ISRAEL JOURNAL OF MATHEMATICS, Vol. 36, No. 2, 1980

ON FINITE GROUPS WITH A SYLOW p-SUBGROUP OF TYPE (m, n)

BY
ARYE JUHÁSZ

ABSTRACT

A finite p-group P is of type (m,n) if P has nilpotency class $m-1$, $P/P' \cong Z_{p^n} \times Z_{p^n}$ and all the lower central factors $K_i(P)/K_{i+1}(P)$ are cyclic of order p^n. Our main result on finite groups with a Sylow p-subgroup of type (m,n) is (Theorem 4.1): *Let G be a finite group with a Sylow p-subgroup P of type (m,n), $n \geqq 2$ $p \geqq 3$, $m \geqq (n+5)(p-1)+1$. For $H \leqq G$ denote $\bar{H} = HO_{p'}(G)/O_{p'}(G)$. If $O_p(G)$ is not cyclic and $P_1' \neq 1$, then $\bar{P} \triangle \bar{G}$ and $\bar{G} = \bar{P} \cdot \bar{T}$ is a semidirect product of $\bar{P}$ and $\bar{T}$, where $\bar{T}$ is cyclic of order t, $t \mid p-1$. Here P_1 is the subgroup defined in section* 0. This theorem easily yields that under its assumptions $N_G(P)/O^p(N_G(P)) \cong G/O^p(G)$, it gives information on the conjugacy pattern of p-elements of G and gives information on the structure of p-local subgroups of G (Theorems 4.2, 4.3 and 4.4).

Introduction

This work consists of two parts: Part A (sections 0–3) contains the relevant results on p-groups of type (m,n), while Part B (section 4) contains the proof of the main theorems. In section 0 we collect the necessary elementary results on the structure of p-groups of type (m,n). Section 1 contains the collection formula for p-groups of type (m,n), which is basic for all the work. Let P be a p-group of type (m,n). Since, for $2 \leqq i \leqq m-1$, $K_i(P)/K_{i+1}(P)$ is cyclic of order p^n, there are elements $s_i \in K_i(P)$ such that $K_i(P) = \langle K_{i+1}(P), s_i \rangle$. In section 2 we compute the exact order of these s_i (Theorem 2.6), by introducing the concept of an "admissible word" and studying the set of all such words in P (Theorems 2.1 and 2.2).

In section 3 we derive some results on the power-structure of P and in particular we show that certain subgroups and homomorphic images of P are regular in the sense of P. Hall (Theorem 3.4). This result is crucial in the proof of the main theorems. In order to achieve it we correspond to every p-group P of

Received November 16, 1978

type (m, n) a Lie-algebra which depends on the "fine structure" of P (Theorem 3.2). This algebra differs in general from the usual one, but is similar in principle to that constructed by R. Shepherd in [12]. By this algebra we get some limitations on the p-degree of commutativity of P (Theorem 3.3), a concept which generalizes the notion of "degree of commutativity" introduced by N. Blackburn in [1], which lead by the aid of results of the previous sections to the desired result.

The main result of section 4 is Theorem 4.1. Two difficulties arise in its proof: the location of $O_p(G)$ in a Sylow p-subgroup P of G and finding a maximal subgroup N of $O_p(G)$ which is normal in G. Here G is a minimal counterexample to Theorem 4.1. The location of $O_p(G)$ is the subject of the first three propositions, which still deal with p-groups. In Proposition 4 we show that $C_G(H) = C_P(P)$ for every noncyclic p-subgroup H of G, while in Proposition 5 we show that the desired subgroup N exists, by Green's transfer theorem [6]. This finishes the proof of Theorem 4.1 immediately. Theorems 4.2, 4.3 and 4.4 follow from Theorem 4.1 by standard considerations.

PART A

0. Notation and basic properties of finite p-groups of type (m, n)

G is a finite group, P a Sylow p-subgroup of G (or just a p-group). $A \leqq G$ means that A is a subgroup of G. $K_2(P) = [P, P]$ and for $i \geqq 3$ $K_i(P) = [K_{i-1}(P), P]$. Define P_1 by $P_1/P_4 = C_{P/P_4}(P_2/P_4)$ and for $i \geqq 2$ let $P_i = K_i(P)$. Denote by $Z_i = Z_i(P)$, $0 \leqq i$ $(Z_0 = 1)$ the upper central series of P. For $n = 1$ a finite p-group of type (m, n) is a p-group of maximal class. The following results follow easily from this fact and the results of Blackburn [1] on p-groups of maximal class.

Proposition 1. *Let P be a p-group of type (m, n). Then*

(a) $Z_i = P_{m-i}$ *for* $1 \leqq i \leqq m - 2$,

(b) P/P_1 *is cyclic of order* p^n.

Let us denote by P_i^j, $0 \leqq j < n$, the subgroup of P_i which contains P_{i+1} and has index p^j in P_i, $P_{i+1} < P_i^j \leqq P_i$.

Definition. Let $k \in N$, $k/n = k_0 + r/n$, $r < n$ and let P be a p-group of type (m, n). P has degree of commutativity k/n if $[P_i, P_j] \leqq P^r_{1+j+k_0}$ for every $i, j \geqq 1$. If $k > 0$ then P has a positive degree of commutativity.

From now on P denotes a p-group of type (m, n).

PROPOSITION 2. *Assume that P/P_{m-1} has positive degree of commutativity. Then:*

(a) *There exists an element $s \in P \setminus P_1$ such that $s \notin C_P(P_{m-2}/P^1_{m-1})$ and $s \notin C_P(P_2/P^1_3)$.*

(b) *If $P_1 = \langle P_2, s_1 \rangle$, s as in* (a) *and for $2 \leqq i \leqq m-1$, $s_i = [s_{i-1}, s]$, then $P_i = \langle P_{i+1}, s_i \rangle$.*

(c) *For every $s \in P \setminus P_1 \cdot \Phi(P)$, $C_P(s) \cap P_2 = P_{m-1}$.*

(d) *For every $s \in P \setminus P_1 \cdot \Phi(P)$, $s^P = \{s^g \mid g \in P\} = s \cdot P_2$.*

(e) *For every $s \in P \setminus P_1 \cdot \Phi(P)$, $s^{p^n} \in P_{m-1}$.*

PROPOSITION 3. *Assume that P/P_{m-1} has degree of commutativity k/n, $0 < k \leqq n$, $m \geqq 5$.*

(a) *If m is odd then P has degree of commutativity k/n.*

(b) *If m is even then P has degree of commutativity k/n iff $P_{\frac{1}{2}m-1}/P^k_m$ is abelian.*

(c) *If P_2/P^k_{m-1} is abelian then P has degree of commutativity k/n.*

LEMMA 1. *Let $s \in P \setminus P_1 \cdot \Phi(P)$ and $H = \langle s, P_2 \rangle$. Then*

(a) *H is a p-group of type $(m-1, n)$.*

(b) *$H_i = K_i(H) = P_{i+1}$, $i \geqq 1$.*

THEOREM 1. *Let P be a p-group of type (m, n). If m is odd and $5 \leqq m \leqq 2p+1$ then P has degree of commutativity $k/n \geqq 1/2$.*

THEOREM 2. *Let P be a p-group of type (m, n). If $m \geqq p+2$ then P has degree of commutativity > 0.*

The result of Theorem 1 is best possible.

LEMMA 2. *Let P be a p-group of type (m, n). If $m \leqq p+1$ then* $\exp(P/P_{m-1}) = \exp(P_2) = p^n$.

Finally we need the following result on $\mathrm{Aut}(P)$, the group of automorphisms of P.

THEOREM 3. [9] *Let P be a p-group of type (m, n), $m \geqq 4$, $A = \mathrm{Aut}(P)$, B a Sylow p-subgroup of A. Then*

(a) *$B \triangle A$ and A is a splitting extension of B by an abelian subgroup Q which is isomorphic to a subgroup of $\mathbf{Z}_{p-1} \times \mathbf{Z}_{p-1}$.*

(b) *To every $q \in Q$ there exists an element $s \in P \setminus P_1$ such that $P = \langle s, s_1 \rangle$ and $s_1^q \equiv s_1^b \bmod P_2$, $s^q \equiv s^a \bmod P_2$, $a, b \not\equiv o(p)$, $0 < a$, $b < p^n$ and $a^{p-1} \equiv b^{p-1} \equiv 1 \bmod p$.*

(c) *For $1 \leqq i \leqq m-1$, $s_i^q \equiv s_i^{a^{i-1} \cdot b} \bmod P_{i+1}$.*

(d) *If* $P_1' \neq 1$ *then* Q *is cyclic of order* t, $t \mid p-1$ *and* $b \equiv a^r \bmod p^n$ *for some* $r \in \mathbf{Z}$.

COROLLARY. *If* G *is a finite group with a Sylow* p*-subgroup of type* (m,n) *and* $P_1' \neq 1$ *then* $N_G(P)/P \cdot C_G(P)$ *is cyclic of order* t, $t \mid p-1$.

Finally, in Section z recall Theorem x of Section y by Theorem $y.x$ if $y \neq z$ and by Theorem x if $y = z$.

1. The collection formula for p-groups of type (m,n)

By the collection formula [8] if F is the free group generated by x and y and $n \in \mathbf{Z}$ then

$$(x \cdot y)^{p^n} = x^{p^n} \cdot y^{p^n} \cdot c_2^{\binom{p^n}{2}} \cdots c_t^{\binom{p^n}{t}} \cdots c_{p^n},$$

where $c_i \in K_i(\langle x,y\rangle)$, $c_i \equiv [y,x,x,\cdots,x]^{\alpha_i}\pi[y,z_1,\cdots,z_{i-1}] \bmod K_{i+1}(\langle x,y\rangle)$, $z_t \in \{x,y\}$,

$$\pi[y,\overset{i-1}{z_1,\cdots,z_{i-1}}] \not\equiv [y,\underset{i-1}{x,x,\cdots,x}] \bmod K_{i+1}(\langle x,y\rangle).$$

For $n=1$, $\alpha_p = \alpha_{p^n} \equiv 1 \bmod p$ ([8]). Our aim is to generalize this result for $n \geqq 2$. For this purpose we fine a finite group P s.t. P is a homomorphic image of F and the result is true in P. It turns out that a metabelian p-group of type (m,n) is suitable for this aim. Hence we shall construct such a group.

PROPOSITION 0. [11] *Let* P *be a metabelian* p*-group of type* (m,n), $P = \langle s, s_1\rangle$ *and for* $i \geqq 2$, $s_i = [s_{i-1}, s]$. *Then*

$$(1)\qquad [s_1^i, s^j] = s_2^{\binom{j}{1}i} s_3^{\binom{j}{2}i} \cdots s_{j+1}^i \cdot \prod_{\nu=2}^{i} \prod_{\mu=1}^{j} [s_2, (\nu-1)s_1, (\mu-1)s]^{\binom{i}{\nu}\binom{j}{\mu}}$$

where $[s_2,(\nu-1)s_1,(\mu-1)s] = [s_2, \underset{\nu-1}{s_1,\cdots,s_1}, \underset{\mu=1}{s,\cdots,s}]$.

$$(2)\qquad [s_k^i, s^j] = s_{k+1}^{\binom{j}{1}i} \cdots s_{k+t}^{\binom{j}{t}i} \cdots s_{k+j}^{\binom{j}{j}i}, \quad k \geqq 2.$$

$$(3)\qquad [s_k^i, s_1^j] = \prod_{\nu=1}^{j} [s_k, \nu s_1]^{\binom{j}{\nu}i}.$$

PROPOSITION 1. *Let* P *be a metabelian* p*-group of type* (m,n). *Then*

(4) *For* $i \geqq 2$

$$\prod_{t=0}^{p^n-1} s_{i+t}^{\binom{p^n}{t+1}} = 1 \quad \textit{and} \quad \prod_{t=0}^{p^n-1} s_{1+t}^{\binom{p^n}{t+1}} \in Z(P)\cdot K_2(P_1).$$

If P is embedded in a p-group of type $(m+1,n)$ then

$$\prod_{t=0}^{p^n-1} s_{1+t}^{\binom{p^n}{t+1}} \in K_2(P_1). \tag{4'}$$

PROOF. Let $H_i = \langle s, P_i \rangle$. Then by Lemma 0.1, H_i is a p-group of type $(m-i+1,n)$. Since for $i \geqq 2$, P_i is abelian,

$$(ss_i)^{p^n} = s^{p^n} s_i^{p^n} s_{i+1}^{\binom{p^n}{2}} \cdots s_{i+p^n-1}^{\binom{p^n}{p^n}}.$$

By 0.2(e), $s^{p^n}, (ss_i)^{p^n} \in Z(P)$ and by 0.2(d) for H_i, $(ss_i)^{p^n}$ and s^{p^n} are conjugate in P. But two elements in the center are conjugate iff they are equal. Hence $(ss_i)^{p^n} = s^{p^n}$. This proves the first part of (4) and (4'). Similarly, expanding $(ss_1)^{p^n} \bmod K_2(P_1)$ we obtain the second part of (4).

