]. \end{aligned}$$

By Lemma 2,

$$[s_1^{\eta(1)}, s^\xi] = \left(\prod_{x=1}^{\xi} s_{x+1}^{\binom{\xi}{x}\eta(1)}\right) h_2'$$

where $h_2' \in G_{n-k}$, and, for $i \geqq 2$,

$$[s_i^{\eta(i)}, s^\xi] = \prod_{x=1}^{\xi} s_{i=x}^{\binom{\xi}{x}\eta(i)}.$$

Consequently,

$$[t_1^\theta, s^\xi](h_2')^{-1} = \prod_{i=1}^{n-1} \prod_{x=1}^{\xi} s_{i+x}^{\binom{\xi}{x}\eta(i)} = \prod_{j=2}^{n-1} s_j^{m(2,j)}$$

where

$$m(2,j) = \sum_{i+x=j;\, i,x \geqq 1} \eta(i)\binom{\xi}{x} = \sum_{x=1}^{j-1} \eta(j-x)\binom{\xi}{x}.$$

This completes the proof of Lemma 13.

Note that for $r = 2$,

$$F(r-1, x) = F(1, x) = \sum_{\nu_1 = x;\, \nu_1 \geqq 1} \binom{\xi}{\nu_1} = \binom{\xi}{x}.$$

Consequently

$$m(2,j) = \sum_{x=1}^{j-1} \eta(j-x)F(1,x),$$

and, by Lemmas 12 and 13, Lemma 11 is true for the case $r=2$.

We begin our induction with

LEMMA 14. *Suppose that for $r \geqq 2$, $t_r^\theta = P(r)Q(r)$ where $Q(r)=\prod_{j=r}^{n-1} s_j^{m(r,j)}$. Then*

$$t_{r+1}^\theta = P(r+1) \prod_{j=r+1}^{n-1} s_j^{m(r+1,j)}$$

where $P(r+1)=[P(r), s^\xi]h_r$, $h_r \in [G_r, G_1]$, and

$$m(r+1,j) = \sum_{i+x=j;\, i \geqq r,\, x \geqq 1} m(r,i)\binom{\xi}{x}.$$

Proof. First, by the usual arguments,

$$t_{r+1}^\theta = [t_r^\theta, t^\theta] = [t_r^\theta, s^\xi]h_r$$

where $h_r \in [G_r, G_1]$. Next,

$$[t_r^\theta, s^\xi] = [P(r), s^\xi][Q(r), s^\xi].$$

Finally,

$$[Q(r), s^\xi] = \prod_{i=r}^{n-1} [s_i^{m(r,i)}, s^\xi] = \prod_{i=r}^{n-1}\prod_{x=1}^{\xi} s_{i+x}^{\binom{\xi}{x} m(r,i)} = \prod_{j=r+1}^{n-1} s_j^{m(r+1,j)}$$

where

$$m(r+1,j) = \sum_{i+x=j;\, i \geqq r,\, x \geqq 1} m(r,i)\binom{\xi}{x}.$$

We can now prove Lemma 11. By Lemmas 12 and 13, $P(2) \in G_{n-k}$. By Lemma 14, $P(3)=[P(2), s^\xi]h_2$, $h_2 \in [G_2, G_1]=G_{n-k}$; thus $P(3) \in G_{n-k}$. Inductively, suppose that $r \geqq 3$ and $P(r) \in G_{n-k+r-3}$. Then

$$P(r+1) = [P(r), s^\xi]h_r \in [G_{n-k+r-3}, G][G_r, G_1] \leqq G_{n-k+r+1-3}.$$

Consequently, $P(r)$ is where it was asserted to be.

Suppose next that

$$m(r,i) = \sum_{y=r-1}^{i-1} \eta(i-y)F(r-1,y).$$

Then, by Lemma 14,

$$m(r+1,j) = \sum_{i+x=j;\, i \geqq r,\, x \geqq 1} \binom{\xi}{x} \sum_{y=r-1}^{i-1} \eta(i-y)F(r-1,y).$$

Rearranging we get,

$$m(r+1,j) = \sum_{z=r}^{j-1} \eta(j-z) \sum{}^{*} \binom{\xi}{x} F(r-1,y)$$

where * indicates the inner sum is to be taken over all those i, j, and x such that $i+x=j$, $i-y=j-z$, $x\geqq 1$, $i\geqq r$, $r-1\leqq y\leqq i-1$. Set $l=j-i$. Then, on one hand, $x=j-i=l\geqq 1$. On the other, $y=i-j+z=z-l\geqq r-1$; that is $l\leqq z-r+1$. Consequently the inner sum is taken over those x and y such that

$$x = l, \quad y = z-l, \qquad l = 1, 2, \ldots, z-r+1,$$

and it is equal to

$$\sum_{l=1}^{z-r+1} \binom{\xi}{l} F(r-1, z-l) = \sum_{l=1}^{z-r+1} \binom{\xi}{l} \sum_{\nu_1+\cdots+\nu_{r-1}=z-l;\nu_i\geqq 1} \binom{\xi}{\nu_1}\cdots\binom{\xi}{\nu_{r-1}}$$
$$= \sum_{\nu_1+\cdots+\nu_r=z;\nu_i\geqq 1} \binom{\xi}{\nu_1}\cdots\binom{\xi}{\nu_r} = F(r, z).$$

Hence

$$m(r+1, j) = \sum_{z=r}^{j-1} \eta(j-z)F(r, z).$$

This completes the proof of Lemma 11.

LEMMA 15. *We have*

$$[t_1^\theta, t_2^\theta] = (s_{n-k}^{A(n-k)}\cdots s_{n-1}^{A(n-1)})^{\eta(1)}h$$

where

$$A(n-k+j) = \sum_{x=0}^{j} a(n-k+x)m(2, j+2-x), \qquad j = 0, 1, \ldots, k-1,$$

and $h \in [G_1, G_{n-k}]$.

Proof. By Lemma 11,

$$[t_1^\theta, t_2^\theta] = [s_1^{\eta(1)}s_2^{\eta(2)}\cdots s_{n-1}^{\eta(n-1)}, Q(2)P(2)]$$
$$= [s_1^{\eta(1)}, Q(2)P(2)] = [s_1^{\eta(1)}, P(2)][s_1^{\eta(1)}, Q(2)].$$

Since $P(2) \in G_{n-k}$ we have $[s_1^{\eta(1)}, P(2)] \in [G_1, G_{n-k}]$. To continue,

$$[s_1^{\eta(1)}, Q(2)] = \prod_{i=2}^{n-1} [s_1^{\eta(1)}, s_i^{m(2,i)}].$$

By Lemma 2,

$$[s_i^{m(2,i)}, s_1^{\eta(1)}] = \prod_{j=1}^{\eta(1)} [s_i, \overset{j}{\overline{s_1, \ldots, s_1}}]^{\binom{\eta(1)}{j}m(2,i)}.$$

For $j\geqq 2$

$$[s_i, \overset{j}{\overline{s_1, \ldots, s_1}}] \in [G_2, G_1, G_1] = [G_{n-k}, G_1].$$

Thus

$$[s_1^{\eta(1)}, Q(2)] = g \prod_{i=2}^{n-1} [s_1, s_i]^{\eta(1)m(2,i)}$$

where $g \in [G_1, G_{n-k}]$. By Lemma 4,

$$[s_1^{\eta(1)}, Q(2)]g^{-1} = \prod_{i=2}^{n-1}\left(\prod_{x=0}^{k-i+1} s_{n-k+i-2+x}^{a(n-k+x)}\right)^{\eta(1)m(2,i)}$$

$$= \prod_{j=0}^{k-1} s_{n-k+j}^{A(n-k+j)\eta(1)},$$

where

$$A(n-k+j) = \sum_{i-2+x=j;i\geqq 2,x\geqq 0} a(n-k+x)m(2,i)$$

$$= \sum_{x=0}^{j} a(n-k+x)m(2,j+2-x).$$

This proves Lemma 15.

If we combine Lemmas 11 and 15 and also assume that $n \geqq 2k+3$, we get

Lemma 16. *Let G, $\bar{G}$, and θ be as above and suppose that $n \geqq 2k+3$. Then, for $j=0, 1, \ldots, k-1$, we have*

$$\sum_{x=0}^{j} m(n-k+x, n-k+j)b(n-k+x) \equiv \eta(1)\left(\sum_{x=0}^{j} a(n-k+x)m(2,j+2-x)\right)\cdot$$

Proof. By Lemmas 11 and 15,

$$h(s_{n-k}^{A(n-k)}\cdots s_{n-1}^{A(n-1)})^{\eta(1)} = [t_1^{\theta}, t_2^{\theta}] = [t_1, t_2]^{\theta}$$

$$= (t_{n-k}^{b(n-k)}\cdots t_{n-1}^{b(n-1)})^{\theta}$$

$$= (Q(n-k)P(n-k))^{b(n-k)}\cdots(Q(n-1)P(n-1))^{b(n-1)}$$

where $h \in [G_1, G_{n-k}] = G_{2n-2k-2}$ and $P(n-k) \in G_{2n-2k-3}$. Since $n \geqq 2k+3$ we have $2n-2k-3 \geqq n$, so

$$h = P(n-k) = \cdots = P(n-1) = 1.$$

Thus

$$s_{n-k}^{A(n-k)\eta(1)}\cdots s_{n-1}^{A(n-1)\eta(1)} = (Q(n-k))^{b(n-k)}\cdots(Q(n-1))^{b(n-1)}.$$

Now

$$\prod_{y=0}^{k-1}(Q(n-k+y))^{b(n-k+y)} = \prod_{y=0}^{k-1}\prod_{j=n-k+y}^{n-1} s_j^{m(n-k+y,j)b(n-k+y)}$$

$$= \prod_{w=0}^{k-1} s_{n-k+w}^{B(n-k+w)}$$

where $B(n-k+w) = \sum_{y=0}^{w} m(n-k+y, n-k+w)b(n-k+y)$. Thus, since $G_{n-k}, \ldots, G_{n-1}$ are groups of exponent p,

$$B(n-k+j) \equiv \eta(1)A(n-k+j) \mod p$$

for $j=0, 1, \ldots, k-1$. If we replace $B(n-k+j)$ and $A(n-k+j)$ by their defining sums we have Lemma 16.

From this point on we shall assume that $n \geqq 2k+3$.

LEMMA 17. *The system of congruences of Lemma* 16 *is equivalent to the system*

$$F(n-k-1, n-k-1)b(n-k) \equiv \eta(1)a(n-k)F(1, 1),$$

$$\sum_{x=0}^{j} \frac{b(n-k+x)}{b(n-k)} F(n-k-1+x, n-k-1+j)$$
$$\equiv \frac{F(n-k-1, n-k-1)}{F(1, 1)} \sum_{x=0}^{j} \frac{a(n-k+x)}{a(n-k)} F(1, j+1-x)$$

for $j=1, 2, \ldots, k-1$.

Proof. The first congruence of Lemma 16 is

$$m(n-k, n-k)b(n-k) \equiv \eta(1)a(n-k)m(2, 2).$$

Thus by the definition of $m(n-k, n-k)$ given in Lemma 11,

$$F(n-k-1, n-k-1)b(n-k) \equiv \eta(1)a(n-k)F(1, 1).$$

Let us set $N=n-k$ and assume that

$$(1) \qquad \sum_{t=0}^{y} b(N+t)F(N-1+t, N-1+y) \equiv \eta(1) \sum_{t=0}^{y} a(N+t)F(1, y+1-t)$$

for $y=0, 1, \ldots, j-1$. Next, consider the jth congruence of Lemma 16,

$$\sum_{x=0}^{j} m(N+x, N+j)b(N+x) \equiv \sum_{x=0}^{j} \eta(1)a(N+x)m(2, j+2-x).$$

Call the left-hand side of this congruence L, the right R. Then

$$L = \sum_{x=0}^{j} B(N+x) \sum_{y=N+x-1}^{N+j-1} \eta(N+j-y)F(N-1+x, y)$$
$$= \sum_{r=0}^{j} \eta(j+1-r) \sum_{x=0}^{r} b(N+x)F(N-1+x, N-1+r).$$

Similarly

$$R = \sum_{r=0}^{j} \eta(j+1-r) \sum_{x=0}^{r} \eta(1)a(N+x)F(1, r+1-x).$$

By the inductive hypothesis the coefficients of $\eta(2), \ldots, \eta(j+1)$ are identical, so (1) also holds for $y=j$. To complete the proof replace $\eta(1)$ in (1) by the corresponding value given by the first congruence.

The problem that arises at this point can be best understood by examining the first few congruences of Lemma 17. Since

$$F(M+t, M+y) = \sum_{\nu_1+\cdots+\nu_{M+t}=M+y;\nu_i\geqq 1} \binom{\xi}{\nu_1}\cdots\binom{\xi}{\nu_{M+t}}$$

can be evaluated without any difficulty for $M=n-k-1$, $0\leqq t\leqq y$, $y=0$, 1, or 2 we find, after a few computations, that the congruence of Lemma 17 corresponding to $j=1$ is equivalent to

$$\left[\frac{b(n-k+1)}{b(n-k)}+\frac{n-k-2}{2}\right]\xi \equiv \left[\frac{a(n-k+1)}{a(n-k)}+\frac{n-k-2}{2}\right].$$

Recall that we are assuming we have an isomorphism and that there is a nonzero ξ satisfying this congruence. So, if the coefficient of ξ is not zero the constant term is not zero; no difficulties arise. However, if the coefficient of ξ is zero then the constant term is zero and the congruence is an identity in ξ.

If we assume that this congruence is vacuous then the congruence of Lemma 17 corresponding to $j=2$ is equivalent to the pure quadratic congruence

$$\left[\frac{b(n-k+2)}{b(n-k)}+\cdots\right]\xi^2 \equiv \left[\frac{a(n-k+2)}{a(n-k)}+\cdots\right].$$

The same situation arises: the congruence is an identity in ξ for certain values of our parameters.

We shall need several results on Stirling numbers to analyze this pattern.

3. This section contains a variety of useful results about binomial sums and the Stirling numbers. We begin with the well-known

Lemma 18 (Vandermonde's Convolution).

$$\sum_{j=0}^{n}\binom{A}{j}\binom{B}{n-j} = \binom{A+B}{n}.$$

This can be established by equating coefficients in the two expansions of $(1+z)^A(1+z)^B=(1+z)^{A+B}$.

We now develop, in Lemmas 19 and 20, a result employed in §1.

Lemma 19.

$$\binom{r}{j} = \sum_{t=0}^{j}(-1)^{t+j}\binom{j}{t}\binom{r+t}{t}.$$

To prove this apply the convolution formula to the right-hand side.

Lemma 20. *If $j \leqq v$ then*

$$\sum_{r=v}^{m}\binom{r}{j}\binom{r}{v} = \sum_{t=0}^{j}(-1)^{t+j}\binom{j}{t}\binom{v+t}{t}\binom{m+t+1}{v+t+1}.$$

Proof. Let L denote the left-hand side of this equation. Then by Lemma 19,

$$L = \sum_{r=v}^{m}\binom{r}{v}\sum_{t=0}^{j}(-1)^{t+j}\binom{j}{t}\binom{r+t}{t}$$
$$= \sum_{t=0}^{j}(-1)^{t+j}\binom{j}{t}\sum_{r=v}^{m}\binom{r+t}{t}\binom{r}{v}.$$

To complete the proof note that the last inner sum is equal to

$$\binom{\nu+t}{t}\sum_{r=\nu+t}^{m+t}\binom{r}{\nu+t} = \binom{\nu+t}{t}\binom{m+t+1}{\nu+t+1}.$$

The remaining lemmas of this section are connected with the system given in Lemma 17.

Lemma 21. *Let $(y)_m=y(y-1)\cdots(y-m+1)$. Then for $m\leqq r-1$ we have*

$$\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}((r-t)x)_m = 0.$$

Proof. For $m=1$

$$\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}(r-t)x = \sum_{t=0}^{r-1}(-1)^t\frac{r!}{t!(r-1-t)!}x$$
$$= rx\sum_{t=0}^{r-1}(-1)^t\binom{r-1}{t} = 0.$$

In addition since $((r-t)x)_{m+1}=((r-t)x)_m((r-t)x-m)$ we have

$$\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}((r-t)x)_{m+1} = (rx-m)\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}((r-t)x)_m$$
$$+rx\sum_{t=0}^{r-2}(-1)^t\binom{r-1}{t}((r-1-t)x)_m.$$

That is, Lemma 21 can be proved by induction.

The next lemma is used in evaluating the functions $F(r, x)$ of Lemmas 11 and 17.

Lemma 22. *Let x be a nonnegative integer. Then*

$$\sum_{\nu_1+\cdots+\nu_r=N;\,\nu_i\geqq 1}\binom{x}{\nu_1}\cdots\binom{x}{\nu_r} = \sum_{t=0}^{r-1}(-1)^t\binom{r}{t}\binom{(r-t)x}{N}.$$

Proof. The assertion is easy to verify for $r=1$. So, let

$$S = \sum_{\nu_1+\cdots+\nu_{r+1}=N;\,\nu_i\geqq 1}\binom{x}{\nu_1}\cdots\binom{x}{\nu_{r+1}}$$
$$= \sum_{\nu=1}^{N-r}\binom{x}{\nu}\sum_{\nu_1+\cdots+\nu_r=N-\nu;\,\nu_i\geqq 1}\binom{x}{\nu_1}\cdots\binom{x}{\nu_r}.$$

Then, by the induction hypothesis,

$$S = \sum_{\nu=1}^{N-r}\binom{x}{\nu}\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}\binom{(r-t)x}{N-\nu}$$
$$= \sum_{t=0}^{r-1}(-1)^t\binom{r}{t}\sum_{\nu=1}^{N-r}\binom{x}{\nu}\binom{(r-t)x}{N-\nu}.$$

If we extend the inner sum from $\nu=0$ to $\nu=N$, subtract the proper quantities, apply Vandermonde's convolution to the full sum, and then perform several elementary manipulations we get $S=A-B$ where

$$A = \sum_{t=0}^{r-1}(-1)^t\binom{r}{t}\left[\binom{(r+1-t)x}{N}-\binom{(r-t)x}{N}-\binom{x}{N}\right]$$

and

$$B = \sum_{\nu=N-r+1}^{N-1}\binom{x}{\nu}\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}\binom{(r-t)x}{N-\nu}.$$

To continue, if we split the defining sum for A into three sums, corresponding to the three terms in the brackets, reindex the resulting middle sum by replacing $(r-t)x$ by $(r+1-(t+1))x$, and then proceed in the (then) obvious way we get

$$A = \sum_{t=0}^{r}(-1)^t\binom{r+1}{t}\binom{(r+1-t)x}{N}.$$

This is the desired sum for the induction.

As for B, the inner sum of the defining sum can be written as

$$\frac{1}{(N-\nu)!}\sum_{t=0}^{r-1}(-1)^t\binom{r}{t}((r-t)x)_{N-\nu}.$$

In addition, according to the index of summation of the ν, $N-\nu \leqq r-1$. That is, the one assumption of Lemma 21 holds. Applying it we get $B=0$. This completes the proof of Lemma 22.

The Stirling numbers of the first kind, S_n^m, are defined by $(x)_n=\sum_{m=1}^n S_n^m x^m$. The Stirling numbers of the second kind, $\mathcal{S}_n^m$, are defined by $x^n=\sum_{m=1}^n \mathcal{S}_n^m(x)_m$. The known results about these numbers that we shall need are

(1) $$(-1)^{n-m}\frac{m!}{n!}S_n^m = \sum_{\nu_1+\cdots+\nu_m=n;\,\nu_i\geq 1}\frac{1}{\nu_1\cdots\nu_m},$$

(2) $$\frac{m!}{n!}\mathcal{S}_n^m = \sum_{\nu_1+\cdots+\nu_m=n;\nu_i\geq 1}\frac{1}{\nu_1!\cdots\nu_m!},$$

(3) $$m!\mathcal{S}_n^m = \sum_{x=1}^{m}(-1)^{m-x}\binom{m}{x}x^n,$$

(4) $$S_{n+1}^m = S_n^{m-1}-nS_n^m,$$

(5) $$\sum_{\nu=j}^{N}\mathcal{S}_N^\nu S_\nu^j = 1 \quad \text{if } j = N, \qquad = 0 \quad \text{if } j < N.$$

Proofs can be found in Jordan [3]. See pages 146, 176, 143, and 183, respectively.

The following lemma has an important role in the analysis of the system of Lemma 17.

LEMMA 23. *If $c+2 \leqq j \leqq N-c$ where $c \geqq 0$ then*

$$G(j, c) = \sum_{\nu=j+c}^{N} (\nu)_c \mathcal{S}_N^\nu S_{\nu-c}^j = \binom{N}{j} c! \mathcal{S}_{N-j}^c$$

where $\mathcal{S}_m^0 = 0$ if $m > 0$ and $\mathcal{S}_0^0 = 1$.