PROPOSITION 2. *Let P be a metabelian p-group of type (m,n) and let $x \in P_i$, $i \geqq 2$. Then*

(a) *For every integer k, $x^{kp^n} = s_{i+p-1}^{a_p} \cdots s_{i+p-2+t}^{a_t} \cdots s_{m-1}^{a_{m-1}}$, where for every j, $p \leqq j \leqq m-1$, $0 \leqq a_j < p^n$ and $p^{n-r} \mid a_j$ for $p^r \leqq j < p^{r+1}$, $1 \leqq r \leqq n-1$.*

(b) *Let $x = s_i^{\alpha_1} \cdots s_{i+t}^{\alpha_t} \cdots s_{m-1}^{\alpha_{m-i}}$, $0 \leqq \alpha_i < p^n$. If x has another representation $x = s_i^{\beta_1} \cdots s_{i+t-1}^{\beta_t} \cdots s_{m-1}^{\beta_{m-1}}$, where $\beta_1, \cdots, \beta_{m-1}$ are integers such that $p^{n-r} \mid \beta_j$ for $p^r \leqq j < p^{r+1}$, $0 \leqq r \leqq n-1$, then $p^{n-r} \mid \alpha_j$ for $p \leqq j < p^{r+1}$, $0 \leqq r \leqq n-1$.*

PROOF. We may assume that $m \geqq p+2$, in view of Lemma 0.2. Say that the depth $l(x)$ of x (in (b)) is μ if $\alpha_\mu \neq 0$ but $\alpha_{\mu-t} = 0$ for every $t > 0$. We prove Proposition 2 by induction on $l(x)$. By Lemma 0.2 the proposition holds for $l(x) \leqq p-1$. Let $y = s_{i+1}^{\alpha_2} \cdots s_{m-1}^{\alpha_{m-i}}$. Then $x = s_i^{\alpha_1} y$ and as P_2 is abelian, $x^{kp^n} = s_i^{\alpha_1 kp^n} y^{kp^n}$. By (4)

$$s_i^{\alpha_1 kp^n} = s_{i+1}^{-\alpha_1 k\binom{p^n}{2}} \cdots s_{i+t-1}^{-\alpha_1 k\binom{p^n}{t}} \cdots s_{m-1}^{-\alpha_1 k\binom{p^n}{m-1}}.$$

So we compute $s_{i+t-1}^{-\alpha_1 k\binom{p^n}{t}}$. Let

$$-\alpha_1 k \binom{p^n}{t} = k_t p^n + r_t, \qquad \text{where } 0 \leqq r_t < p^n.$$

Then $p^{n-t} \mid r_t$ for $p^c \leqq t < p^{c+1}$, $0 \leqq c \leqq n-1$, and

$$s_{i+t-1}^{-\alpha_1 k\binom{p^n}{t}} = s_{i+t-1}^{k_t p^n} \cdot s_{i+t-1}^{r_t}.$$

By the induction hypothesis (a)

$$s_{i+t-1}^{k_t p^n} = s_{i+t+p-2}^{a(t,1)} \cdots s_{t+r+p-3+\mu}^{a(t,\mu)} \cdots,$$

where $0 \leqq a(t,\mu) < p^n$ and $p^{n-r} \mid a(t,\mu)$ for $p^r - p + 1 \leqq \mu < p^{r+1} - p + 1$, $1 \leqq r \leqq n$. Therefore

$$(*) \qquad s_{i+t-1}^{-\alpha_1 k\binom{p^n}{t}} = s_{i+t-1}^{r_t} \cdot s_{i+t+p-2}^{a(t,1)} \cdots s_{i+t+p-3+\mu}^{(t,\mu)} \cdots,$$

where $0 \leqq r_t$, $\alpha(t,\mu) < p^n$ and $p^{n-r} \mid a(t,\mu)$ for $p^r - p + 1 \leqq \mu < p^{r+1} - p + 1$, $1 \leqq r \leqq n$ and $p^{n-c} \mid r_t$ for $p^c \leqq t < p^{c+1}$, $1 \leqq c \leqq n-1$.

This yields, by (4), that $s_i^{k\alpha_1 p^n} = s_{i+p-1}^{A_1} \cdots s_{i+p-2+q}^{A_q} \cdots$, where $A_q = \Sigma_{t+\mu=q}\, a(t,\mu) + r_{p-2+q}$. But then by (*) $p^{n-r} \mid A_q$ for $p^r - p + 1 \leqq q < p^{r+1} - p + 1$. Hence, as $l(s_i^{k\alpha_1 p^n}) < l(x)$, $s_i^{k\alpha_1 p^n} = s_{i+p-1}^{B_1} \cdots s_{i+p-2+q}^{B_q} \cdots$, where $p^{n-r} \mid B_q$ for $p^r - p + 1 \leqq q < p^{r+1} - p + 1$ and $0 \leqq B_q < p^n$, by the induction hypothesis (b). Also, $y^{kp^n} = s_{i+p-2}^{C_1} \cdots s_{i+p-3+k}^{C_h} \cdots$, where $0 \leqq c_h < p^n$ and $p^{n-r} \mid C_h$ for $p^r - p + 1 \leqq h < p^{r+1}$, by the induction hypothesis (b). Hence $x^{kp^n} = s_{i+p-1}^{B_1} \cdots s_{i+p-2+q}^{B_q + C_{q-1}} \cdots$, where $p^{n-r} \mid B_q + C_{q-1}$ for $p^r - p + 1 \leqq q < p^{r+1} - p + 1$ $(C_0 = 0)$ and part (a) follows from this by the induction hypothesis (b).

We prove (b). Let $\beta_j = k_j p^n + h_j$, where $0 \leqq h_j < p^n$ and $p^{n-r} \mid h_j$ for $p^r \leqq j < p^{r+1}$, $0 \leqq r \leqq n-1$. Then $x = (s_i^{k_i} \cdots s_{m-1}^{k_{m-1}})^{p^n} \cdots s_{m-1}^{h_{m-i}}$. By part (a)

$$(s_i^{k_i} \cdots s_{m-1}^{k_{m-1}})^{p^n} = s_{i+p-1}^{u_p} \cdots s_{m-1}^{u_{m-i}},$$

where $p^{n-r} \mid u_j$ for $p^r \leqq j < p^{r+1}$, $1 \leqq r \leqq n-1$ and $0 \leqq u_j < p^n$. Hence $x = s_i^{h_1} \cdots s_{i+p-2}^{h_{p-1}} \cdot z$, where

$$z = \prod_{t=0}^{m-i+p} s_{i+p-1+t}^{u_{p+t} + h_{p+t}}.$$

Since $l(z) < l(x)$, $z = \Pi_{t=0}^{m-i+p} s_{i+p-1+t}^{v_{p+t}}$, where $0 \leqq v_{p+t} < p^n$ and $p^{n-r} \mid v_j$ for $p^r \leqq j < p^{r+1}$, by the hypothesis (b) of the proposition. Consequently x has the desired representation.

The proof of the following lemma is elementary and straightforward, hence we omit it.

LEMMA 1. *Let $m, n\ \alpha, \delta \in \mathbf{Z}$, $m \geqq 3$, $n \geqq 2$, $0 \leqq \alpha$, $\delta \leqq p^n - 1$. Then there exists a unique p-group P of type (m,n) with $P_1' = 1$, s.t. $P = \langle s, s_1 \rangle$, for every i, $2 \leqq i \leqq m-1$, $s_i = [s_{i-1}, s]$, $(ss_i)^{p^n} = s_{m-1}^{\alpha}$ and $s^{p^n} = s_{m-1}^{\delta}$.*

We come now to the main result of this section:

THEOREM 1. *Let F be the free group generated by x and y and let*

$$(*) \qquad (xy)^{p^n} = x^{p^n} y^{p^n} c_2^{\binom{p^n}{2}} \cdots c_t^{\binom{p^n}{t}} \cdots c_{p^n},$$

$c_i \in K_i(F) := K_i$ by the collection formula, $c_i \equiv [y,(i-1)x]^{\alpha_i} \pi [y, z_1, \cdots, z_{i-1}] \bmod K_{i+1}$,

$$[y, z_1, \cdots, z_{i-1}] \not\equiv [y,(i-1)x] \bmod K_{i+1}, \quad z_t \in \{x, y\}.$$

Then $\alpha_{p^i}\binom{p^n}{p^i} \equiv \binom{p^n}{p^i} + r \cdot p^{n-i+1} \bmod p^n$, *for some integer* r.

PROOF. By Lemma 1, to every i, $1 \leqq i \leqq n$ there exists a p-group P of type $(p^i + 1, n)$ with abelian P_1 such that

$$(ss_1)^{p^n} = s^{p^n} s_1^{p^n} s_2^{\binom{p^n}{2}} \cdots s_{p^n}.$$

Let $1 \to N \to F \xrightarrow{\tau} P \to 1$ be a presentation of P, $x^\tau = s$, $y^\tau = s_1$. Obviously we have

$$(*)(*) \qquad \begin{cases} K_{p^i}(F)^\tau = K_{p^i}(P) = P_{p^i}, \\ ([y, (i-1)x]^{\alpha_i})^\tau = [s_1, (i-1)s]^{\alpha_i} = s_i^{\alpha_i}. \end{cases}$$

Hence there exist elements $d_i = c_i^\tau \in P_i$, $d_i = s_i^{\alpha_i} u_i$, $u_i \in P_{i+1}$ s.t.

$$(ss_1)^{p^n} = s^{p^n} \cdot s_1^{p^n} \cdot d_2^{\binom{p^n}{2}} \cdots d_{p^n}.$$

On the other hand

$$(ss_1)^{p^n} = s^{p^n} \cdot s_1^{p^n} s_2^{\binom{p^n}{2}} \cdots s_{p^n}.$$

Hence

$$s_2^{\binom{p^n}{2}} \cdots s_{p^n} = d_2^{\binom{p^n}{2}} \cdots d_{p^n}.$$

Since P is a p-group of type $(p^i + 1, n)$

$$(*)(*)(*) \qquad s_2^{\binom{p^n}{2}} \cdots s_t^{\binom{p^n}{t}} \cdots s_{p^i}^{\binom{p^n}{p^i}} = d_2^{\binom{p^n}{2}} \cdots d_{p^i}^{\binom{p^n}{p^i}}.$$

By Proposition 2(a)

$$s_t^{\binom{p^n}{t}} = s_t^{c_t} \cdots s_{t+\mu}^{c_{t+\mu}} \cdots s_{p^i}^{\varepsilon_t}, \qquad d_t^{\binom{p^n}{t}} = s_t^{h_t} \cdots s_{t+\mu}^{h_{t+\mu}} \cdots s_{p^i}^{\varepsilon_t},$$

where $0 \leqq \mu \leqq p^i - t$, $p^{n-i+1} \mid \varepsilon_t$ and $p^{n-i+1} \mid e_t$ for $2 \leqq t \leqq p^i - 1$. Hence

$$d_2^{\binom{p^n}{2}} \cdots d_{p^i-1}^{\binom{p^n}{p^i-1}} = s_2^{a_2} \cdots s_j^{a_j} \cdots s_{p^i}^{e}, \qquad s_2^{\binom{p^n}{2}} \cdots s_{p^i-1}^{\binom{p^n}{p^i-1}} = s_2^{b_2} \cdots s_j^{b_j} \cdots s_{p^i}^{e},$$

where $0 \leqq a_j$, $b_j < p^n$ for $2 \leqq j \leqq p^i - 1$, $e \equiv \Sigma e_t \equiv 0 \bmod p^{n-i+1}$ and $\varepsilon = \Sigma \varepsilon_t \equiv 0 \bmod p^{n-i+1}$ (see Proposition 2). Therefore, considering the exponents of s_{p^i} in the left-hand side and the right-hand side of $(*)(*)(*)$, we find that

$$e + \binom{p^n}{p^i} \equiv \varepsilon + \alpha_{p^i}\binom{p^n}{p^i} \bmod p^n.$$

Consequently,

$$\alpha_{p^i}\binom{p^n}{p^i} \equiv \binom{p^n}{p^i} + rp^{n-i+1} \bmod p^n \qquad \text{for some integer } r,$$

as required.