The proof of this lemma is rather complicated. We begin by defining three functions:

$$U(j, k) = \sum_{\nu=j+k}^{N} \mathcal{S}_N^\nu S_{\nu-k}^j,$$

$$V(j, k, r) = \sum_{\nu=j+k+r}^{N} (\nu)_{r-1} \mathcal{S}_N^\nu S_{\nu-k-r}^j \quad \text{for } r \geqq 1,$$

$$W(j, k, r) = \sum_{\nu=j+k+r}^{N} (\nu)_r \mathcal{S}_N^\nu S_{\nu-k-r}^j \quad \text{for } r \geqq 0.$$

As usual, $(\nu)_0 = 1$. We have the following relations:

$$W(j, k, r) = V(j-1, k, r+1) + (k+1)V(j, k, r+1) - W(j, k, r+1), \tag{6}$$

$$V(j, k, r) = W(j, k+1, r-1), \tag{7}$$

$$V(j, k, 1) = U(j, k+1). \tag{8}$$

To prove (6) start from

$$S_{\nu-k-r}^j = S_{\nu-k-r-1}^{j-1} + (k+1)S_{\nu-k-r-1}^j - (\nu-r)S_{\nu-k-r-1}^j,$$

an equation that can be derived from (4). Then multiply this equation by $(\nu)_r \mathcal{S}_N^\nu$ and sum from $\nu = j+k+r$ to $\nu = N$. Equations (7) and (8) are, upon examination of the defining sums, obvious.

The first step in the proof of Lemma 23 is

LEMMA 24. *If $c \geqq 0$ then*

$$G(j, c+1) = W(j-1, 1, c) + W(j, 1, c) - G(j, c). \tag{9}$$

Proof. By (4),

$$S_{\nu-c}^j = S_{\nu-c-1}^{j-1} + S_{\nu-c-1}^j - (\nu-c)S_{\nu-c-1}^j.$$

To get (9) multiply this equation by $(\nu)_c \mathcal{S}_N^\nu$ and then sum from $\nu = j+c$ to $\nu = N$.

LEMMA 25. *If $R \geqq 1$ then*

$$(-1)^R W(j, k, R) = U(j, k) + \sum_{r=1}^{R} (-1)^r [V(j-1, k, r) + (k+1)V(j, k, r)]. \tag{10}$$

Proof. For $R=1$ we have

$$\begin{aligned} U(j,k) &= \sum_{v=j+k}^{N} \mathscr{S}_N^v S_{v-k}^j \\ &= \sum_{v=j+k}^{N} \mathscr{S}_N^v [S_{v-k-1}^{j-1}+(k+1)S_{v-k-1}^j - vS_{v-k-1}^j] \\ &= V(j-1,k,1)+(k+1)V(j,k,1)-W(j,k,1). \end{aligned}$$

So (10) is true for $R=1$. We can, by (6), complete the proof by induction on R.

LEMMA 26. *If* $j \geq k$ *then*

$$\sum_{t=1}^{k} (-1)^{t-1} S_k^{k-t+1} U(j-k+t,k) = \binom{N-1}{j} k^{N-1-j}.$$

Proof. By the definition of the Stirling numbers of the second kind

$$(k+x)^N = \sum_{v=1}^{N} \mathscr{S}_N^v (k+x)_v.$$

In addition since for $v>k$

$$(k+x)_v = (x+1)(x+2)\cdots(x+k)(x)_{v-k} = (x+1)\cdots(x+k)\sum_{n=1}^{v-k} S_{v-k}^n x^n,$$

it follows that

$$(k+x)^{N-1} = \sum_{v=1}^{k} \mathscr{S}_N^v (k-1+x)_{v-1} + (x+1)\cdots(x+k-1) \sum_{v=k+1}^{N} \mathscr{S}_N^v \sum_{n=1}^{v-k} S_{v-k}^n x^n.$$

Now the first sum on the right-hand side of this equation is a polynomial in x of degree at most $k-1$;

$$(x+1)(x+2)\cdots(x+k-1) = \sum_{t=1}^{k} (-1)^{t-1} S_k^{k-t+1} x^{k-t};$$

the double sum is equal to $\sum_{n=1}^{N-k} U(n,k)x^n$; and the product of these last two quantities is

$$P + \sum_{j=k}^{N-1} x^j \sum_{t=1}^{k} (-1)^{t-1} S_k^{k-t+1} U(j-k+t,k)$$

where P is a polynomial of degree at most $k-1$.

Consequently

$$(k+x)^{N-1} = P' + \sum_{j=k}^{N-1} x^j \sum_{t=1}^{k} (-1)^{t-1} S_k^{k-t+1} U(j-k+t,k)$$

where P' is a polynomial in x of degree at most $k-1$. To conclude the proof compare coefficients of x^j for $j \geq k$.

LEMMA 27. *If $j \geqq x+2$ then*

$$\sum_{t=0}^{x+1} (-1)^t S_{x+2}^{x+2-t} U[j-(x+1)+t, x+1] = \binom{N}{j}(x+1)^{N-j}.$$

Proof. Multiplying the equation of Lemma 26 by k we get

$$\sum_{t=1}^{k} (-1)^{t-1} k S_k^{k-t+1} U(j-k+t, k) = \binom{N-1}{j} k^{N-j}.$$

Next, replacing j by $j-1$ in Lemma 26 yields

$$\sum_{t=1}^{k} (-1)^{t-1} S_k^{k-t+1} U(j-k+t-1, k) = \binom{N-1}{j-1} k^{N-j}.$$

If we add these two equations, making use of (4), and then replace k by $x+1$ we have the stated assertion.

LEMMA 28. *Let $H(j, k, a) = \sum_{u=1}^{a} (-1)^{u-1} V(j, k, u)$. Then*

$$H(j, k, a) = aU(j, k+1) - \sum_{u=1}^{a-1} [H(j-1, k+1, u) + (k+2)H(j, k+1, u)].$$

Proof. If we apply (8) to the first term of the defining sum for $H(j, k, a)$ and (7) to the remaining ones we get

$$\begin{aligned} H(j, k, a) &= U(j, k+1) + \sum_{u=2}^{a} (-1)^{u-1} W(j, k+1, u-1) \\ &= U(j, k+1) + \sum_{u=1}^{a-1} (-1)^{u} W(j, k+1, u). \end{aligned}$$

Thus, by Lemma 25,

$$\begin{aligned} H(j, k, a) = {} & U(j, k+1) \\ & + \sum_{u=1}^{a-1} \left[U(j, k+1) + \sum_{v=1}^{u} (-1)^v \{V(j-1, k+1, v) + (k+2)V(j, k+1, v)\} \right] \\ = {} & aU(j, k+1) - \sum_{u=1}^{a-1} [H(j-1, k+1, u) + (k+2)H(j, k+1, u)]. \end{aligned}$$

LEMMA 29. *If $j \geqq c+2$ then*

$$(-1)^c [W(j-1, 1, c) + W(j, 1, c)] = \binom{N}{j} \sum_{x=0}^{c} (-1)^x \binom{c}{x} (x+1)^{N-j}.$$

Proof. Let L denote the left-hand side of the above equation. Then, by Lemma 25 with $k=1$ and $R=c$,

$$L = U(j-1, 1) + U(j, 1) + \sum_{u=1}^{c} (-1)^u [V(j-2, 1, u) + 3V(j-1, 1, u) + 2V(j, 1, u)].$$

Since $S_2^2 = 1$, $-S_2^1 = 1$, $S_3^3 = 1$, $-S_3^2 = 3$, and $S_3^1 = 2$, we have

$$L = \sum_{t=0}^{1} (-1)^t S_2^{2-t} U(j-1+t, 1) - \sum_{t=0}^{2} (-1)^t S_3^{3-t} \sum_{u=1}^{c} (-1)^{u-1} V(j-2+t, 1, u).$$

Next, set

$$S(x) = (-1)^x\binom{c}{x}\sum_{t=0}^{x+1}(-1)^t S_{x+2}^{x+2-t}U[j-(x+1)+t, x+1].$$

Then, by this definition and the definition of Lemma 28,

$$L = S(0)-\sum_{t=0}^{2}(-1)^t S_3^{3-t}H(j-2+t, 1, c).$$

The inductive hypothesis is

$$L = S(0)+\cdots+S(x)+(-1)^{x+1}\sum_{t=0}^{x+2}(-1)^t S_{x+3}^{x+3-t}\sum\nolimits^{(x)} H[j-x-2+t, x+1, u(x)]$$

where $\sum^{(x)}$ denotes the x-fold sum with variables of summation $u(1), u(2), \ldots, u(x)$ where $u(1)=1, \ldots, c-1$ and $u(v)=1, \ldots, [u(v-1)-1]$ for $v=2, 3, \ldots, x$.

The induction is fairly straightforward. One applies Lemma 28 to the H functions in the x-fold sum, getting U functions and H functions. The U functions combine to give $S(x+1)$; the set of H functions combine to give the $(x+1)$-fold sum.

We finally get $L=S(0)+S(1)+\cdots+S(c)$. So, by Lemma 27,

$$L = \binom{N}{j}\sum_{x=0}^{c}(-1)^x\binom{c}{x}(x+1)^{N-j}.$$

This completes the proof of Lemma 29.

We can now prove Lemma 23. First, by the definition of $G(j, c)$, by (5) and by the assumption that $j \leqq N-c$ we have

$$G(j, 0) = \sum_{v=j}^{N}\mathscr{S}_N^v S_v^j = \binom{N}{j}(0!)\mathscr{S}_{N-j}^0.$$

So, let

$$G(j, c) = \binom{N}{j}c!\mathscr{S}_{N-j}^c$$

be our inductive hypothesis. Note that by (3),

$$G(j, c) = \binom{N}{j}\sum_{x=1}^{c}(-1)^{c-x}\binom{c}{x}x^{N-j}.$$

Now, by Lemma 24 and then Lemma 29,

$$\begin{aligned} G(j, c+1) &= W(j-1, 1, c)+W(j, 1, c)-G(j, c) \\ &= \binom{N}{j}\sum_{x=0}^{c}(-1)^{c-x}\binom{c}{x}(x+1)^{N-j}-\binom{N}{j}\sum_{x=1}^{c}(-1)^{c-x}\binom{c}{x}x^{N-j} \\ &= \binom{N}{j}\sum_{x=1}^{c+1}(-1)^{c+1+x}\binom{c+1}{x}x^{N-j} = \binom{N}{j}(c+1)!\mathscr{S}_{N-j}^{c+1}. \end{aligned}$$

This completes the proof of Lemma 23.

At another point in this paper we shall come upon a sequence of numbers, $e(n)$, which are defined in terms of the sequence, $g(n, t)$, in the following way: First

$$g(n, t) = \sum{}^{*} \frac{1}{r_1 \cdots r_t}$$

where * indicates the summation is taken over all those integral t-tuples $(r_1, \ldots, r_t)$ such that $r_i \geqq 2$ for $i = 1, 2, \ldots, t$ and such that $r_1 + \cdots + r_t = n + t$. Secondly,

$$e(0) = 1, \qquad e(n) = \sum_{t=1}^{n} (-1)^t g(n, t) \qquad \text{for } n \geqq 1.$$

Thus, for example, $e(0) = 1$, $e(1) = -1/2$, $e(2) = -1/3 + 1/(2 \cdot 2)$.