COROLLARY 1. $\alpha_{p^i} \equiv 1 \bmod p$.

COROLLARY 2. *In the expansion of* $(xy)^{k \cdot p^n}$, $(k,p)=1$ *by the collection formula* $\alpha_{p^i} \equiv k \bmod p$.

These corollaries follows by the facts:

$$p^{n-i} \Big\| \binom{p^n}{p^i} \quad \text{and} \quad \binom{k \cdot p^n}{p^i} \equiv kp^{n-i} \bmod p^n.$$

2. The order of s_i

In this section we assume that P is a p-group of type (m,n) and notations are as in the previous sections.

Let $x = s_i^{\alpha_i} \cdot s_{i+1}^{\alpha_{i+1}} \cdots s_{m-1}^{\alpha_{m-1}}$, $0 \leqq \alpha_t \leqq p^n$. We say that x is an *admissible word* (a.w.) if, for every i, $p^\alpha \leqq i \leqq p^{\alpha+1}-1$, $p^{n-\alpha} \mid \alpha_i$. We say that the depth $l(x)$ of x is i if $\alpha_i \neq 0$ but for every $t>0$, $\alpha_{i-t}=0$.

Denote by Λ the set of all the admissible words of P.

THEOREM 1. *Let* $x = s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_{m-1}^{\alpha_{m-1}}$ *and* $y = s_1^{\beta_1} \cdots s_{m-1}^{\beta_{m-1}}$, $0 \leqq \alpha_i, \beta_i \leqq p^n$, *be two admissible words. Then*

(a) $x \cdot y \in \Lambda$.

(b) *For every* $u \in P$, $[x,u] \in \Lambda$.

(c) *If* $z = s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}}$, $p^\alpha \leqq i < p^{\alpha+1}$ *then* $z^{ap^r} \in \Lambda$ *for* $r \geqq n-\alpha$, $(a,p)=1$.

(In other words Λ is a normal — in fact characteristic — subgroup of P which contains $\Omega_r(P_i)$ for i and r as in (c).)

PROOF. Let $l(x)=i$, $l(y)=j$. Suppose that we have proved the theorem for a.w.s x and y with $j \geqq i$. If u and v are a.w.s. $l(u)=i$, $l(v)=j$, and $j<i$ then $u \cdot v$ is an a.w.: $u \cdot v = v \cdot u \cdot [u,v]$. Now, by (a) $v \cdot u$ is an a.w. and by (b) $[u,v]$ is an a.w. and $l([u,v])>i$. Hence by (a) $uv = v \cdot u[u,v] \in \Lambda$. Therefore, without loss of generality, we may assume that $l(y) \geqq l(x)$.

Assume that the theorem is true for a.w.s with depth $i+1$ and prove it is true for i. First we prove (a). suppose $y = s_j^b$, $j \geqq i$ $(y \in \Lambda)$.

CLAIM. $x \cdot s_j^b \in \Lambda$.

PROOF. $x \cdot s_j^b = s_i^{\alpha_i} s_{i+1}^{\alpha_{i+1}} \cdots s_{m-1}^{\alpha_{m-1}} \cdot s_j^b = s_i^{\alpha_i} \cdots s_{m-1-j}^{\alpha_{m-1-j}} \cdot s_j^b \cdot s_{m-j}^{\alpha_{m-j}} \cdots s_{m-1}^{\alpha_{m-1}}$. We may assume $m-1-j>j \geqq i$. $s_{m-j-1}^{\alpha_{m-j-1}} \cdot s_j^b = s_j^b s_{m-j-1}^{\alpha_{m-j-1}} [s_{m-j-1}^{\alpha_{m-j-1}}, s_j^b]$. Since $i<m-1-j$, it follows from the induction hypothesis (b) that $[s_{m-1-j}^{\alpha_{m-1-j}}, s_j^b] \in \Lambda$ and hence $s_{m-j-1}^{\alpha_{m-j-1}} [s_{m-j-1}^{\alpha_{m-j-1}}, b_j^b] \in \Lambda$, by (a). By a similar application of the identity $\zeta\eta = \eta\xi[\xi,\eta]$ $m-2j-1$ times, we obtain

$$xs_j^b = s_i^{\alpha_i} s_{i+1}^{\alpha_{i+1}} \cdots s_j^{\alpha_j+b} \cdots s_{j+1}^{b_{j+1}} \cdots s_{m-1}^{b_{m-1}}$$

and the subword $s_j^{\alpha_j+b} \cdot s_{j+1}^{b_{j+1}} \cdots s_{m-1}^{b_{m-1}}$ is an a.w. But then $x \cdot s_j^b$ is an a.w. by its definition. This proves our Claim.

Let $j \geqq i$ and let $y = s_j^{\beta_j} \cdots s_{m-1}^{\beta_{m-1}}$. Then

$$\begin{aligned} x \cdot y &= (s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}})(s_j^{\beta_j} \cdots s_{m-1}^{\beta_{m-1}}) \\ &= (s_i^{\alpha_i} \cdots s_{j-1}^{\alpha_{j-1}} \cdot s_j^{\alpha_j+\beta_j} s_{i+1}^{\delta_{j+1}} \cdots s_{m-1}^{\delta_{m-1}}) \cdot s_{j+1}^{\beta_{j+1}} \cdots s_{m-1}^{\beta_{m-1}} \end{aligned}$$

and by our Claim the word $s_i^{\alpha_i} \cdots s_{j-1}^{\alpha_{j-1}} s_j^{\alpha_j+\beta_j} s_{j+1}^{\delta_{j+1}} \cdots s_{m-1}^{\delta_{m-1}}$ is admissible. Hence, again by our Claim, $(s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}}) \cdot s_j^{\beta_j} \cdot s_{j+1}^{\beta_{j+1}}$ is an a.w. If we apply the last Claim $m-1-j$ times we obtain that $x \cdot y$ is an a.w. To prove (b) we denote $x_{i+t} = s_{i+t}^{\alpha_{i+t}} \cdots s_{m-1}^{\alpha_{m-1}}$ for $t \geqq 1$. Then to every $u \in P$,

$$[x, u] = [s_i^{\alpha_i}, u]^{x_{i+1}} [s_{i+1}^{\alpha_{i+1}}, u]^{x_{i+2}} \cdots [s_{i+t}^{\alpha_{i+t}}, u]^{x_{i+t+1}} \cdots [s_{m-2}^{\alpha_{m-2}}, u].$$

Now, for $t \geqq 1$, $[s_{i+t}, u]$ is an a.w. by the induction hyp(b). Hence

$$[s_{i+t}, u]^{x_{i+t+1}} = [s_{i+t}, u][s_{i+t}, u, x_{i+t+1}]$$

is an a.w. by (a) and (b). Therefore, by (a)

$$(*) \qquad \prod_{t=1}^{m-1} [s_{i+t}^{\alpha_{i+t}}, u]^{x_{i+t+1}} \quad \text{is an a.w.}$$

and it remains only to show that $[s_i^{\alpha_i}, u]^{x_{i+1}}$ is an a.w. For this it suffices to show that $[s_i^{\alpha_i}, u]$ is an a.w. We may assume $i < p^n$ and $p^{n-\alpha} \mid \alpha_i$. By the collection formula

$$[s_i^{\alpha_i}, u] = s_i^{-\alpha_i}(s_i^{\alpha_i})^u = s_i^{-\alpha_i}(s_i^u)^{\alpha_i} = (s_i^{-1} s_i^u)^{\alpha_i} \cdot k_2^{\binom{\alpha_i}{2}} \cdots k_{\alpha_i} = [s_i, u]^{\alpha_i} k_2^{\binom{\alpha_i}{2}} \cdots k_{\alpha_i},$$

where $k_j \in K_j(\langle s_i, [s_i, u]\rangle) \leqq P_{(i+1)+i(j-1)} = P_{j_0}$, $j_0 = i \cdot j + 1$. We prove that $k_j^{\binom{\alpha_i}{j}}$ and $[s_i, u]^{\alpha_i}$ are a.w. by using (c). To apply (c) to $k_j^{\binom{\alpha_i}{j}}$ we have to show that if

$$\binom{\alpha_i}{j} = p^q b \ (b, p) = 1 \quad \text{and} \quad p^\varepsilon \leqq j_0 < p^{\varepsilon+1}$$

then $q \geqq n - \varepsilon$. If $j = p^h d$, $(d, p) = 1$, then $i \cdot p^h d = ij < j_0$. Hence, if $p^\alpha \leqq i < p^{\alpha+1}$ then $p^{\alpha+h} \leqq j_0 < p^{\alpha+h+1}$ and we have to show $q \geqq n - (\alpha + h)$. Let $\alpha_i = a \cdot p^r$, $(a, p) = 1$. Then $q \geqq r - h$. But $n - \alpha \leqq r$, by the definition of an a.w., hence $n - \alpha - h \leqq r - h \leqq q$ and we may apply (c). Therefore $\Pi_{j=2}^{\alpha_i} k_j^{\binom{\alpha_i}{j}}$ is admissible by (a) and (c). We show that $[s_i, u]^{\alpha_i}$ is admissible. Since $[s_i, u] \in P_{i+1}$, obviously $[s_i, u]^{\alpha_i}$ is an a.w., by applying (c) to $z = [s_i, u]$ with $l(z) \leqq m - i - 1$. This shows that $[s_i^\alpha, u]$ is an a.w. and by (a) and (*) $[x, u]$ is.

Finally we prove (c). Let $z = s_i^{\gamma_i} u$, $u = s_{i+1}^{\gamma_{i+1}} \cdots s_{m-1}^{\gamma_{m-1}}$. If $b = a \cdot p^r$, $(a,p) = 1$, then by the collection formula

$$z^b = (s_i^{\gamma_i} u)^b = s_i^{\gamma_i b} k_2^{\binom{b}{2}} \cdots k_j^{\binom{b}{j}} \cdots k_b,$$

$k_j \in K_j(\langle s_i^{\gamma_i}, u\rangle) \leqq P_{i(j-1)+i+1} = P_{j_0}$, $j_0 = ij + 1$. Just as in the proof of (b) we find that $k_j^{\binom{b}{j}}$ is admissible. Since $u \in G_{i+1}$, u^b is admissible by (c) and since $r \geqq n - \alpha$, $(s_i^{\gamma_i})^b$ is admissible. Hence z^b is an a.w. by (a). Q.E.D.

REMARK. Let $x = s_1^{\alpha_1} \cdots s_{m-1}^{\alpha_{m-1}}$. We say that x is admissible of rank r, if $p^{n-\alpha+r-1} \mid \alpha_i$ for $p^\alpha \leqq i < p^{\alpha+1}$ and we say that $x = s_j^{\alpha_1} \cdots s_{m-1}^{\alpha_{m-1}}$ is admissible of rank r with respect to j if x is admissible of rank r in the subgroup $H_j = \langle G_j, s\rangle$. By using the same arguments as in the proof of the previous theorem we may prove:

THEOREM 2. *Let* $x = s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_{m-1}^{\alpha_{m-1}}$, $y = s_1^{\beta_1} s_2^{\beta_2} \cdots s_{m-1}^{\beta_{m-1}}$, $0 \leqq \alpha_i, \beta_i$.

(a) *If x is admissible of rank r and y is admissible of rank r w.r. to j, $j \geqq 2$, then xy is admissible of rank r and* $xy = s_1^{\varepsilon_1} \cdots s_{m-1}^{\varepsilon_{m-1}}$, $\varepsilon_i \equiv \alpha_i \bmod p^{n-\alpha+r}$ *for* $p^\alpha \leqq i < p^{\alpha+1}$.

(b) *If x is admissible of rank r then for every u, $[x,u]$ is admissible of rank r w.r. to* 2.

(c) *If x is admissible of rank r then x^{p^a} is admissible of rank $r + a$ and if* $x^{p^a} = s_i^{\beta_i} \cdots s_{m-1}^{\beta_{m-1}}$ *then* $\beta_i \equiv p^a \alpha_i \bmod p^{n-\alpha+r+a}$ *for* $p^\alpha \leqq i < p^{\alpha+1}$.