These numbers are related to the coefficients of the Bernoulli polynomial of the second kind. If these coefficients are denoted by $b_0, b_1, \ldots, b_n$ it is known that $b_0 = 1$,

$$\sum_{m=0}^{n-1} (-1)^m \frac{b_m}{n-m} = 0 \quad \text{for } n \geqq 2.$$

See [3, pp. 264–265] for the details. Thus $b_0 = 1$, $b_1 = 1/2$, $b_2 = -1/3 + 1/(2 \cdot 2)$.

One can easily prove by induction that $(-1)^n e(n) = b_n$.

The main result we shall need about these numbers is

Lemma 30. *If $y > 0$ then*

$$\sum_{n=1}^{y} (-1)^n n!\, e(n) \mathscr{S}_y^n = \frac{1}{y+1}.$$

See [3, p. 267] for the proof.

4. This section deals with the system of congruences of Lemma 17.

First, a typographical note: The Stirling numbers S_n^m and $\mathscr{S}_n^m$ will appear in many of the following statements with fairly complicated arguments m and n. For that reason the notation $S_n^m = S(n, m)$ and $\mathscr{S}_n^m = \mathscr{S}(n, m)$ will be employed.

We begin with a result that turns out to be the first step of an inductive argument.

Lemma 31. *Let $M = n-k-1$, $S(n, m)$ denote a Stirling number of the first kind, and $\mathscr{S}(n, m)$ denote a Stirling number of the second kind. Let*

$$q(j, y, l) = \frac{(M+l)!}{(M+j)!} S(M+j, M+y) \mathscr{S}(M+y, M+l)$$

and

$$r(j, y, l) = \frac{S(j+1-l, y+1)}{(j+1-l)!}.$$

Then the system of congruences of Lemma 17 *is equivalent to the system*

$$F(M, M) b(n-k) \equiv \eta(1) a(n-k) F(1, 1),$$

$$\sum_{y=0}^{j} \xi^y \left[\sum_{l=0}^{y} \frac{b(n-k+l)}{b(n-k)} q(j, y, l) - \sum_{l=0}^{j-y} \frac{a(n-k+l)}{a(n-k)} r(j, y, l) \right] \equiv 0,$$

for $j = 1, 2, \ldots, k-1$.

Proof. The jth congruence of Lemma 17 is

$$(1)\quad \sum_{l=0}^{j} \frac{b(n-k+l)}{b(n-k)} F(M+l, M+j) \equiv \frac{F(M, M)}{F(1, 1)} \sum_{l=0}^{j} \frac{a(n-k+l)}{a(n-k)} F(1, j+1-l)$$

where

$$F(M+l, M+j) = \sum_{\nu_1+\cdots+\nu_{M+l}=M+j;\, \nu_i \geqq 1} \binom{\xi}{\nu_1}\cdots\binom{\xi}{\nu_{M+l}}.$$

Note for later purposes that since each summand is a product of $M+l$ binomial coefficients $\binom{\xi}{\nu}$ with $\nu \geqq 1$ the function $F(M+l, M+j)$, considered as a polynomial in ξ with rational coefficients, is divisible by ξ^{M+l}.

We want to express (1) as a polynomial in ξ. To begin, by Lemma 22,

$$F(M+l, M+j) = \sum_{t=0}^{M+l-1} (-1)^t \binom{M+l}{t} \binom{(M+l-t)\xi}{M+j}.$$

Thus if we set $c(l) = b(n-k+l)/b(n-k)$ and $d(l) = a(n-k+l)/a(n-k)$ and let L denote the left-hand side of (1) we have

$$L = \sum_{l=0}^{j} c(l) \sum_{t=0}^{M+l-1} (-1)^t \binom{M+l}{t} \binom{(M+l-t)\xi}{M+j}.$$

Next, group together those terms where $M+l-t = x$, $1 \leqq x \leqq M+j$. Then

$$L = \frac{1}{(M+j)!} \sum_{x=1}^{M+j} (x\xi)_{M+j} f(x)$$

where

$$f(x) = f(x, j) = \sum_{l=0}^{j} (-1)^{M+l-x} c(l) \binom{M+l}{x}.$$

To continue, set

$$(x\xi)_{M+j} = \sum_{q=1}^{M+j} S(M+j, q)(x\xi)^q$$

Then

$$L = \frac{1}{(M+j)!} \sum_{q=1}^{M+j} S(M+j, q)\xi^q \sum_{x=1}^{M+j} f(x)x^q.$$

Now since $F(M+l, M+j)$ is divisible by ξ^{M+l} and L is a sum of these quantities with $l \geqq 0$, it follows that L is divisible by ξ^M. In particular the coefficient of ξ^q in this last expression for L must be 0 for $q = 1, 2, \ldots, M-1$. Thus we have

$$L = \frac{1}{(M+j)!} \sum_{q=M}^{M+j} \xi^q S(M+j, q) \sum_{x=1}^{M+j} f(x)x^q.$$

Rearranging and then using (3) of §3 we find that

$$\sum_{x=1}^{M+j} f(x)x^q = \sum_{l=0}^{j} c(l) \sum_{x=1}^{M+l} (-1)^{M+l-x} \binom{M+l}{x} x^q$$

$$= \sum_{l=0}^{j} c(l)(M+l)!\mathscr{S}(q, M+l).$$

Consequently,

$$L = \sum_{q=M}^{M+j} \xi^q \sum_{l=0}^{j} c(l)\frac{(M+l)!}{(M+j)!} S(M+j, q)\mathscr{S}(q, M+l).$$

If we reindex, by setting $q=M+y$, $y=0, 1, \ldots, j$ we get

$$L = \xi^M \sum_{y=0}^{j} \xi^y \sum_{l=0}^{j} c(l)q(j, y, l). \tag{2}$$

The right-hand side of (1), R, can be treated in a similar fashion. We have $F(M, M)/F(1, 1)=\xi^{M-1}$. In addition

$$F(1, j+1-l) = \binom{\xi}{j+1-l} = \frac{1}{(j+1-l)!}\sum_{t=1}^{j+1-l} S(j+1-l, t)\xi^t.$$

Thus, with $a(n-k+l)/a(n-k)=d(l)$,

$$R = \xi^{M-1}\sum_{l=0}^{j} \frac{d(l)}{(j+1-l)!}\sum_{t=1}^{j+1-l} S(j+1-l, t)\xi^t.$$

If we rearrange and then reindex this double sum we get

$$R = \xi^M \sum_{y=0}^{j} \xi^y \sum_{l=0}^{j-y} d(l)r(j, y, l). \tag{3}$$

Lemma 31 now follows from (2) and (3).

To proceed to the induction, let $e(n)$ be defined as in §3 and let

$$D(M, l) = (-1)^l \sum_{\nu=0}^{l} e(l-\nu)(-1)^\nu \frac{M!}{(M+\nu)!} S(M+\nu, M).$$

Suppose, in terms of the process described in the introduction of this paper, that $b(n-k), \ldots, b(n-1)$ has the invariants $j_1, \ldots, j_s$. That is

$$\frac{b(n-k+l)}{b(n-k)} = D(M, l)+b_1(l),$$

etc., and the process stops at the sth step. Let

$$\begin{aligned} \omega = \omega(d) &= 0 && \text{if } d = 0, \\ &= j_1+\cdots+j_d && \text{if } d \geqq 1. \end{aligned}$$

Let, for $j=1, 2, \ldots, k-1-\omega$, $\omega=\omega(d)$,

$$L(\xi, j, d) = \sum_{y=0}^{j} \xi^y \sum_{l=0}^{y} \frac{b_d(j_d+l)}{b_d(j_d)} q[\omega+j, \omega+y, \omega+l]$$

and

$$R(\xi, j, d) = \sum_{y=0}^{j} \xi^y \sum_{l=0}^{j-y} \frac{a_d(j_d+l)}{a_d(j_d)} r[\omega+j, y, \omega+l],$$

where the q and r functions are defined as in Lemma 31. Let

$$J(\xi, j, d) = L(\xi, j, d) - R(\xi, j, d), \qquad j = 1, \ldots, k-1-\omega,\ \omega = \omega(d).$$

We then have

LEMMA 32. *Suppose the sequence $b(n-k), \ldots, b(n-1)$ has the invariants $j_1, \ldots, j_s$. Suppose the system of congruences, for $j = 1, 2, \ldots, k-1$ of Lemma 31, is equivalent to the system*

$$\begin{aligned} b_t(j_t)\xi^{j_t} &\equiv a_t(j_t), & t &= 1, 2, \ldots, d, \\ J(\xi, j, d) &\equiv 0, & j &= 1, \ldots, k-1-\omega, \quad \omega = \omega(d). \end{aligned}$$

Then it is equivalent to the system

$$b_t(j_t)\xi^{j_t} \equiv a_t(j_t), \qquad t = 1, 2, \ldots, d,$$

$$\sum_{y=0}^{j} \xi^y \left[\sum_{l=1}^{y} b_{d+1}(l) q[\omega+j, \omega+y, \omega+l] - \sum_{l=1}^{j-y} a_{d+1}(l) r[\omega+j, y, \omega+l] \right] \equiv 0$$

for $j = 1, \ldots, k-1-\omega$, $\omega = \omega(d)$. Finally, if $d+1 < s$ then this last system of congruences is equivalent to the system

$$\begin{aligned} b_t(j_t)\xi^{j_t} &\equiv a_t(j_t), & t &= 1, 2, \ldots, d+1, \\ J(\xi, j, d+1) &\equiv 0, & j &= 1, \ldots, k-1-\omega, \quad \omega = \omega(d+1). \end{aligned}$$

The proof of Lemma 32 has several parts. Note first of all that when $d = 0$ the set of pure congruences $b(j)\xi^j \equiv a(j)$ is an empty one. In addition $\omega = \omega(0) = 0$ so if we take $b_0(j_0+l) = b(n-k+l)$, $a_0(j_0+l) = a(n-k+l)$, $l = 0, 1, \ldots, k-1$, we then have $J(\xi, j, 0) \equiv 0$, $j = 1, \ldots, k-1$. That is, we have a starting point that makes sense.

So let us suppose that the original system is equivalent to the first system given in Lemma 32 for some d.