(d) *If x and y are admissible of rank r then $x \cdot y$ is.*

(e) *If x is admissible of rank r then to every $u \in P$, $[x,u]$ is.*

(f) *If* $z = s_i^{\delta_i} \cdots s_{m-1}^{\delta_{m-1}}$ *and* $p^\alpha \leqq i < p^{\alpha+1}$ *and* $t \geqq n - \alpha + r - 1$ *then* z^{ap^t} *is admissible of rank r,* $(a,p) = 1$.

The next theorem shows that a formula analogous to (4) holds for a nonmetabelian p-group of type (m,n).

THEOREM 3. *Let P be a p-group of type (m,n) and let k be a natural number, $(k,p) = 1$. Then there exist natural numbers e_j^i such that*

$$s_1^{kp^n} \cdot s_2^{e_2^1} \cdot s_3^{e_3^1} \cdots s_{p^n}^{e_{p^n}^1} \cdot u_1 = 1, \quad u_1 \in P_{p^n+1} \cdot Z(P)$$

and for $i \geqq 2$

$$s_i^{kp^n} \cdot s_{i+1}^{e_2^i} \cdots s_{i+p^n-1}^{e_{p^n}^i} \cdot u_i, \qquad u_i \in P_{p^n+i}.$$

The e_j^i's satisfy:

$$(*) \qquad p^{n-\alpha} \mid e_j^i \textit{ for } p^\alpha \leqq j < p^{\alpha+1} \quad \textit{and} \quad p^{n-\alpha} \,\|\, e_j^i \textit{ for } j = p^\alpha.$$

If P is embedded in a p-group of type $(m+1, n)$ then for $i = 1$, $u_1 \in P_{p^n+1}$.

PROOF. It follows from the collection formula and 0.2(e) that

$$s_1^{kp^n} c_2^{\binom{kp^n}{2}} \cdots c_t^{\binom{kp^n}{t}} \cdots c_{p^n} \cdot z = 1, \qquad c_i \in P_i, \quad z \in Z(P).$$

By Theorem 1 $c_i^{\binom{kp^n}{i}}$ are admissible words, hence $s_1^{kp^n} \cdot c_2^{\binom{kp^n}{2}} \cdots c_t^{\binom{kp^n}{t}} \cdots c_{p^n}^{\binom{kp^n}{p^n}}$ is. Therefore there exist numbers e_j, $0 \leqq e_j \leqq p^n$ s.t.

$$s_1^{kp^n} \cdot c_2^{\binom{kp^n}{2}} \cdots c_{p^n}^{\binom{kp^n}{p^n}} = s_1^{kp^n} \cdot s_2^{e_2} \cdots s_{p^n}^{e_{p^n}} u_0,$$

$u_0 \in P_{p^n+1}$ and for $p^\alpha \leqq j < p^{\alpha+1}$, $p^{n-\alpha} \mid e_j$. It remains to show that $p^{n-\alpha} \| e_j$ for $j = p^\alpha$. The exponent of s_{p^α} in c_{p^α} is

$$k_\alpha \equiv \binom{kp^\alpha}{p^\alpha} + rp^{n-\alpha+1} \bmod p^n,$$

by Theorem 1.1. We prove that the contribution of $\Pi_{i=2}^{p^\alpha-1} c_i^{\binom{kp^n}{i}}$ to the exponent of s_{p^α} is divisible by $p^{n-\alpha+1}$. Let $c_i = s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}}$. Denote

$$\binom{kp^n}{i} = r.$$

Then, by the collection formula,

$$c_i^r = s_i^{\alpha_i r} \cdots s_{m-1}^{\alpha_{m-1} r} \cdot d_2^{\binom{r}{2}} \cdots d_t^{\binom{r}{t}} \cdots d_r, \qquad d_t \in P_{t \cdot i+1}.$$

If $p^\beta \leqq t < p^{\beta+1}$ then $p^{\alpha+\beta} < ti + 1$. Hence as $p^{n-(\alpha+\beta)} \mid \binom{r}{t}$, $d_t^{\binom{r}{t}} \in \Lambda(P_2)$ by Theorem 1(c) and $\Pi d_t^{\binom{r}{t}} \in \Lambda(P_2)$ by Theorem 1(a). Therefore

$$c_i^{\binom{kp^n}{i}} \equiv s_i^{\alpha_i \binom{p^n}{i}} \cdots s_{m-1}^{\alpha_{m-1} \binom{p^n}{i}} \bmod \Lambda(P_2).$$

Now, if $x = s_1^{\alpha_1} \cdots s_{m-1}^{\alpha_{m-1}}$, $y = s_1^{\beta_1} \cdots s_{m-1}^{\beta_{m-1}}$ are elements of $\Lambda(P_1)$ then as $[s_i^{\alpha_i}, s_j^{\beta_j}] \in \Lambda(P_2)$ by Theorem 2(b),

$$x \cdot y \equiv s_1^{\alpha_1+\beta_1} \cdots s_{m-1}^{\alpha_{m-1}+\beta_{m-1}} \bmod \Lambda(P_2).$$

Hence

$$\prod_{i=2}^{p^\alpha-1} c_i^{\binom{kp^n}{i}} \equiv s_2^{\delta_2} \cdots s_{m-1}^{\delta_{m-1}} \bmod \Lambda(P_2), \qquad p^{n-\alpha+1} \mid \delta_j, \quad i \leqq j$$

and by Theorem 2(a)

$$\prod_{i=2}^{p^\alpha} c_i^{\binom{p^n}{i}} \equiv s_2^{\varepsilon_2} \cdots s_{p^\alpha}^{\varepsilon_{p^\alpha}} \bmod P_{p^\alpha+1}, \qquad \text{where } \varepsilon_{p^\alpha} \equiv k_\alpha \bmod p^{n-\alpha+1}.$$

Hence the e_j^1 satisfy the required conditions. If P is embedded in a p-group of type $(m+1, n)$ then by Proposition 0.2 $(ss_1)^{kp^n} = s^{kp^n}$. Hence the results follow by the case $i = 1$ and by Lemma 0.1 considering the subgroups $H_i = \langle P_i, s\rangle$, $i \geqq 2$.

The following two theorems refine Theorem 3. Theorem 5 gives a formula for $s_i^{p^{n-1+t}}$.

THEOREM 4. *Let P be a p-group of type (m, n). Then for every k, $(k, p) = 1$,*

$$s_1^{kp^n} \equiv \prod_{\mu=0}^{m-p-1} s_{p+\mu}^{b_{\mu+1}} \bmod Z(P)\cdot P_{i+p^n}$$

and for $i \geqq 2$, or if P is embedded in a p-group of type $(m+1, n)$ P_0 then for $i \geqq 1$,

$$s_i^{kp^n} \equiv \prod_{\mu=0}^{m-p-i} s_{i+p-1+\mu}^{b_{\mu+1}} \bmod P_{i+p^n}.$$

The b_μ's satisfy

$$(*)(*) \qquad \begin{cases} p^{n-\alpha} \mid b_{\mu+1} & \text{for } p^{\alpha-1} - p \leqq \mu \leqq p^\alpha - p - 1, \\ p^{n-\alpha} \| b_\mu & \text{for } \mu = p^\alpha - p. \end{cases}$$

PROOF. By Theorem 3, $s_1^{kp^n} = s_2^{e_2} s_3^{e_3} \cdots s_{p^n}^{e_{p^n}} u$ where $p^n \mid e_i$ for $2 \leqq i \leqq p-1$, the e_j's satisfy $(*)$ for $j \geqq p$, and $u \in P_{p^n+1}$ if P is embedded in P_0, $u \in P_{p^n+1}Z(P)$ if P is not embedded in P_0. Hence, by Theorem 1(c)

$$s_1^{kp^n} \equiv s_p^{e_p} \cdots s_{p^n}^{e_{p^n}} u \bmod \Lambda(P_2)$$

and by Theorem 2(a) $s_1^{kp^n} = s_p^{\varepsilon_p} \cdots s_{p^n}^{\varepsilon_{p^n}} u$, where $\varepsilon_i \equiv e_i \bmod p^{n-\alpha+1}$ for $p^\alpha \leqq i < p^{\alpha+1}$. This proves the theorem for $i = 1$. For $i \geqq 2$ we consider the subgroups $H_i = \langle P_i, s\rangle$ and apply Lemma 0.1 to the result for $i = 1$.

THEOREM 5. *Let P be a p-group of type (m, n). Then*

(1) *To every k with $(k, p) = 1$ and to every $t \geqq 1$,*

$$s_1^{kp^{n-1+t}} = s_{1+t(p-1)}^{a_0} \cdots s_{1+t(p-1)+\mu}^{a_\mu} \cdots s_{1+t(p-1)+p^n-p}^{a_{p^n-p}} \cdot u_1,$$

where $u_1 \in P_{1+t(p-1)+p^n-p+1} \cdot Z(P)$.

(2) *If P is embedded in a p-group P_0 of type $(m+1, n)$ then for every $i \geqq 1$ and every $t \geqq 1$*

$$s_i^{kp^{n-1+t}} = s_{i+t(p-1)}^{a_0} \cdots s_{i+t(p-1)+\mu}^{a_\mu} \cdots s_{i+t(p-1)+p^n-p}^{a_{p^n-p}} \cdot u_i \quad \textit{where } u_i \in P_{i+t(p-1)+p^n-p+1}.$$

The a_j's in (1) and (2) satisfy

$$p^{n-\alpha} \mid a_\mu \quad \text{for } p^\alpha - p \leqq \mu < p^{\alpha+1} - p,$$

$$p^{n-\alpha} \| a_\mu \quad \text{for } \mu = p^\alpha - p.$$

PROOF. CLAIM 1. *Let* $x = s_p^{a_p}\cdots s_{p^n}^{a_{p^n}}v$, $v\in P_{p^n+1}$, *be an admissible word, i.e.* $x\in\Lambda(P_1)$. *Then* $x^p\in\Lambda(P_p)$.

PROOF. Induction on $l(x)$. $x = s_p^{\alpha}u$, $u\in P_{p+1}$, $p^{n-1}\mid\alpha$ $(\alpha = a_p)$ and $u\in\Lambda(P_1)$. By the collection formula

$$x^p = (s_p^{\alpha}u)^p = s_p^{\alpha p}u^p c_2^{\binom{p}{2}}\cdots c_p,\qquad c_i\in K_i(\langle s_p^{\alpha}, u\rangle).$$

Now, $s_p^{\alpha p}\in\Lambda(P_p)$ by definition and $u^p\in\Lambda(P_p)$ by hypothesis. We show that

$$c_i^{\binom{p}{i}}\in\Lambda(P_p).$$

$u\in\Lambda(P_1)\Rightarrow c_i\in\Lambda(P_1)\cap P_{p+1}$ by Theorem 1(b). Hence, for $2\leqq t\leqq p-1$, $c_i^{\binom{p}{i}}\in\Lambda(P_p)$. Finally $c_p\in P_p$ by Theorem 2(b). Therefore by Theorem 1(a) $x^p\in\Lambda(P_p)$.

CLAIM 2. *If* $x,u\in\Lambda(P_1)$ *then* $[x,u]\in\Lambda(P_{p+1})$.

PROOF. Induction on $l(x)$. Let $x = s_i^{\alpha}v$, $p\mid\alpha$, $v\in P_{i+1}$. $[x,u]=[s_i^{\alpha}\cdot v,u]=[s_i^{\alpha},u]\cdot[s_i^{\alpha}\cdot u, v][v,u]$. By the induction hypothesis $[v,u]\in\Lambda(P_{p+1})$ and if we show that $[s_i^{\alpha},u]\in\Lambda(P_{p+1})$ then $[x,u]\in\Lambda(P_{p+1})$, by Theorem 1. By the collection formula

$$[s_i^{\alpha},u]=[s_i,u]^{\alpha}c_2^{\binom{p}{2}}\cdots c_{\alpha},\qquad c_t\in K_t(\langle[s_i,u],u\rangle)\leqq P_{i(t+1)+1}.$$

By Theorem 1 $[s_i,u]\in\Lambda(P_1)$ and by assumption $u\in\Lambda(P_1)$. Hence by the induction hypothesis

$$c_t^{\binom{d}{t}}\in\Lambda(P_{p+1})\qquad\text{for } t\geqq 2$$

and by Theorem 1

$$\prod_t c_t^{\binom{d}{t}}\in\Lambda(P_{p+1}).$$

Since $[s_i,u]\in\Lambda(P_2)$ by Theorem 2(b), $[s_i,u]^{\alpha}\in\Lambda(P_{p+1})$ by Claim 1 and $[x,u]\in\Lambda(P_{p+1})$ by Theorem 1.