Let, for $y = 0, 1, \ldots, j$,

$$Q(y) = \sum_{l=0}^{y} D(M+\omega, l) q[\omega+j, \omega+y, \omega+l]$$

and

$$T(y) = \sum_{l=0}^{j-y} D(M+\omega, l) r[\omega+j, y, \omega+l].$$

Then since

$$\frac{b_d(j_d+l)}{b_d(j_d)} = D(M+\omega, l) + b_{d+1}(l), \qquad \frac{a_d(j_d+l)}{a_d(j_d)} = D(M+\omega, l) + a_{d+1}(l)$$

for $l = 0, 1, \ldots, k-1-\omega$, $\omega = \omega(d)$, we have

$$L(\xi, j, d) = \sum_{y=0}^{j} Q(y)\xi^y + \sum_{y=0}^{j} \xi^y \sum_{l=0}^{y} b_{d+1}(l) q[\omega+j, \omega+y, \omega+l]$$

and

$$R(\xi, j, d) = \sum_{y=0}^{j} T(y)\xi^y + \sum_{y=0}^{j} \xi^y \sum_{l=0}^{j-y} a_{d+1}(l)r[\omega+j, y, \omega+l].$$

Note that the difference of the double sums appearing in the equations for $L(\xi, j, d)$ and $R(\xi, j, d)$ is the jth congruence given in the second system of Lemma 32. Thus we will have the first part of Lemma 32 once we show that $Q(y)=T(y)$.

Lemma 33. *For $y=0, 1, \ldots, j$,*

$$Q(y) = \frac{(M+\omega+y)!}{(M+\omega+j)!}\frac{1}{(y+1)!} S(M+\omega+j, M+\omega+y).$$

Proof. Starting from the definition of $Q(y)$ and working through the definitions involved we get

$$\begin{aligned} L &= \left[\frac{(M+\omega)!}{(M+\omega+j)!} S(M+\omega+j, M+\omega+y)\right]^{-1} Q(y) \\ &= \sum_{l=0}^{y} (M+\omega+l)!\mathscr{S}(M+\omega+y, M+\omega+l) \\ &\quad \cdot \sum_{\nu=0}^{l} (-1)^{l-\nu} e(l-\nu) \frac{S(M+\omega+\nu, M+\omega)}{(M+\omega+\nu)!}. \end{aligned}$$

If we group together those terms where $l-\nu=c$, replace ν in the resulting inner sum by $\nu=l-c$, and then reindex by setting $M-\omega+l=\nu$ we get

$$L = \sum_{c=0}^{y} (-1)^c e(c) \sum_{\nu=M+\omega+c}^{M+\omega+y} (\nu)_c \mathscr{S}(M+\omega+y, \nu) S(\nu-c, M+\omega).$$

We wish to apply Lemma 23 with $N=M+\omega+y$ and $j=M+\omega$. To do so we must have $c+2 \leqq j \leqq N-c$. That is

$$c+2 \leqq M+\omega \leqq M+\omega+y-c.$$

The right-hand inequality holds since $c \leqq y$. As for the left, since $M=n-k-1$ and $n \geqq 2k+3$ we have $M+\omega \geqq k+2+\omega$. But

$$c+2 \leqq y+2 \leqq j+2 \leqq k-1-\omega+2 \leqq k+1-\omega.$$

So, Lemma 23 is applicable. Applying it we find that

$$L = \binom{M+\omega+y}{y} \sum_{c=0}^{y} (-1)^c c!e(c)\mathscr{S}^c_y = \binom{M+\omega+y}{y}\frac{1}{y+1},$$

the last equation following by inspection of $y=0$ and by Lemma 30 if $y>0$. Lemma 33 now follows easily.

Lemma 34. *We have $Q(j)=1/(j+1)!$ and*

$$Q(y) = \frac{(-1)^{j+y}}{(y+1)!} \sum_{t=1}^{j-y} \binom{M+\omega+y}{t} g(j-y, t)$$

for $y=0, 1, \ldots, j-1$.

Proof. The first assertion is an immediate consequence of Lemma 33, so let us assume that $y \leqq j-1$. According to (1) of §3,

$$(-1)^{j+y}\frac{(M+\omega+y)!}{(M+\omega+j)!}S(M+\omega+j, M+\omega+y) = \sum \frac{1}{u(1)\cdots u(M+\omega+y)},$$

the summation being extended over all the integral solutions of

$$u(1)+\cdots+u(M+\omega+y) = M+\omega+j, \qquad u(i) \geqq 1. \tag{4}$$

Classify the solutions of (4) according to the number of $u(i)$ that are equal to 1. If $M+\omega+y-t$ of the $u(i)$ are equal to (1) then we have

$$M+\omega+y-t+r_1+\cdots+r_t = M+\omega+j, \qquad r_i \geqq 2.$$

That is

$$r_1+\cdots+r_t = j-y+t, \qquad r_i \geqq 2. \tag{5}$$

Furthermore, since $r_i \geqq 2$ we have $2t \leqq r_1+\cdots+r_t = j-y+t$, or $t \leqq j-y$; since $y \leqq j-t$, $t \geqq 1$. Consequently, since

$$g(j-y, t) = \sum \frac{1}{r_1\cdots r_t}$$

where the summation is taken over the integral solutions of (5), we have

$$(-1)^{j+y}\frac{(M+\omega+y)!}{(M+\omega+j)!}S(M+\omega+j, M+\omega+y) = \sum_{t=1}^{j-y}\binom{M+\omega+y}{M+\omega+y-t}g(j-y, t).$$

Lemma 34 now follows from this equation and Lemma 33.

Lemma 35.

$$T(y) = \frac{(-1)^{j+y}}{(y+1)!}\left[e(j-y)+\sum_{c=0}^{j-y-1} e(c)\sum_{t=1}^{j-y-c}\binom{M+\omega+y+1}{t}g(j-y-c, t)\right].$$

Proof. We have

$$T(y) = \sum_{l=0}^{j-y} D(M+\omega, l)r(\omega+j, y, w+l).$$

Define $s(n, t)$ by

$$s(n, t) = (-1)^{n-t}\frac{t!}{n!}S(n, t) = \sum_{x_1+\cdots+x_t=n; x_i \geqq 1}\frac{1}{x_1\cdots x_t}.$$

Then

$$r(\omega+j, y, \omega+l) = \frac{S(j+1-l, y+1)}{(j+1-l)!} = \frac{(-1)^{j+y+l}}{(y+1)!}s(j+1-l, y+1)$$

and

$$D(M+\omega, l) = (-1)^l\sum_{v=0}^{l} e(l-v)s(M+\omega+v, M+\omega).$$

Thus

$$T(y) = \frac{(-1)^{j+y}}{(y+1)!}\sum_{c=0}^{j-y} e(c)\sum_{l=c}^{j-y} s(j+1-l, y+1)s(M+\omega+l-c, M+\omega).$$

Now

$$\sum_{l=c}^{j-y} s(j+1-l, y+1)s(M+\omega+l-c, M+\omega) = s(M+\omega+j+1-c, M+\omega+y+1),$$

an equation that can be verified by writing out the sums involved.

Thus

$$T(y) = \frac{(-1)^{j+y}}{(y+1)!}\sum_{c=0}^{j-y} e(c)s(M+\omega+j+1-c, M+\omega+y+1)$$

where

$$s(M+\omega+j+1-c, M+\omega+y+1) = \sum \frac{1}{u(1)\cdots u(M+\omega+y+1)},$$

the summation being taken over the integral solutions of

$$u(1)+\cdots+u(M+\omega+y+1) = M+\omega+j+1-c, \qquad u(i) \geqq 1.$$

If we classify the solutions of this equation according to the number of $u(i)$ that are equal to 1 we find that, for $c \leqq j-y-1$,

$$s(M+\omega+j+1-c, M+\omega+y+1) = \sum_{t=1}^{j-y-c} \binom{M+\omega+y+1}{t} g(j-y-c, t).$$

Lemma 35 now follows.

Lemma 36. *We have* $T(j)=1/(j+1)!$ *and*

$$T(y) = \frac{(-1)^{j+y}}{(y+1)!}\sum_{t=1}^{j-y} \binom{M+\omega+y}{t} g(j-y, t)$$

for $y=0, 1, \ldots, j-1$.

Proof. The first assertion is an immediate consequence of Lemma 35, so suppose that $y \leqq j-1$ in what follows.

If we make the substitution

$$\binom{M+\omega+y+1}{t} = \binom{M+\omega+y}{t} + \binom{M+\omega+y}{t-1}$$

in Lemma 35, collect similar binomial coefficients together, and then reverse the order of summation, we find that

$$\left(\frac{(-1)^{j+y}}{(j+y)!}\right)^{-1} T(y) = e(j-y) + \sum_{t=0}^{j-y} \binom{M+\omega+y}{t}(h(t)+h(t+1))$$

where $h(0)=h(j-y+1)=0$ and

$$h(t) = \sum_{c=0}^{j-y-t} e(c)g(j-y-c, t), \qquad t = 1,\dots,j-y.$$

Since $e(c)=\sum_{x=1}^{c}(-1)^x g(c, x)$, it follows that

$$\begin{aligned} h(t)-g(j-y, t) &= \sum_{c=1}^{j-y-t} g(j-y-c, t) \sum_{x=1}^{c} (-1)^x g(c, x) \\ &= \sum_{x=1}^{j-y-t} (-1)^x \sum_{c=x}^{j-y-t} g(c, x)g(j-y-c, t) \\ &= \sum_{x=1}^{j-y-t} (-1)^x g(j-y, x+t). \end{aligned}$$

That is

$$h(t) = \sum_{x=0}^{j-y-t} (-1)^x g(j-y, x+t).$$

Consequently,

$$h(1) = \sum_{x=0}^{j-y-1} (-1)^x g(j-y, x+1) = -\sum_{x=1}^{j-y} (-1)^x g(j-y, x) = -e(j-y)$$

and for $t\geqq 1$, $h(t)+h(t+1)=g(j-y, t)$.

Bringing these results together, we have Lemma 36.

Lemmas 34 and 36 give $Q(y)=T(y)$. As mentioned earlier, in the remarks following Lemma 32, this completes the proof of the first part of Lemma 32.

To pass from the second system of Lemma 32 to the third recall that if $d+1<s$ then there is an integer $j_{d+1}\geqq 2$ such that

$$b_{d+1}(1) \equiv \cdots \equiv b_{d+1}(j_{d+1}-1) \equiv 0, \qquad b_{d+1}(j_{d+1}) \not\equiv 0.$$

Next, the congruence of the second system corresponding to $j=1$ can be written as $b_{d+1}(1)\xi\equiv a_{d+1}(1)$. Thus $a_{d+1}(1)\equiv 0$. Inductively, if $a_{d+1}(1)\equiv\cdots\equiv a_{d+1}(m)\equiv 0$ where $1\leqq m\leqq j_{d+1}-1$ then the congruence of the second system corresponding to $j=m+1$ is equivalent to $b_{d+1}(m)\xi^{m+1}\equiv a_{d+1}(m+1)$. Consequently

$$a_{d+1}(1) \equiv \cdots \equiv a_{d+1}(j_{d+1}-1) \equiv 0, \qquad a_{d+1}(j_{d+1}) \not\equiv 0,$$

and the second system is equivalent to

$$b_t(j_t)\xi^{j_t} \equiv a_t(j_t), \qquad t = 1, 2, \dots, d+1,$$

$$\sum_{y=0}^{j} \xi^y \left[\sum_{l=1}^{y} b_{d+1}(l)q[\omega+j, \omega+y, \omega+l] - \sum_{l=1}^{j-y} a_{d+1}(l)r[\omega+j, y, \omega+l] \right] \equiv 0$$

for $j=j_{d+1}+1,\dots, k-1-\omega$, $\omega=\omega(d)=j_1+\cdots+j_d$.