We prove Theorem 5 by induction on t. As we have seen in the proofs of the previous theorems, we may assume $i=1$ and P is embedded in P_0. By assumption

$$s_1^{kp^{n-1+t+1}} = (s_1^{kp^{n-1+t}})^p = (s_{1+t(p-1)}^{a_0}\cdots s_{1+t(p-1)+p^n-p}^{a_{p^n-p}}u_1)^p.$$

By the collection formula

$$(s_{1+t(p-1)}^{a_0}\cdots s_{1+t(p-1)+p^n-p}^{a_{p^n-p}}\cdot u_1)^p = s_{1+t(p-1)}^{a_0p}\cdots s_{1+t(p-1)+p^n-p}^{pa_{p^n-p}}\cdot u_1^p\cdot c_2^{\binom{p}{2}}\cdots c_p,$$

$$c_i\in K_i(\langle s_{1+t(p-1)}^{a_0}\cdots s_{1+t(p-1)+p^n-p}^{a_{p^n-p}}, u_1\rangle).$$

Hence by the last Claim

$$s_1^{kp^{n-1+t+1}} \equiv s_{1+t(p-1)}^{a_0 p} \cdots s_{1+t(p-1)+p^n-p}^{p \cdot a_{p^n-p}} u_1^p \bmod \Lambda(P_{2+(t+1)(p-1)}).$$

Since for $\mu \geqq 1$, u_1, $s_{1+t(p-1)+\mu}^{a_\mu} \in \Lambda(P_{2+t(p-1)})$, by Claim 1,

$$u_1^p, s_{1+t(p-1)+\mu}^{pa_\mu} \in \Lambda(P_{2+(t+1)(p-1)}).$$

Hence $s_1^{kp^{n-1+t+1}} \equiv s_{1+t(p-1)}^{a_0 p} \bmod \Lambda(P_{2+(t+1)(p-1)})$. By assumption $p^{n-1} \| a_0$. Hence $p^n \mid a_0 p$ and by Theorem 4

$$s_1^{kp^{n-1+t+1}} \equiv s_{1+(t+1)(p+1)}^{b_0} \cdots s_{s+(t+1)(p-1)+\mu}^{b_\mu}$$

$$\cdots s_{1+(t+1)(p-1)+p^n-p}^{b_{p^n-p}} \bmod \Lambda(P_{2+(t+1)(p-1)}) \cdot P_{2+(t+1)(p-1)+p^n-p},$$

where the b_μ's satisfy $(*)(*)$. Therefore our theorem follows from Theorem 2(a).

The following theorem is the main result of this section.

THEOREM 6. *Let P be a p-goup of type (m, n) and let $m = (p-1)q + r$, $0 \leqq r \leqq p-2$. For every i, $1 \leqq i \leqq m-1$, let $i = q_i(p-1) + r_i$, $0 \leqq r_i \leqq p-2$ and define $\delta(i) = 1$ if $r_i < r$, $\delta(i) = 0$ if $r_i \geqq r$. Denote $l_p(p^e) = e$. Then $l_p|s_i| = q - q_i + n - 1 + \delta(i)$ for $i \geqq 1$ if P is embedded in a p-group P_0 of type $(m+1, n)$ and for $i \geqq 2$ if P is not embedded in P_0.*

PROOF. By induction on $\mathrm{cl}(P)$. If $\mathrm{cl}(P) \leqq p-1$ then $|s_i| = p^n$ by Lemma 0.2. For $i < p-1$ $q = q_i = 0$, $\delta(i) = 1$ and for $i = p-1$, $q = q_i = 1$ and $\delta(i) = 0$, hence in any case the theorem is true. Assume we have proved the theorem for groups of type $(m-1, n)$. We prove it for groups of type (m, n). Assume first $r \geqq 2$. Then $1 + q(p-1) = 1 + m - r \leqq m-1$ and $1 + q(p-1) \geqq m - p + 3$. Therefore $P_{m-1} \leqq P_{1+q(p-1)} \leqq P_{m-p+2}$. By Theorem 5

$$s_1^{p^{n-1+q}} = s_{1+q(p-1)}^{b_0} \cdots s_{r-1+q(p-1)}^{b_{r-2}},$$

$p^{n-1} \| b_0$, $p^{n-1} \mid b_i$ for $i \geqq 1$. Hence, by Lemma 0.2 $s_1^{p^{n-1+q}}$ is of order p and $|s_1| = p^{n+q}$. By the notations of the theorem $r_1 = 1$, $\delta(1) = 1$, $q_1 = 0$ and $n + q = q - q_1 + n - 1 + \delta(1)$, as required.

If $r \leqq 1$ then by Theorem 5:

$$s_1^{p^{n-1+1-1}} = s_{1+(q-1)(p-1)}^{b_0} \cdots s_{q(p-1)}^{b_{p-2}} \qquad \text{for } r = 1,$$

$$s_1^{p^{n-1+q-1}} = s_{1+(q-1)(p-1)}^{b_0} \cdots s_{q(p-1)-1}^{b_{p-3}} \qquad \text{for } r = 0.$$

Since $p^{n-1} \| b_0$ and $p^{n-1} \mid b_j$ for $j \geqq 1$, $|s_1| = p^{n-1+q}$, by Lemma 0.2.

Now, $r_1 = 1$, $r \geqq 1$, $\delta(1) = 0$ and $q_1 = 0$. Hence $q - q_1 + \delta(1) + n - 1 = q + n - 1$. This proves the theorem for $i = 1$. Define $H_i = \langle P_i, s \rangle$ for $i \geqq 2$. H_i is a

p-group of type (m', n), $m' = m - i + 1$. Let $m' = q'(p-1) + r'$, $0 \leqq r' \leqq p-2$. Then $m' = m + i + 1 = q(p-1) + r - q_i(p-1) - r_i + 1 = (q - q_i)(p-1) + (r - r_i) + 1$. Hence if $0 \leqq r - r_i + 1 \leqq p-2$ then $r' = r - r_i + 1$, $q' = q - q_i$. Suppose $0 \leqq r - r_i + 1 \leqq p - 2$. Then by induction $lp(|s_i|) = n - 1 + q - q' + \delta'(i)$, where $\delta'(i) = 1$ for $r' > 1$ and $\delta'(i) = 0$ for $r' \leqq 1$, i.e. $\delta'(i) = 1$ for $r_i < r$ and $\delta'(i) = 0$ for $r_i \geqq r$. Therefore $\delta'(i) = \delta(i)$ and $lp(|s_i|) = n - 1 + q - q_i + \delta(i)$. If $r - r_i + 1 \geqq p - 1$ then $r - r_i + 1 = p - 1$ and this is possible only if $r = p - 2$, $r_i = 0$, $r' = 0$ and $m' = (q' + 1)(p - 1)$. By induction $lp(|s_i|) = n - 1 + q - q' + 1 + \delta'(i)$. We show that $1 + \delta'(i) = \delta(i)$. Since $r' = 0$, $\delta'(i) = 0$, and as $r_i = 0$ and $r = p - 2$, $\delta(i) = 1$. Hence $1 + \delta'(i) = \delta(i)$. Finally, assume $r - r_i + 1 < 0$. Then $r' = (p-1) + (r - r_i + 1)$, $m' = (q' - 1)(p - 1) + r'$ and by the induction hypothesis $lp(|s_i|) = n - 1 + q - q_i - 1 + \delta'(i)$, where $\delta'(i) = 1$ for $r' > 1$ and $\delta'(i) = 0$ for $r' \leqq 1$. We show that $\delta'(i) - 1 = \delta(i)$. $\delta'(i) = 1 \Leftrightarrow r' > 1 \Leftrightarrow p - 1 + (r - r_i) + 1 > 1 \Leftrightarrow r - r_i + p - 1 > 0 \Leftrightarrow r - r_i + 1 + (p-2) > 0$. Since $0 \leqq r$, $r_i \leqq p - 2$, $-p + 2 \leqq r - r_i \leqq 0$ and $-p + 3 \leqq r - r_i + 1$. Hence $r - r_i + 1 + p - 2 \geqq 1 > 0$ and $\delta'(i) = 1$. Now, $\delta(i) = 1$ for $r_i < r$ and $\delta(i) = 0$ for $r_i \geqq r$. Since $r - r_i + 1 < 0$, $\delta(i) = 0$ and $\delta(i) = \delta'(i) - 1$. This proves Theorem 6.

The following theorem, which essentially is a consequence of Theorem 5, has a different nature than the previous ones. It shows that for large i, $\mho_i(P_1)$ and the subgroups of admissible words of high rank coincide and they are regular.

THEOREM 7. *Let P be a p-group of type (m, n), $\exp(P_1) = p^e$, $e \geqq n$. Let $m = (p-1)q + r$, $0 \leqq r \leqq p - 2$ and $\delta(1)$ as in Theorem 6. Denote $u = m - p(p-1) + \delta(1)(p-1) - r$ if $e - p - n + 1 \geqq 0$ and let $u = p - 1$ if $e - p - n + 1 < 0$. Also denote $K = \mho_{e-p}(P_1)$ if $e - p - n + 1 \geqq 0$ and $K = \mho_n(P_1)$ if $e - p - n + 1 < 0$. Finally, for $t \leqq 0$ define*

$$H_{u+t} = \{x \in P_{u+t} \mid x = s_{u+t}^{\alpha_1} \cdots s_{m-1}^{\alpha_{m-u-t}}, p^{n-1} \mid \alpha_i\}.$$

Then

(a) $K = H_{u+1}$.

(b) $|K/\mho(K)| \leqq p^{p-1}$.

(c) *K is regular.*

(d) *If $1 \leqq i \leqq p$ and $e - i \geqq n$ then $\mho_{e-i}(P) \leqq \mho_{e-i}(P_1) \cdot \mho_{e-i-n}(P_{m-1})$.*

(e) *If $1 \leqq i \leqq p$ and $e - i - n \geqq n$ then $\mho_{e-i}(P_1) = \mho_{e-i}(P)$.*

PROOF. (a) First assume $e - p - n + 1 \geqq 0$. We show that $H_{u+1} \leqq \mho_{e-p}(P_1)$. By Theorem 5

$$s_1^{p^{e-p}} \equiv s_{1+(e-p-n+1)(p-1)}^{a_0} \bmod P_{2+(e-p-n+1)(p-1)}, \qquad \text{where } p^{n-1} \| a_0$$

and by Theorem 6

$$1+(e-p-n+1)(p-1)=1+(q+(n-1)+\delta(1)-p-(n-1))(p-1)$$
$$=m-p(p-1)+(\delta(1)(p-1)-r)+1=u+1.$$

Now, it follows from the definitions of $\delta(1)$ and r that $\delta(1)(p-1)-r+1 \geqq 0$ and $m-p(p-1) \geqq 1+(e-p-n+1)(p-1)=u+1$. Therefore $s_i^{p^{e-p}} \in H_{u+1}$ for $i \geqq 1$, by Theorem 5. We claim that

$$L=\langle s_i^{p^{e-p}} \mid 1 \leqq i \leqq m-1\rangle = H_{u+1}.$$

For this we show $s_{u+j}^{p^{n-1}} \in L$ for $j \geqq 1$. By Theorem 5 $s_{m-1-u}^{p^{e-p}} = s_{m-1}^{\alpha \cdot p^{n-1}}$, $(\alpha, p)=1$. Therefore $s_{m-1}^{p^{n-1}} \in L$. Suppose that $s_{m-t}^{p^{n-1}} \in L$ for $1 \leqq t \leqq i-1$. We prove that $s_{m-i}^{p^{n-1}} \in L$ $(i \leqq m-u-1)$. By Theorem 5 $s_{m-i-u}^{p^{e-p}} = s_{m-i}^{a_0} \cdots s_{m-1}^{a_{i-1}}$, $p^{n-1} \| a_0$, $p^{n-1} \mid a_i$, $i>0$. Hence by Theorem 1

$$s_{m-i-u}^{p^{e-p}} \cdot s_{m-i+1}^{-a_1} = s_{m-i}^{a_0} \cdot s_{m-i+1}^{a_1-a_1} \cdot s_{m-i+2}^{\beta_2} \cdots s_{m-1}^{\beta_{i-1}} = s_{m-i}^{a_0} \cdot s_{m-i+2}^{\beta_2} \cdots s_{m-1}^{\beta_{i-1}},$$

where $p^{n-1} \mid \beta_i$. This way we obtain an element $y = s_{m-i+1}^{\gamma_1} \cdots s_{m-1}^{\gamma_{i-1}}$, $p^{n-1} \mid \gamma_t$ s.t. $s_{m-i+u}^{p^{e-p}} \cdot y = s_{m-i}^{a_0}$. Therefore $s_{m-i}^{a_0} \in L$ and $H_{u+1} = L \leqq \mho_{e-p}(P_1)$. To show that $H_{u+i} = \mho_{e-p}(P_1)$ it is enough to show that $x^{p^{e-p}} \in H_{u+1}$ for every $x \in P_1$. By Theorem 2 (f) $x^{p^{e-p}}$ is an admissible word of rank $e-p-(n-1)$, hence $x^{p^{e-p}} = s_1^{a_1} \cdots s_{m-1}^{a_{m-1}}$, where $p^{e-p-\alpha} \mid a_i$ for $p^\alpha \leqq i \leqq p^{\alpha+1}-1$. If $i = 1+t(p-1)+j$, $0 \leqq t$, $0 \leqq j \leqq p-2$ then by Theorem 5 $s_i^{p^{e-p-t}} \in H_{u+1}$. Hence to show $s_i^{a_i} \in H_{u+1}$, it is enough to show $e-p-\alpha \geqq e-p-t$, i.e. $t \geqq \alpha$.

(*) For $\alpha \geqq 1$ $\quad p^\alpha \leqq i \Rightarrow p^\alpha \leqq 1+t(p-1)+j \Rightarrow \alpha \leqq \dfrac{p^\alpha-1-j}{p-1} \leqq t.$

If $\alpha = 0$ then $t=0$ and of course $s_i^{p^{e-p}} \in H_{u+1}$. Therefore $s_i^{a_i} \in H_{u+1}$ and consequently $x^{p^{e-p}} \in H_{u+1}$, i.e. $\mho_{e-p}(P_1) = H_{u+1}$. The same arguments show that $\mho_{e-p+1}(P_1) = H_{u+p}$. Assume now that $e-p-n+1<0$ and show that $\mho_n(P_1) = H_p$, $\mho_{n+1}(P_1) = H_{2p-1}$. $e-p-n+1<0 \Rightarrow q+\delta(1)-p<0 \Rightarrow q<p-\delta(1) \leqq p-1 \Rightarrow m \leqq p^2-2$. Hence $s_1^{p^n} = s_p^{a_0} s_{p+1}^{a_1} \cdots s_{m+1}^{a_{m-1-p}}$ by Theorem 5 and $p^{n-1} \| a_0$, $p^{n-1} \mid a_i$ for $i \geqq 1$. From this point on the proof is the same as for the case $e-p-n+1 \geqq 0$ but write p^n instead of p^{e-p} and p^{n+1} instead of p^{e-p+1}.

(b) $\mho(K) = H_{u+p}$. Hence $|K/\mho(K)| = |H_{u+1}/H_{u+p}| \leqq p^{p-1}$.

(c) Follows from (b) (see [8, p. 332]).

(d) Let $x = s^\alpha u$, $u \in P_1$ and denote $\varepsilon = e-i$. By the collection formula

$$x^{p^{e-i}} = (s^\alpha)^p \cdot u^{p^\varepsilon} \cdot c_2^{\binom{p^\varepsilon}{2}} \cdots c_t^{\binom{p^\varepsilon}{t}} \cdots c_\varepsilon, \qquad c_t \in K_t(\langle s^\alpha, u\rangle) \leqq P_t.$$

Now $(s^\alpha)^{p^\varepsilon} \in \mho_{\varepsilon-n}(P_{m-1})$, $u^{p^\varepsilon} \in \mho_\varepsilon(P_1)$, for $2 \leqq t \leqq p-1$,

$$c_t^{\binom{p^\varepsilon}{t}} \in \mho_\varepsilon(P_1) \quad \text{and} \quad c_p^{\binom{p^\varepsilon}{p}} \in \mho_{\varepsilon-1}(P_p).$$

But $\mho_{\varepsilon-1}(P_p) = \mho_{\varepsilon}(P_1)$ by part (a) of the theorem. Hence it is enough to show that for $t > p$

$$c_t^{\binom{p^\varepsilon}{t}} \in \mho_{\varepsilon}(P_1).$$

If $p+1 \leqq t$, $p^\alpha \leqq t \leqq p^{\alpha+1}-1$ and $1 + k(p-1) \leqq t \leqq (k+1)(p-1)$ then $\mho_{\varepsilon-\alpha}(P_t) \leqq \mho_{\varepsilon-k}(P_1)$ by the argument in (*), with k instead of t and t instead of i. Therefore

$$c_t^{\binom{p^\varepsilon}{t}} \in \mho_{\varepsilon-\alpha}(P_t) \leqq \mho_{e-i}(P_1)$$

and by (*)(*) $x^{p^{e-i}} \in \mho_{e-i}(P_1) \cdot \mho_{e-i-n}(P_{m-1})$ for $1 \leqq i \leqq p$.

(e) If $e-i-n \geqq n$ then $\mho_{e-i-n}(P_{m-1}) = 1$ and by part (d) the theorem $\mho_{e-i}(P) \leqq \mho_{e-i}(P_1)$. But obviously $\mho_{e-i}(P_1) \leqq \mho_{e-i}(P)$. This proves (e) and the theorem.

3. The p-degree of commutativity of P

If $m \geqq p+2$, then $[P_i, P_j] \leqq P_{i+j+1} \cdot \mho(P_{i+j})$ by Theorem 0.2. Our aim is here to strengthen this result.

Definition. $x = s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_t^{\alpha_t} \cdots s_{m-1}^{\alpha_{m-1}}$ is a *word of p rank r* if $p \mid \alpha_i$ for $1 \leqq i \leqq r$. If $\alpha_i = 0$ for $1 \leqq i \leqq \mu - 1$ but $\alpha_\mu = 0$ denote $l(x) = \mu$.

Definition. P has p-degree of commutativity k if to every i, j s.t. $i + j + k \leqq m-1$,

$$[s_i, s_j] \equiv s_{i+j}^{a_0} \cdots s_{i+j+t}^{a_t} \cdots s_{i+j+k}^{\alpha(i,j)} \bmod P_{i+j+k+1},$$

where $p \mid a_i$ for $0 \leqq i \leqq k-1$, but $p \nmid \alpha(i,j)$ for some i and j.

Denote by $\Gamma_\mu(P_i)$ the set of all the words of P_i of p-rank μ and write Γ_μ for $\Gamma_\mu(P_1)$. If P has p-degree of commutativity k, then $[s_i, s_j] \in \Gamma_k$ for every i, j.

Theorem 1. *Let P be a p-group of type (m, n) of p-degree of commutativity k, $k < (p^n + 1)/2$.*

(a) *If $k \leqq \mu \leqq 2k+1$ and $x, y \in \Gamma_\mu$, then $x \cdot y \in \Gamma_\mu$.*

(b) *If $x \in \Gamma_k$, $u \in \mathrm{Aut}(P_1)$, $|u| = p^r$ and to every i, $1 \leqq i \leqq m-1$, $[u, s_i] \in \Gamma_k \cap P_{i+1}$ then $[x, u] \in \Gamma_{2k+1}$.*

(c) $\mho(\Gamma_k) \leqq \Gamma_{2k+1}$.

Proof. Assume we have proved (a)–(c) for words x in Γ_μ or Γ_k resp. with $l(x) = i+1$ and we prove for x with $l(x) = i$. Suppose we proved the theorem for words x and y s.t. $i \leqq j$. If $u, v \in \Gamma_\mu$, $l(u) = i$, $l(v) = j$ and $j < i$ then we claim that $u \cdot v \in \Gamma_\mu$. Since P has p-degree of commutativity k, $[s_i, s_j] \in \Gamma_k$, hence by

(b) of the theorem, to every $a \in \Gamma_\mu$ (with $u = s_j$) $[a, s_j] \in \Gamma_\mu$. Therefore it follows from (b), now with $a = u$, that $[u, s_j] \in \Gamma_k$. But then to every $a, b \in \Gamma_\mu$, $[a, b] \in \Gamma_\mu$. Therefore $[u, v] \in \Gamma_\mu$ and since $uv = vu[u, v]$, $uv \in \Gamma_\mu$ by (a) and (b) of the theorem. Hence it is sufficient to prove the theorem for words x and y in Γ_μ (or Γ_k resp.) with $l(x) = i$, $l(y) = j$ and $j \geqq i$.

(a) PROPOSITION 1. *To every $x, y \in P_1$ with $l(x) \geqq i$, $[x, y] \in \Gamma_k$.*

PROOF. Induction on $l(x)$. Assume we have proved Proposition 1 for x with $l(x) > i$ and prove for x with $l(x) = i$. $x = s_i^\alpha \cdot u$, $u \in P_{i+1}$. Hence

$$(*) \qquad [x, y] = [s_i^\alpha u, y] = [s_i^\alpha, y][s_i^\alpha, y, u][u, y].$$

We prove $[s_i^\alpha, y] \in \Gamma_k$. By the collection formula

$$[s_i^\alpha, y] = [s_i, y]^\alpha c_2^{\binom{\alpha}{2}} \cdots c_\alpha, \qquad c_t \in K_t\langle [s_i, y], s_i \rangle.$$

Since $[s_i, y] \in P_{i+1}$, $l([s_i, y]) \geqq i + 1$ and by the induction hypothesis (a) of the theorem $c_t \in \Gamma_k$ for $2 \leqq t \leqq \alpha$. Hence by hypothesis (a)

$$c_2^{\binom{\alpha}{2}} \cdots c_\alpha \in \Gamma_k.$$

Let $y = s_j^{\beta_j} \cdots s_{m-1}^{\beta_{m-1}}$ and denote $y_t = s_{j+t}^{\beta_{j+t}} \cdots s_{m-1}^{\beta_{m-1}}$ for $t \geqq 0$. Then

$$(*)(*) \qquad [y, s_i] = [s_j^{\beta_j}, s_i]^{y_1}[s_{j+1}^{\beta_{j+1}}, s_i]^{y_2} \cdots [s_{m-1}^{\beta_{m-1}}, s_i].$$

Now, by the collection formula

$$[s_{j+t}^{\beta_{j+t}}, s_i] = [s_{j+t}, s_i]^{\beta_{j+t}} d_2^{\binom{\beta_{j+t}}{2}} \cdots d_{\beta_{j+t}} \qquad \text{where } d_\mu \in K_\mu(\langle [s_{j+t}, s_i], s_i \rangle).$$

Since P has p-degree of commutativity k, $[s_{j+t}, s_i]^{\beta_{j+t}} \in \Gamma_k$ by hypothesis (a) and since $[s_{j+t}, s_i] \in P_{i+1}$ it follows from hypothesis (a) and the induction hypothesis of Proposition 1 that

$$d_\mu^{\binom{\beta_{j+t}}{\mu}} \in \Gamma_k.$$

Hence by hypothesis (a) $[s_{j+t}^{\beta_{j+t}}, s_i] \in \Gamma_k \cap P_{i+1}$ and again the induction hypothesis $[s_{j+t}^{\beta_{j+t}}, s_i, y_{t+1}] \in \Gamma_k$. Therefore hypothesis (a) and $(*)(*)$ yield $[y, s_i] \in \Gamma_k$ and this implies $[s_i^\alpha, y] \in \Gamma_k \cap P_{i+1}$. But then $[[s_i^\alpha, y], u] \in \Gamma_k$. Hence $(*)$, hypothesis (a) and the induction hypothesis imply that $[x, y] \in \Gamma_k$. This proves Proposition 1.

Let $x = s_i^{\alpha_i} \cdots s_{i+t}^{\alpha_{i+t}} \cdots s_{m-1}^{\alpha_{m-1}}$, $y = s_j^{\beta_j} \cdots s_{j+t}^{\beta_{j+t}} \cdots s_{m-1}^{\beta_{m-1}}$, $l(x) = i$, $l(y) = j$ and assume that $x, y \in \Gamma_\mu$. To prove (a) first assume $y = s_j^b$, $p \mid b$. (If $p \nmid b$ nothing has to be proved.)