To complete the proof of Lemma 32 reindex the last set of congruences, using the facts that $a_{d+1}(1)\equiv\cdots\equiv b_{d+1}(j_{d+1}-1)\equiv 0$ and $\xi^{j_{d+1}}\equiv a_{d+1}(j_{d+1})/b_{d+1}(j_{d+1})$.

A statement of the consequences of Lemma 32 will be deferred for the moment; there are two other congruences to be considered.

We need to derive the congruences connecting w and z with $\bar{w}$ and $\bar{z}$. To begin, by Theorem 2, $t^p = t_{n-1}^{\bar{w}}$. Consequently $(t^p)^\theta = (t_{n-1}^{\bar{w}})^\theta = s_{n-1}^c$ where $c = \bar{w}\eta(1)\xi^{n-2}$; this follows from Lemma 11 and the fact that $n \geqq \max\{2k+3, p+1\}$. In addition, by Lemma 10,

$$(t^p)^\theta = (t^\theta)^p = (s^\xi s_1^{\xi(1)} \cdots s_{n-1}^{\xi(n-1)})^p = s_{n-1}^a$$

where $a = w\xi + z\xi(1) + \psi\xi^2(1)\xi^{-1}$. Thus we have

$$\bar{w}\eta(1)\xi^{n-2} \equiv w\xi + z\xi(1) + \psi\xi^2(1)\xi^{-1}. \tag{6}$$

To continue, by Lemma 10, $(tt_1)^p = t_{n-1}^{\bar{w}+\bar{z}+\bar{\psi}}$. So, going one way

$$[(tt_1)^p]^\theta = (t_{n-1}^{\bar{w}+\bar{z}+\bar{\psi}})^\theta = s_{n-1}^d$$

where $d = (\bar{w}+\bar{z}+\bar{\psi})\eta(1)\xi^{n-2}$. Going in the opposite direction,

$$[(tt_1)^p]^\theta = [(tt_1)^\theta]^p = (s^\xi s_1^{\xi(1)} \cdots s_{n-1}^{\xi(n-1)} s_1^{\eta(1)} \cdots s_{n-1}^{\eta(n-1)})^p.$$

But

$$\begin{aligned} s^\xi s_1^{\xi(1)} \cdots s_{n-1}^{\xi(n-1)} s_1^{\eta(1)} \cdots s_{n-1}^{\eta(n-1)} &\equiv s^\xi s_1^{\xi(1)+\eta(1)} && \bmod G_2 \\ &\equiv (ss_1^e)^\xi && \bmod G_2, \end{aligned}$$

where $e = (\xi(1)+\eta(1))\xi^{-1}$. Thus by [3, Theorem 14.13-d, p. 368] and then Lemma 10,

$$[(tt_1)^p]^\theta = (ss^e)^{\xi \cdot p} = s_{n-1}^b$$

where $b = w\xi + z(\xi(1)+\eta(1)) + \psi(\xi(1)+\eta(1))^2\xi^{-1}$. Thus we have

$$(\bar{w}+\bar{z}+\bar{\psi})\eta(1)\xi^{n-2} \equiv w\xi + z(\xi(1)+\eta(1)) + \psi(\xi(1)+\eta(1))^2\xi^{-1}. \tag{7}$$

Equations (6) and (7) can be simplified. First, applying (6) to (7) we get

$$(\bar{z}+\bar{\psi})\xi^{n-2} \equiv z + \psi\xi^{-1}(2\xi(1)+\eta(1)). \tag{8}$$

Next if $k = p-2$ then $\psi = a(n-k)$ and $\bar{\psi} = b(n-k)$. Thus, by the first congruence of Lemma 31,

$$\psi = a(n-k) \equiv b(n-k)(\xi^{n-k-2}/\eta(1)) \equiv \bar{\psi}(\xi^{n-k-2}/\eta(1)) \equiv \bar{\psi}(\xi^{n-1}/\eta(1)),$$

since $\xi^k \equiv \xi^{p-2} \equiv \xi^{-1}$. Since $\psi = \bar{\psi} = 0$ if $k \leqq p-3$ we have

$$\psi = \bar{\psi}(\xi^{n-1}/\eta(1)), \qquad k = 0, 1, \ldots, p-2. \tag{9}$$

Combining (8) and (9) we find that

$$z \equiv \xi^{n-2}(\bar{z} - 2\bar{\psi}(\xi(1)/\eta(1))). \tag{10}$$

Finally, (6) and (10) yield

$$w \equiv \xi^{n-3}[\bar{w}\eta(1) - \xi(1)\bar{z} + \bar{\psi}(\xi^2(1)/\eta(1))]. \tag{11}$$

We can now state the main result of this section:

Lemma 37. *Let $\bar{G}$ be a metabelian p-group of maximal class, order p^n, with invariants $k, j_1, \ldots, j_s$, where $n \geqq \max\{p+1, 2k+3\}$. Set $\omega=0$ if $s=1$ and $\omega=j_1+\cdots+j_{s-1}$ if $s>1$. Suppose that $\bar{G}=\langle t, \bar{G}_1\rangle$, $\bar{G}_1=\langle t_1, \bar{G}_2\rangle$,*

$$[t_1, t_2] = t_{n-k}^{b(n-k)} \cdots t_{n-1}^{b(n-1)},$$

and $\bar{G}$ is defined in terms of the parameters

$$(b(n-k), b_1(j_1), \ldots, b_s(j_s), b_s(j_s+1), \ldots, b_s(k-1-\omega), \bar{w}, \bar{z}).$$

Similarly, suppose that $G=\langle s, G_1\rangle$, $G_1=\langle s, G_2\rangle$,

$$[s_1, s_2] = s_{n-k}^{a(n-k)} \cdots s_{n-1}^{a(n-1)},$$

and G is defined in terms of the parameters

$$(a(n-k), a_1(j_1), \ldots, a_s(j_s), a_s(j_s+1), \ldots, a_s(k-1-\omega), w, z).$$

Let θ be an isomorphism from $\bar{G}$ to G such that

$$t^\theta = s^\xi s_1^{\xi(1)} \cdots s_{n-1}^{\xi(n-1)}, \qquad t_1^\theta = s_1^{\eta(1)} \cdots s_{n-1}^{\eta(n-1)}, \qquad (\xi\eta(1), p) = 1.$$

Then

$$a(n-k) \equiv b(n-k)\xi^{n-k-2}/\eta(1),$$
$$b_t(j_t)\xi^{j_t} \equiv a_t(j_t), \qquad t = 1, 2, \ldots, s,$$
$$\sum_{y=0}^{j} \xi^y \left[\sum_{l=1}^{y} b_s(l)q[\omega+j, \omega+y, \omega+l] - \sum_{l=1}^{j-y} a_s(l)r[\omega+j, y, \omega+l]\right] \equiv 0,$$

for $j=j_s+1, \ldots, k-1-\omega$;

$$w \equiv \xi^{n-3}[\bar{w}\eta(1)-\xi(1)\bar{z}+\bar{\psi}(\xi^2(1)/\eta(1))],$$
$$z \equiv \xi^{n-2}[\bar{z}-2\bar{\psi}(\xi(1)/\eta(1))],$$

where the q and r functions are defined as in Lemma 31, $\bar{\psi}=0$ if $k \leqq p-3$ and $\bar{\psi}=b(n-k)$ if $k=p-2$.

Proof. The first congruence of the conclusion is the first congruence of Lemma 31; the next two blocks of congruences follow from Lemma 32 with $d+1=s$; the final two congruences are restatements of (10) and (11).

It is also possible and not too difficult to prove that if the congruences of Lemma 37 are valid then $\bar{G}$ is isomorphic to G.

5. This section contains the proofs of Theorems 3 to 8.

The proof of Theorem 3 is quite simple, for if $k=0$ the only congruences of Lemma 37 that are not vacuous are:

$$w \equiv \xi^{n-3}[\bar{w}\eta(1)-\xi(1)\bar{z}], \qquad z \equiv \xi^{n-2}\bar{z}.$$

Thus if $\bar{z}=\bar{w}=0$, i.e. $(\lambda, \tau)=(0, 0)$ then $w=z=0$. If $\bar{z}=0$ and $\bar{w}\neq 0$, i.e. $(\lambda, \tau)=(0, 1)$ then $z=0$ and, for any given ξ, $\eta(1)$ can be chosen so that $w=1$.

If $\bar{z}\neq 0$, i.e. $(\lambda, \tau)=(1, 0)$ then since $\xi(1)=0, 1, \dots, p-1$ the two congruences are equivalent to

$$\begin{aligned} w &\equiv \beta, \qquad \beta = 0, 1, \dots, p-1, \\ z &\equiv \xi^{n-2}\bar{z}. \end{aligned}$$

Thus, we must split the couples

$$\{(w, z) : w = 0, 1, \dots, p-1, z = 1, \dots, p-1\}$$

into equivalence classes by means of the congruences $w\equiv\beta$, $z\equiv\xi^{n-2}\bar{z}$. Let $d=(n-2, p-1)$. Then, for fixed w and z, each equivalence class contains $p(p-1)/d$ distinct elements, so there are d distinct classes. Next let g be a primitive root modulo p and l and q be integers such that $0\leqq l, q\leqq d-1$. Then the couples

$$w \equiv 0, \quad z \equiv g^{l}, \quad \text{and} \quad w \equiv 0, \quad z \equiv g^{q}$$

are not equivalent for $l\neq q$. If they were there would be a $\xi=g^{m}$ such that $z\equiv g^{l}\equiv\bar{z}\xi^{n-2}\equiv g^{q}\xi^{m(n-2)}$. That is $l-q\equiv m(n-2) \bmod p-1$. Since $d=(n-2, p-1)$, this is impossible.

This completes the proof of Theorem 3.

The proof of Theorem 4 is also quite simple. We are supposing that $j_s=1$ so the congruence of Lemma 37 corresponding to $t=s$ assumes the linear form $a_s(1)\equiv b_s(1)\xi$. The first congruence of Lemma 37 is

$$a(n-k) \equiv b(n-k)\xi^{n-k-2}/\eta(1).$$

Consequently, in any class of isomorphic images of a given group $\bar{G}$, there is precisely one value of $(\xi, \eta(1))$ for which $a_s(1)\equiv 1$ and $a(n-k)\equiv 1$.