PROPOSITION 2. $x \cdot s_j^b \in \Gamma_\mu$.

PROOF. $x \cdot s_j^b = s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}} \cdot s_j^b = s_i^{\alpha_i} \cdots s_{m-j-1}^{\alpha_{m-j-1}} \cdot s_j^b \cdot s_{m-j}^{\alpha_{m-j}} \cdots s_{m-1}^{\alpha_{m-1}}$. We may assume that $m-1-j > j \geqq i$. Now, $s_{m-1-j}^{\alpha_{m-1-j}} \cdot s_j^b = s_j^b s_{m-1-j}^{\alpha_{m-1-j}} [s_{m-1-j}^{\alpha_{m-1-j}}, s_j^b]$. Since $i < m-1-j$ it follows from hypothesis (b) and Proposition 1 that $[s_{m-1-j}^{\alpha_{m-1-j}}, s_j^b] \in \Gamma_{2k+1}$ hence $s_{m-1-j}^{\alpha_{m-1-j}}[s_{m-1-j}^{\alpha_{m-1-j}}, s_j^b] \in \Gamma_\mu$, by hypothesis (a). This way, using the identity $\xi\eta = \eta\xi \cdot [\xi, \eta]$ $m-2j-1$ times we obtain

$$xs_j^b = s_i^{\alpha_i} \cdots s_j^{\alpha_j + b} s_{j+1}^{b_{j+1}} \cdots s_{m-1}^{b_{m-1}} \quad \text{and} \quad s_j^{\alpha_j+b} \cdots s_{m-1}^{b_{m-1}} \in \Gamma_\mu.$$

But then $x \cdot s_j^b \in \Gamma_\mu$, by definition. This proves Proposition 2.

Let $y = s_j^{\beta_j} \cdots s_{m-1}^{\beta_{m-1}}$, $j \geqq i$ and assume that $y \in \Gamma_\mu$. By Proposition 2

$$x \cdot y = (s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}})(s_j^{\beta_j} \cdots s_{m-1}^{\beta_{m-1}}) = s_i^{\alpha_i} \cdots s_{j-1}^{\alpha_{j-1}} s_j^{\alpha_j + \beta_j} (s_{j+1}^{\delta_{j+1}} \cdots s_{m-1}^{\delta_{m-1}})$$

and

$$s_i^{\alpha_i} \cdots s_{j-1}^{\alpha_{j-1}} s_j^{\alpha_j+\beta_j} (s_{j+1}^{\delta_{j+1}} \cdots s_{m-1}^{\delta_{m-1}}) \in \Gamma_\mu.$$

If we repeat this process $m-1-j$ times we obtain that $x \cdot y \in \Gamma_\mu$. This proves (a).

(b) Let $x = s_i^\alpha g$, $g \in P_{i+1} \cap \Gamma_k$, $p \mid \alpha$, and assume that $x \in \Gamma_\mu$, $u \in \operatorname{Aut}(P_1)$ and u satisfies the conditions of (b).

$$(*) \qquad [x, u] = [s_i^\alpha g, u] = [s_i^\alpha, u][s_i, u, g][g, u].$$

Since P has p-degree of commutativity k and u satisfies the conditions of (b), $[s_i, u] \in \Gamma_k \cap P_{i+1}$. Hence by the induction hypothesis, to every $w \in \operatorname{Aut}(P_1)$ that satisfies the conditions of (b), $[s_i, u, w] \in \Gamma_{2k+1}$. In particular $c_t \in \Gamma_{2k+1}$ and

$$c_2^{\binom{\alpha}{2}} \cdots c_\alpha \in \Gamma_{2k+1}.$$

It remains to show that $[s_i, u]^\alpha \in \Gamma_{2k+1}$. $[s_i, u] \in \Gamma_k \cap P_{i+1}$. Hence by hypothesis (c) $[s_i, u]^\alpha \in \Gamma_{2k+1}$ $(p \mid \alpha)$ and by (a) and $(*)(*)$ $[s_i^\alpha, u] \in \Gamma_{2k+1}$. Now, $g \in \Gamma_k \cap P_{i+1}$ and since $[s_i, s_j] \in P_{i+1} \cap \Gamma_k$ to every s_t and s_j, $[g, s_j] \in P_{j+1} \cap \Gamma_k$ to every s_j, by hypothesis (b). But then, $[s_i^\alpha, u, g] \in \Gamma_{2k+1}$, the induction hypothesis (b). Also, by the induction hypothesis $[u, g] \in \Gamma_{2k+1}$, hence $[x, u] \in \Gamma_{2k+1}$ by $(*)$ and (a). This proves (b).

(c) Let $x = s_i^\alpha g$, $g \in P_{i+1}$ and assume that $x \in \Gamma_k$. Then, by the collection formula

$$x^p = (s_i g)^p = s_i^{\alpha p} g^p c_2^{\binom{\alpha}{2}} \cdots c_p, \qquad \text{where } c_t \in K_t(\langle s_i^\alpha, g\rangle).$$

Since $s_i^\alpha \in \Gamma_k$ and $g \in \Gamma_k \cap P_{i+1}$, (b) implies that $c_t \in \Gamma_{2k+1}$ for $2 \leqq t \leqq p$. Hence $c_2^{\binom{p}{2}} \cdots c_p \in \Gamma_{2k+1}$, by (a). Now by the induction hypothesis (c) $u^p \in \Gamma_{2k+1}$ and, of course, $s_i^{\alpha p} \in \Gamma_{2k+1}$ since $2k+1 < p^n$. Therefore by (a) $x^p \in \Gamma_{2k+1}$. As every element of $\mho(\Gamma_k)$ is a product $x_1^p \cdot x_2^p \cdots x_r^p$, $x_j \in \Gamma_k$, $\mho(\Gamma_k) \leqq \Gamma_{2k+1}$, as required.

Corollary 1. *Under the conditions of Theorem* 1, $[\mho(P_1), P_1] \leqq \Gamma_{2k+1}$.

Proof. By Theorem 1(a) it is enough to prove that to every $x, y \in P_1$, $[x^p, y] \in \Gamma_{2k+1}$.

$$(*) \qquad [x^p, y] = [xy]^p c_2^{\binom{p}{2}} \cdots c_p, \langle c_i \in K_i(\langle [x,y], y \rangle)\rangle.$$

By Proposition 1 $[x,y] \in \Gamma_k$, hence by Theorem 1 (a), (b)

$$c_i^{\binom{p}{i}} \in \Gamma_{2k+1}.$$

Hence, by Theorem 1 (a)

$$c_2^{\binom{p}{2}} \cdots c_p \in \Gamma_{2k+1}.$$

Since $[x,y]^p \in \Gamma_{2k+1}$, by Theorem 1(c), (*) and Theorem 1(a) imply $[x^p, y] \in \Gamma_{2k+1}$.

Proposition 3. *Let P be a p-group of type (m,n) and assume that P has p-degree of commutativity $k < (p^n - 1)/2$. Let*

$$[s_{i_1}, s_{j_1}] \equiv s_{i_1+j_1}^{a_0} s_{i_1+j_1+1}^{a_1} \cdots s_{i_1+j_1+k}^{\alpha(i_1,j_1)} \bmod P_{i_1+j_1+k+1},$$

$$[s_{i_2}, s_{j_2}] \equiv s_{i_2+j_2}^{b_0} s_{i_2+j_2+1}^{b_1} \cdots s_{i_2+j_2+k}^{\alpha(i_2,j_2)} \bmod P_{i_2+j_2+k+1}.$$

(a) *If $i_1 + j_1 = i_2 + j_2$ then*

$$[s_{i_1}, s_{j_1}] \cdot [s_{i_2}, s_{j_2}] \equiv s_{i_1+j_1}^{c_0} \cdots s_{i_1+j_1+k}^{\alpha(i_1,j_1)+\alpha(i_2,j_2)+pr} \bmod P_{i_1+j_1+k+1}.$$

(b) *If $i_1 + j_2 < i_2 + j_2$ then*

$$[s_{i_1}, s_{j_1}] \cdot [s_{i_2}, s_{j_2}] \equiv s_{i_1+j_1}^{c_0} \cdots s_{i_1+j_1+k}^{\alpha(i_1,j_1)+pr} \bmod P_{i_1+j_1+k+1}.$$

Proof. (a) $[s_{i_1}, s_{i_1}][s_{i_2}, s_{j_2}] \equiv (s_{i_1+j_1}^{a_0} \cdots s_{i_1+j_1+k}^{\alpha(i_1,j_1)})(s_{i_2+j_2}^{b_0} \cdots s_{i_2+j_2+k}^{\alpha(i_2,j_2)}) \bmod P_{i_1+j_1+k+1}$.

In the collecting process we use the formula $\xi\eta = \eta\xi[\xi,\eta]$. Hence it will suffice to show that

$$[s_{i_1+j_1+\nu}^{a_\nu}, s_{i_2+j_2+\mu}^{b_\mu}] \in \Gamma_{2k+1}(P_{i_1+j_1}) \quad \text{and} \quad [s_{i_1+j_1+\nu}^{a_\nu}, a_{i_2+j_2+k}^{\alpha(i,j)}] \in \Gamma_{2k+1}(P_{i_1+j_1}).$$

Since $p \mid a_\nu$, $p \mid b_\mu$ the first membership follows from Theorem 1(b) and the second from Corollary 1. This proves (a). (b) is proved similarly.

Theorem 2. *Let P be a p-group of type (m,n) and assume that P has* *p-degree of commutativity* $k < (p^n - 1)/2$. *Let* $[s_i, s_j] \equiv s_{i+j}^{a_0} \cdots s_{i+j+k}^{\alpha(i,j)} \bmod P_{i+j+1}$. *Then*

(a) $\alpha(i,j)\alpha(i+j+k,l) + \alpha(j,l)\alpha(j+l+k,i) + \alpha(l,i)\alpha(1+i+k,j) \equiv o(p)$ *for every* i, j, l *with* $i+j+l+2k < m$.

(b) $\alpha(i,j) + \alpha(j,i) \equiv 0 \bmod p$, *for every* i *and* j *with* $i+j+k < m$.

(c) *If* $k \leqq p-1$ *then* $\alpha(i,j) \equiv \alpha(i+1,j) + \alpha(i,j+1) \bmod p$ *for every* i, j *with* $i+j+1+k < m$.

(d) *If* $k \leqq p-2$, *then* $\alpha(i+p-1,j) \equiv \alpha(i,j+p-1) \equiv \alpha(i,j) \bmod p$, *for every* i *and* j *which satisfy* $i+j+p-1+k < m$.

PROOF. (a) $[s_i, s_j, s_l] = [s_{i+j}^{a_0} \cdots s_{i+j+k}^{\alpha(i,j)} u, s_l] = [s_{i+j}^{a_0}, s_l]^{\sigma_0} \cdots [s_{i+j+k}^{\alpha(i,j)}, s_l]^{\sigma_k} \cdot [u, s_l]$ where $u \in P_{i+j+k+1}$, $\sigma_t = s_{i+j+t+1}^{a_{t+1}} \cdots s_{i+j+k}^{\alpha(i,j)} \cdot u$ and $p \mid a_i$ for $0 \leqq i \leqq k-1$. Let us compute $[s_{i+j+t}^{a_t}, s_l]$. By the collection formula

$$[s_{i+j+t}^{a_t}, s_l] = [s_{i+j+t}, s_l]^{a_t} \cdot d_2^{\binom{a_t}{2}} \cdots d_{a_t} \quad \text{where } d_i \in K_i(\langle [s_{i+j+t}, s_l], s_l \rangle := K_i.$$

Now, by definition, $[s_{i+j+t}, s_l] \in \Gamma_k(P_{i+j+t+l})$. Hence $[s_{i+j+t}, s_l]^{\alpha_t} \in \mho(\Gamma_k(P_{i+j+t+l})) \leqq \Gamma_{2k+1}(P_{i+j+t+l})$, by Theorem 1(c). Since $d_i \in K_i$, Theorem 1(b) implies $d_i \in [\Gamma_k(P_{i+j+t+l}), P_l] \leqq \Gamma_{k+1}(P_{i+j+t+l})$ and Theorem 1(a) together with the collection formula implies $[s_{i+j+t}^{a_t}, s_l] \in \Gamma_{2k+1}(P_{i+j+t+l})$. Obviously, $[[s_{i+j+t}^{a_t}, s_l], \sigma_t] \in \Gamma_{2k+1}(P_{i+j+t+l})$. Hence by Theorem 1(a)

(*) $[s_i, s_j, s_l] \equiv s_{i+j+l}^{l_0} \cdots s_{i+j+l+2k}^{l_{2k}} [s_{i+j+k}^{\alpha(i,j)}, s_l] \bmod P_{i+j+l+2k+1}, p \mid l_t$ for $0 \leqq t \leqq 2k$.