We are also supposing that $1\leqq k\leqq p-3$, so $\bar{\psi}=0$ and the last two congruences are

$$w \equiv \xi^{n-3}[\bar{w}\eta(1)-\xi(1)\bar{z}], \qquad z \equiv \xi^{n-2}\bar{z}.$$

Thus if $\bar{z}\neq 0$ the corresponding z is not zero. In addition, for any given $(\xi, \eta(1))$ there will be precisely one value of $\xi(1)$ for which $w=0$. In sum, if $\bar{G}$ has the invariants $(k, j_1, \dots, j_s, \lambda, \tau)$ where $j_s=1$, $\lambda=1$ and $\tau=0$ then the class of parameters defining isomorphic images of $\bar{G}$ will contain exactly one set of parameters

$$(a(n-k), a_1(j_1), \dots, a_s(1), a_s(2), \dots, a_s(k-1-\omega), w, z)$$

with $a(n-k)=1$, $a_s(1)=1$, and $w=0$. Consequently, the set of distinct groups with invariants $(k, j_1, \dots, j_s, \lambda, \tau)$ where $j_1=1$, $\lambda=1$, $\tau=0$ is given by the set of parameters

$$\begin{aligned} a(n-k) &= 1, \\ a_t(j_t) &= \alpha_t, \quad \alpha_t = 1, \dots, p-1, \qquad t = 1, 2, \dots, s-1, \\ a_s(1) &= 1, \\ a_s(l) &= \beta_l, \quad \beta_l = 0, 1, \dots, p-1, \qquad l = 2, \dots, k-1-\omega, \\ z &= \gamma, \quad \gamma = 1, \dots, p-1, \\ w &= 0. \end{aligned}$$

Clearly there are

$$(p-1)^{s-1}p^{k-1-\omega-j_s}(p-1) = (p-1)^{s-1+\lambda+\tau}p^J,$$

where $J=j_1+\cdots+j_s$, such groups.

Similar reasoning can be applied to the cases $(\lambda, \tau)=(0,0)$ or $(0,1)$. Doing so we get Theorem 4.

The proof of Theorem 5 is not quite so simple. We are assuming that $j_s\neq 1$, so $j_s=0$ or $j_s=k-1-j_1-\cdots-j_{s-1}\geqq 2$. If $j_s=0$ then, by definition, $b_s(1)=\cdots=b_s(k-1-\omega)=0$ so $a_s(1)=\cdots=a_s(k-1-\omega)=0$ and the congruences of Lemma 37 corresponding to $t=s$ and $j=1,\cdots,k-1-\omega$ are vacuous. If $j_s=k-1-j_1-\cdots-j_{s-1}\geqq 2$ then the congruence of Lemma 37 corresponding to $t=s$ is of the form

$$b_s(j_s)\xi^{j_s} \equiv a_s(j_s), \qquad b_s(j_s) \not\equiv 0,$$

and the set of congruences corresponding to $j=j_s+1,\dots,k-1-\omega$ is empty. In any event, the congruences of Lemma 37 reduce to the system

$$\begin{aligned}
a(n-k) &\equiv b(n-k)\xi^{n-k-2}/\eta(1),\\
b_t(j_t)\xi^{j_t} &\equiv a_t(j_t), \qquad t = 1,2,\dots,s-1,\\
b_s(j_s)\xi^{j_s} &\equiv a_s(j_s),\\
w &\equiv \xi^{n-3}[\bar{w}\eta(1)-\xi(1)\bar{z}],\\
z &\equiv \xi^{n-2}\bar{z},
\end{aligned}$$

where $b_s(j_s)=0$ if $j_s=0$ and $b_s(j_s)\not\equiv 0$ if $j_s\geqq 2$.

We shall consider the case $j_s\neq 0$, $\bar{z}\neq 0$ in detail. To begin set $j_{s+1}=n-2$, $b_{s+1}(j_{s+1})=\bar{z}$, and $a_{s+1}(j_{s+1})=z$. Then our system can be expressed as

$$\begin{aligned}
a(n-k) &\equiv b(n-k)\xi^{n-k-2}/\eta(1),\\
b_t(j_t)\xi^{j_t} &\equiv a_t(j_t), \qquad t = 1,2,\dots,s+1,\\
w &\equiv \xi^{n-3}[\bar{w}\eta(1)-\xi(1)\bar{z}].
\end{aligned}$$

Next, we wish to count the number of distinct elements in a given equivalence class. Thus if $b(n-k),\dots, b_{s+1}(j_{s+1})$ and $\bar{w}$ are considered to be fixed our problem is one of counting duplications of $a(n-k),\dots, a_{s+1}(j_{s+1})$, and w. Suppose there is a duplication. Then, ignoring the first and last congruences of the above system, there is a ξ^* such that

$$a_t(j_t) \equiv b_t(j_t)\xi^{j_t} \equiv b_t(j_t)(\xi^*)^{j_t}, \qquad t = 1,\dots,s+1.$$

That is $\xi^{j_t}\equiv(\xi^*)^{j_t}$, $t=1,\dots,s+1$. Set $d=(j_1,\dots,j_{s+1},p-1)$. Then since there are integers $x_1,\dots,x_{s+2}$ such that $x_1j_1+\cdots+x_{s+1}j_{s+1}+x_{s+2}(p-1)=d$, we have $\xi^d\equiv(\xi^*)^d$.

To continue, let g be a primitive root modulo p, K be the group of reduced residues modulo p, $q=(p-1)/d$, $H=\{g^{l\cdot q} : l=0,1,\dots,d-1\}=\{\xi : \xi^d\equiv 1\}$ and $K=Hg\cup\cdots\cup Hg^q$ be the coset decomposition of K by H. Since $\xi^d\equiv(\xi^*)^d$ if and only if $\xi^{-1}\xi^* \in H$, we can say that $a_t(j_t) \equiv b_t(j_t)\xi^{j_t} \equiv b_t(j_t)(\xi^*)^{j_t}$ $(t=1, 2, \ldots, s+1)$ if and only if ξ and ξ^* are in the same coset of K by H.

This necessary condition for duplication in an equivalence class can be used to determine the distinct elements of the class. For let

$$\xi = g^{\nu+lq}, \qquad 0 \leqq \nu < q = (p-1)/d, \qquad 0 \leqq l < d.$$

Then the elements of a class are given by

$$\begin{aligned} a(n-k) &\equiv b(n-k)g^{(\nu+l\cdot q)(n-2)}/\eta(1), \\ a_t(j_t) &\equiv b_t(j_t)g^{(\nu+l\cdot q)j_t}, \qquad t = 1, 2, \ldots, s+1, \\ w &\equiv [\bar{w}\eta(1)-\xi(1)\bar{z}]g^{(\nu+l\cdot q)(n-3)}. \end{aligned}$$

Since $1 \leqq \eta(1) \leqq p-1$ the $a(n-k)$ component can be any nonzero value for any fixed ξ and since $0 \leqq \xi(1) \leqq p-1$ the w component can be any value for any fixed $(\xi, \eta(1))$. In short the distinct elements of the equivalence class are given by

$$\{(\lambda, b_1(j_1)g^{\nu j_1}, \ldots, b_{s+1}(j_{s+1})g^{\nu j_{s+1}}, \delta)\}$$

where $\lambda = 1, \ldots, p-1$, $\nu = 1, \ldots, (p-1)/d$, and $\delta = 0, 1, \ldots, p-1$. In addition the class contains $(p-1)^2p/d$ distinct elements.

We now turn to the problem of determining a set of representatives for the classes. By the above, we can assume that $a(n-k) = \lambda = 1$ and $w = \delta = 0$. Thus we need to find a system of representatives for the set of $(s+1)$-tuples $\{(a_1(j_1), \ldots, a_{s+1}(j_{s+1}))\}$. When they are split into equivalence classes by means of the congruences

$$a_t(j_t) \equiv b_t(j_t)g^{\nu j_t}, \qquad \nu = 1, \ldots, (p-1)/d, \qquad t = 1, \ldots, s+1.$$

Now the number of $(s+1)$-tuples $(a_1(j_1), \ldots, a_{s+1}(j_{s+1}))$ under consideration is equal to $(p-1)^{s+1}$ and the number of elements in each class is $(p-1)/d$. Consequently there are $d(p-1)^s$ equivalence classes.

The distinct classes are given by

Lemma 38. *Let $\{(k_1, \ldots, k_{s+1})\}$ be the set of integral $(s+1)$-tuples defined by*

$$\begin{gathered} 0 \leqq k_1 < (p-1, j_1), \\ 0 \leqq k_i < \left(\frac{(p-1)j_i}{(p-1, j_1, \ldots, j_{i-1})}, p-1\right), \qquad i = 2, \ldots, s+1. \end{gathered}$$

Let $d = (j_1, \ldots, j_{s+1}, p-1)$ and g be a primitive root modulo p. Let $E(k_1, \ldots, k_{s+1})$ be the equivalence class defined by

$$E(k_1, \ldots, k_{s+1}) = \{(g^{\nu j_1+k_1}, \ldots, g^{\nu j_{s+1}+k_{s+1}}) : \nu = 1, \ldots, (p-1)/d\}.$$

Then the classes $E(k_1, \ldots, k_{s+1})$ are distinct. Moreover, the number of these equivalence classes is equal to $d(p-1)^s$.

Proof. Suppose the classes $E(k_1, \ldots, k_{s+1})$ and $E(k_1', \ldots, k_{s+1}')$ have an element in common. Then there are integers ν, ρ, and π such that

$$g^{j_i+k_i} \equiv g^{\rho j_i+k_i'}\cdot g^{\pi j_i}, \qquad i = 1, \ldots, s+1.$$

That is

$$(\nu-\rho-\pi)j_i \equiv k_i'-k_i \mod (p-1), \qquad i = 1,\ldots,s+1.$$

Consider the first congruence,

$$(1) \qquad (\nu-\rho-\pi)j_1 \equiv (k_1'-k_1) \mod (p-1).$$

It implies that $k_1'-k_1 \equiv 0 \mod (p-1,j_1)$.

Thus since $0 \leqq k_1$, $k_1' < (p-1,j_1)$ we have $k_1'-k_1=0$. Thus, returning to (1), we have $(\nu-\rho-\pi)j_1 \equiv 0 \mod (p-1)$ or

$$(2) \qquad (\nu-\rho-\pi) \equiv 0 \mod (p-1)/(p-1,j_1).$$

Let us go on to the second congruence,

$$(3) \qquad (\nu-\rho-\pi)j_2 \equiv k_2'-k_2 \mod (p-1).$$

According to (2) and (3) there is an integer t such that

$$t((p-1)/(p-1,j_1))j_2 \equiv k_2'-k_2 \mod (p-1).$$

That is,

$$k_2'-k_2 \equiv 0 \mod ((p-1)j_2/(p-1,j_1), p-1).$$

So, by the restrictions on k_2 and k_2', $k_2'-k_2=0$. Going back to (3) we have

$$(4) \qquad (\nu-\rho-\pi) \equiv 0 \mod (p-1)/(p-1,j_2).$$

Now, let $[a,b]$ be the least common multiple of a and b. Since

$$\left[\frac{(p-1)}{(p-1,j_1)}, \frac{(p-1)}{(p-1,j_2)}\right] = \frac{(p-1)}{(p-1,j_1,j_2)},$$

we have, by (2) and (4),

$$(\nu-\rho-\pi) \equiv 0 \mod (p-1)/(p-1,j_1,j_2).$$

Inductively, suppose that at the ith step $k_1'-k_1=\cdots=k_i'-k_i=0$ and

$$(5) \qquad (\nu-\rho-\pi) \equiv 0 \mod (p-1)/(p-1,j_1,\ldots,j_i).$$

Then since

$$(6) \qquad (\nu-\rho-\pi)j_{i+1} \equiv k_{i+1}'-k_{i+1} \mod (p-1)$$

there is an integer t such that

$$t\frac{(p-1)}{(p-1,j_1,\ldots,j_i)}j_{i+1} \equiv k_{i+1}'-k_{i+1} \mod (p-1).$$

Consequently

$$k_{i+1}'-k_{i+1} \equiv 0 \mod ((p-1)j_{i+1}/(p-1,j_1,\ldots,j_i), p-1).$$

So, by the restrictions on k_{i+1} and k_{i+1}', $k_{i+1}'-k_{i+1}=0$. Returning to (6) we get

$$(7) \qquad \nu-\rho-\pi \equiv 0 \mod (p-1)/(p-1,j_{i+1}).$$

Since

$$\left[\frac{p-1}{(p-1,j_{i+1})},\frac{p-1}{(p-1,j_1,\dots,j_i)}\right]=\frac{(p-1)}{(p-1,j_1,\dots,j_{i+1})}$$

we have, by (5) and (7),

$$(\nu-\rho-\pi)\equiv 0 \quad \bmod (p-1)/(p-1,j_1,\dots,j_{i+1}).$$

This completes the proof of the inductive step and shows that the equivalence classes $E(k_1,\dots,k_{s+1})$ are distinct.

The number of classes $E(k_1,\dots,k_{s+1})$ is given by

$$(p-1,j_1)\prod_{i=2}^{s+1}\left(\frac{(p-1)j_i}{(p-1,j_1,\dots,j_{i-1})},p-1\right).$$

A simple inductive argument shows that this product is equal to $d(p-1)^s$.

The result shows that the distinct groups G having the parameters $(k,j_1,\dots,j_s,\lambda,\tau)$ where $j_s\geqq 2$ and $(\lambda,\tau)=(1,0)$ are given by

$$\begin{aligned} a(n-k) &\equiv 1,\\ a_t(j_t) &\equiv g^{k_t}, \qquad t=1,\dots,s,\\ z &\equiv g^{k_{s+1}},\\ w &\equiv 0, \end{aligned}$$

where $\{(k_1,\dots,k_{s+1})\}$ is defined as in Lemma 38. In addition, the number of such groups is equal to

$$(j_1,\dots,j_s,n-2,p-1)(p-1)^s.$$

It should also be clear that we have a similar result if $j_s=0$ and all other conditions remain the same. We need merely delete the congruence corresponding to $t=s$ and then replace s by $s-1$ in the above argument. If we do so we have Theorem 5 for the case $j_s\neq 1$, $(\lambda,\tau)=(1,0)$.

The argument for the case $\bar{z}=0$, $\bar{w}\not\equiv 0$ has a slight variation. We have the system

$$\begin{aligned} a(n-k) &\equiv b(n-k)\xi^{n-k-2}/\eta(1),\\ a_t(j_t) &\equiv b_t(j_t)\xi^{j_t}, \qquad t=1,\dots,s,\\ z &\equiv 0,\\ w &\equiv \eta(1)\bar{w}\xi^{n-3}. \end{aligned}$$

If we fix ξ and let $\eta(1)$ vary from 1 to $p-1$ we get one element in our equivalence class whose first component, $a(n-k)$, is ρ and whose last component, w, is $b(n-k)\xi^{2n-k-5}/\rho$ for $\rho=1,2,\dots,p-1$. Thus our system of congruences is equivalent to the system

$$\begin{aligned} a(n-k) &\equiv \rho, \qquad p=1,\dots,p-1,\\ a_t(j_t) &\equiv b_t(j_t)\xi^{j_t}, \qquad t=1,\dots,s,\\ w &\equiv (b(n-k)/\rho)\bar{w}\xi^{2n-k-5}. \end{aligned}$$

We now proceed as in the previous case to get that part of Theorem 5 concerning the case $(\lambda, \tau)=(0, 1)$.

The proof of the final case of Theorem 5, $(\lambda, \tau)=(0, 0)$, follows the same lines.

In Theorems 6 and 7 we have $k=p-2$, so $\bar{\psi}=b(n-k)\neq 0$ and $\xi^k\equiv\xi^{p-2}\equiv\xi^{-1}$. Thus the first and last two congruences of Lemma 37 are equivalent to

$$\begin{aligned} a(n-k) &\equiv \frac{\bar{\psi}}{\eta(1)}\,\xi^{n-1}, \\ z &\equiv \xi^{n-2}\Big(\bar{z}-2\psi\,\frac{\xi(1)}{\eta(1)}\Big), \\ w &\equiv \frac{1}{\psi}\left[\frac{z^2}{4}-\xi^{2n-4}\Big(\frac{(\bar{z})^2}{4}-\bar{w}\bar{\psi}\Big)\right], \end{aligned}$$

where $\psi=a(n-k)$. (The last congruence is obtained by completing the square in the w congruence of Lemma 37 and then proceeding in the obvious way.)

Since the w congruence can also be expressed as

$$z^2/4-w\psi \equiv \xi^{2n-4}((\bar{z})^2/4-\bar{w}\bar{\psi})$$

and $\psi=a(n-k)$, $\bar{\psi}=b(n-k)$, it follows that all the quantities $z^2-4wa(n-k)$ will be zero or all will be not zero modulo p in any class of isomorphic images of a group G. Consequently, we have an invariant Δ for these cases.

From this point on the proofs of Theorems 6 and 7 are similar to the proofs of Theorems 4 and 5, so they will be left to the reader.

As for the proof of Theorem 8: since an automorphism of G is an isomorphism from G to G we proceed by replacing $b(n-k),\dots,\bar{w}$ and $\bar{z}$ in Lemma 37 by $a(n-k),\dots, w$ and z.

Consider first the case where G has the invariants $(0, \lambda, \tau)$. Under these circumstances there are but two congruences

$$w \equiv \xi^{n-3}[w\eta(1)-\xi(1)z], \qquad z \equiv \xi^{n-2}z.$$

If $(\lambda, \tau)=(0, 0)$ then $w=z=0$ and these two congruences are vacuous. Furthermore since the automorphism θ is defined by

$$\begin{aligned} s^{\theta} &= s^{\xi}s_1^{\xi(1)}\cdots s_{n-1}^{\xi(n-1)}, \\ & \qquad\qquad\qquad\qquad (\xi\eta(1), p) = 1, \\ s_1^{\theta} &= s_1^{\eta(1)}\cdots s_{n-1}^{\eta(n-1)}, \end{aligned}$$

subject to the congruences of Lemma 37, it follows that the automorphism group is of order $p^{2(n-2)+1}(p-1)^2$. Next, if $(\lambda, \tau)=(0, 1)$ then $z=0$ and $w\neq 0$ and we have $w\equiv\xi^{n-3}\eta(1)w$. That is, ξ is arbitrary and $\eta(1)$ is determined by ξ. Consequently

$$|\text{Aut } G| = p^{2(n-2)+1}(p-1).$$

Finally if $(\lambda, \tau)=(1, 0)$ then $z\neq 0$ and we have

$$\begin{aligned} w &\equiv \xi^{n-3}[w\eta(1)-\xi(1)z], \\ z &\equiv \xi^{n-2}z. \end{aligned}$$

In this case ξ can be any one of $(n-2, p-1)$ values, $\eta(1)$ is arbitrary, and $\xi(1)$ is determined by ξ and $\eta(1)$. Thus

$$|\mathrm{Aut}\, G| = (n-2, p-1)(p-1)p^{2(n-2)}.$$

Suppose next that G has the invariants $(k, j_1, \ldots, j_s, \lambda, \tau)$ where $j_s = 1$. The congruence of Lemma 37 corresponding to $t=s$ yields $\xi=1$ and then the first congruence gives $\eta(1)=1$. The fact that the congruences of Lemma 37 corresponding to $j=2, \ldots, k-1-\omega$ hold for $\xi=1$ follows from: The set of congruences we get by deleting the w and z congruences in Lemma 37 is equivalent to the system of Lemma 17; the system of Lemma 17 has the solution $\xi=1$ when $a(n-k+l)=b(n-k+l)$ for $l=0, \ldots, k-1$. Finally, since $\xi=\eta(1)=1$ the last two congruences are $w \equiv w-\xi(1)z$ and $z \equiv z$. This implies that $|\mathrm{Aut}\, G| = p^{2(n-2)+1-\lambda}$ when $j_s=1$.

If $1 \leqq k \leqq p-3$ and $j_s \neq 1$ we have the system

$$\begin{aligned} 1 &\equiv \xi^{n-k-2}/\eta(1), \\ 1 &\equiv \xi^{j_t}, \qquad t = 1, 2, \ldots, s-1, \\ \varepsilon &\equiv \varepsilon\xi^{j_s}, \\ w &\equiv \xi^{n-3}[\eta(1)w - \xi(1)z], \\ z &\equiv \xi^{n-2}z. \end{aligned}$$

If $z \neq 0$ let $d=(j_1, \ldots, j_s, n-2, p-1)$. Then, in any automorphism ξ can be any number such that $\xi^d \equiv 1$, $\eta(1)$ is determined by ξ and $\xi(1)$ is determined by $(\xi, \eta(1))$. Thus $|\mathrm{Aut}\, G| = dp^{2(n-2)}$. If $z=0$ the argument is similar.

Finally if $k=p-2$ the relevant congruences are

$$\begin{aligned} 1 &\equiv \xi^{n-1}/\eta(1), \\ z &\equiv \xi^{n-2}(z-2\psi(\xi(1)/\eta(1))), \\ (z^2/4 - w\psi) &\equiv \xi^{2n-4}(z^2/4 - w\psi), \end{aligned}$$

and we reach our conclusion in the usual fashion.

Bibliography

1. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92. MR **21** #1349.

2. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR **37** #302.

3. C. Jordan, *Calculus of finite differences*, Hungarian Agent Eggenberger Book-Shop, Budapest, 1939. MR **1**, 74.

4. G. Szekeres, *On finite metabelian p-groups with two generators*, Acta Sci. Math. Szeged **21** (1960), 270–291. MR **24** #A1941.

University of California,
Los Angeles, California 90024