Next, we compute $[s_{i+j+k}^{\alpha(i,j)}, s_l]$. Denote $\alpha = \alpha(i,j)$. Then, by the collection formula

$$[s_{i+j+k}^{\alpha}, s_l] = [s_{i+j+k}, s_l]^{\alpha} d_2^{\binom{\alpha}{2}} \cdots d_\alpha,$$

$$\text{where } d_\nu \in K_\nu := K_\nu(\langle [s_{i+j+k}, s_l], s_l \rangle) \quad \text{for } 2 \leqq \nu \leqq \alpha.$$

By Theorem 1(a) and (b)

$$d_2^{\binom{\alpha}{2}} \cdots d_\alpha \in \Gamma_{2k+1}(P_{i+j+k+l}).$$

Now, $[s_{i+j+k}, s_l]^\alpha = (s_{i+j+k+l}^{c_0} \cdots s_{i+j+l+2k}^{\alpha(i+j+k,l)} \cdot u)^\alpha$, where $u \in P_{i+j+l+2k+1}$ and $p \mid c_t$ for $0 \leqq t \leqq k-1$. There exists a $u' \in P_{i+j+l+2k+1}$ s.t.

$$[s_{i+j+k}, s_l] = (s_{i+j+k+l}^{c_0} \cdots s_{i+j+k+l+k+1}^{c_{k-1}} \cdot u') s_{i+j+l+2k}^{\alpha(i+j+k,l)}.$$

Denote $v = s_{i+j+k+l}^{c_0} \cdots s_{i+j+k+l+k-1}^{c_{k-1}} \cdot u'$. Then by the collection formula

$$[s_{i+j+k}, s_l]^\alpha = (v \cdot s_{i+j+l+2k}^{\alpha(i+j+k,l)})^\alpha = v^\alpha \cdot s_{i+j+l+2k}^{\alpha(i+j+k,l)\cdot\alpha} \cdot c_2^{\binom{\alpha}{2}} \cdots c_\alpha,$$

where $c_t \in K_t := K_t(\langle v, s_{i+j+l+2k}^{\alpha(i+j+k,j)} \rangle)$.

Since $v \in \Gamma_{k+1}(P_{i+j+l+k})$, $c_t \in [\Gamma_{k+1}(P_{i+j+l+k}), P_{i+j+k+l}] \leqq \Gamma_{2k+1}(P_{i+j+l+k})$, by Theorem 1(b). As $v^\alpha \in \Gamma_{k+1}(P_{i+j+l+k})$, by Theorem 1(a), it follows from the collection formula and Theorem 1(a) that

$$[s_{i+j+k}^{\alpha(i,j)}, s_l] \equiv s_{i+j+k+l}^{b_0} \cdots s_{i+j+2k-1+l}^{b_{k-1}} s_{i+j+2k+l}^{\alpha(i,j)\alpha(i+j+k,l)+pr} \bmod P_{i+j+2k+l+1}$$

and by (*)

$$(*)(*) \qquad [s_i, s_j, s_l] \equiv s_{i+j+l}^{a_0} \cdots s_{i+j+2k-1+l}^{a_{2k-1}} \cdot s_{i+j+2k+l}^{\alpha(i,j)\alpha(i+j+k,l)+pr} \bmod P_{i+j+2k+l+1}$$

where $p \mid a_t$ for $0 \leqq t \leqq 2k-1$. We shall use the identity of Witt:

$$\begin{aligned}[s_i, s_j^{-1}, s_l]^{s_j} &= [[s_i, s_j]^{-s_j^{-1}}, s_l]^{s_j} \\ &= [s_j, s_i, s_l[s_l, s_j]] \\ &= [[s_j, s_i], [s_l, s_j]][s_j, s_i, s_l]^{[s_l, s_j]} \\ &= [s_j, s_i, s_l][[s_j, s_i], [s_l, s_j]] \\ &\quad \cdot [[[s_j, s_i], [s_l, s_j]], [s_j, s_i, s_l]] \cdot [[s_j, s_i, s_l], [s_l, s_j]].\end{aligned}$$

Now, using the collection formula and Theorem 1 as several times above we get

$$[[s_j, s_i], [s_l, s_j]] \in \Gamma_{2k+1}(P_{i+j+l}) \quad \text{and} \quad [[s_j, s_i, s_l], [s_l, s_j]] \in \Gamma_{2k+1}(P_{i+j+l}).$$

Hence $[s_i, s_j^{-1}, s_l]^{s_j} \equiv [s_i, s_j, s_l] \bmod \Gamma_{2k+1}(P_{i+j+l})$ and (*)(*), with Theorem 1, yields

$$[s_i, s_j^{-1}, s_l]^{s_j} \equiv s_{i+j+l}^{a_0} \cdot s_{i+j+l+1}^{a_1} \cdots s_{i+j+l+2k-1}^{a_{2k-1}} \cdot s_{i+j+l+2k}^{-\alpha(i,j)\alpha(i+j+k,l)+p\cdot r} \bmod P_{i+j+l+2k+1},$$

where $p \mid a_t$ for $0 \leqq t \leqq 2k-1$. Therefore (a) follows from the identity of Witt.

(b) Follows from the identity $[s_i, s_j][s_j, s_i] = 1$.

(c) Claim. *If* $x \in \Gamma_k(P_i)$ *then* $[x, s] \in \Gamma_{k+1}(P_i)$.

Proof. Induction on $l(x)$. Let $x = s_i^\alpha u$, $u \in P_{i+1}$ and assume that $x \in \Gamma_k(P_i)$. Then $u \in \Gamma_k(P_i) \cap P_{i+1}$ and $p \mid \alpha$.

$$(*) \qquad [x, s] = [s_i^\alpha, s][s_i^\alpha, s, u][u, s].$$

Now,

$$[s_i^\alpha, s] = s_{i+1}^\alpha c_2^{\binom{\alpha}{2}} \cdots c_\alpha, \qquad c_j \in K_j(\langle s_{i+1}, s\rangle) = P_{i+j}.$$

Since $p \mid \alpha$, $s_{i+1}^\alpha \in \Gamma_{k+1}(P_i)$. By Theorem 1

$$c_2^{\binom{\alpha}{2}} \cdots c_{p-1}^{\binom{\alpha}{p-1}} \in \Gamma_k(P_{i+1}) \leqq \Gamma_{k+1}(P_i) \quad \text{hence} \quad s_{i+1}^\alpha c_2^{\binom{\alpha}{2}} \cdots c_{p-1}^{\binom{\alpha}{p-1}} \in \Gamma_{k+1}(P_i).$$

As $c_p \in P_{i+p}$ and $k \leqq p-1$, $[s_i^{\alpha}, s] \in \Gamma_{k+1}(P_i)$, by Theorem 1. This proves our claim.

$$[s_{i+1}, s_j] = s_{i+1}^{-1} s_{i+1}^{s_j} = s_{i+1}^{-1}[s_i[s_i, s_j], ss_{j+1}^{-1}]$$
$$= s_{i+1}^{-1}([s_i, s_{j+1}^{-1}]s_{i+1}[s_{i+1}, s_{j+1}^{-1}])^{[s_i, s_j]} \cdot [s_i, s_j, s_{j+1}^{-1}][s_i, s_j, s]^{s_{j+1}^{-1}}.$$

Denote $v = [s_i, s_{j+1}^{-1}]s_{i+1}[s_{i+1}, s_{j+1}^{-1}]$. Then $v \in P_{i+1}$. Since $[s_i, s_j] \in \Gamma_k(P_{i+j})$, $[v, [s_i, s_j]] \in \Gamma_{2k+1}(P_{i+j})$ and $[s_i, s_j, s_{j+1}^{-1}] \in \Gamma_{2k+1}(P_{i+j})$, $[s_i, s_{j+1}^{-1}, s_{i+1}] \in \Gamma_{2k+1}(P_{i+1})$ by Theorem 1(b). Hence

$$[s_{i+1}, s_j] \equiv [s_i, s_{j+1}^{-1}][s_{i+1}, s_{j+1}^{-1}][s_i, s_j, s] \bmod \Gamma_{2k+1}(P_{i+j}).$$

$\Gamma_{2k+1}(P_{i+j}) \leqq \Gamma_k(P_{i+j+2})$ and $[s_{i+1}, s_{j+1}^{-1}] \in \Gamma_k(P_{i+j+2})$. Hence

$$[s_{i+1}, s_j] \equiv [s_i, s_{j+1}^{-1}][s_i, s_j, s] \bmod \Gamma_k(P_{i+j+2})$$

and $\alpha(i+1, j) \equiv -\alpha(i, j+1) + \alpha(i, j) + kp \bmod p^n$, by our last Claim, Proposition 3 and Theorem 1(a). Therefore $\alpha(i, j) \equiv \alpha(i, j+1) + \alpha(i+1, j) \bmod p$, as required.

(d) For $j \geqq 1$,

$$s_j^{p^n} s_{j+p-1}^{\binom{p^n}{p}} \cdots s_{j+t}^{a_t} \cdots s_{j+p^n-1}^{a_{p^n-1}} \cdot u = 1,$$

where $u \in P_{j+p^n} \cdot Z(P)$ and $p^{n-\alpha} \mid a_t$ for $p_{\alpha+1} \leqq t \leqq p^{\alpha+1}$ and $p^{n-\alpha} \mid a_t$ for $t = p^{\alpha-1}$, by Theorem 2.4. Hence, to every $i \geqq 1$,

$$[s_i, s_j^{p^n} s_{j+p-1}^{\binom{p^n}{p}} \cdots s_{j-p^n-1}^{a_t} \cdot u] = 1.$$

Let $v \in P_{j+2(p-1)+1}$. Then

$$[s_i, s_j^{p^n} \cdot s_{j+p-1}^{\binom{p^n}{p}} \cdots s_{j+2(p-1)}^{a_{2(p-1)}} \cdot v] = [s_i, s_j^{p^n}]^{\sigma_{p-1}} \cdot [s_i, s_{j+p-1}^{a_{p-1}}]^{\sigma_p} \cdots [s_i, s_{j+2(p-1)}]^{\sigma_{2p-1}} \cdot [s_i, v]$$

where $\sigma_t = s_{j+2(p-1)}^{a_t} \cdot v$. We show that for $t \geqq 1$, $[s_i, s_{j+p-1+t}^{a_{p-1+t}}]^{\sigma_{p+t}} \in P_{i+j+p+k}$. For this it is enough to show $[s_i, s_{j+p-1+t}^{s_{p-1+t}}] \in P_{i+j+p+k}$. We may assume that $t = 1$ since the calculations are the same for $t \geqq 1$. It follows from the collection formula that

(I) $[s_i, s_{j+p}^{a_p}] = [s_i, s_{j+p}]^{a_p} c_2^{\binom{a_p}{2}} \cdots c_{a_p}$, where $p^{n-1} \mid a_p$, $c_t \in K_t := K_t(\langle s_i, [s_i, s_{j+p}]\rangle)$.

Since P has p-degree of commutativity k, $[s_i, s_{j+p}] = s_{i+j+p}^{\rho_0} \cdots s_{i+j+p+k}^{\alpha(i,j+p)} \cdot v_1$ where $v_1 \in P_{i+j+p+k+1}$ and $p \mid c_t$ for $0 \leqq t \leqq k-1$. Hence, by the collection formula

(II) $[s_i, s_{j+p}]^{a_p} = s_{i+j+p}^{a_p \cdot \rho_0} \cdots s_{i+j+p+k}^{\alpha(i,j+p)a_p} v_1^{a_p} \cdot d_2^{\binom{a_p}{2}} \cdots d_{a_p}$, $d_\mu \in K_\mu(P_{i+j+p})$.

Since $p^n \mid \rho_t \cdot a_p$ for $0 \leqq t \leqq k-1$, as $p \mid \rho_t$ and $p^{n-1} \mid a_p$, it follows from Theorem 2.4 that $s_{i+j+p+t}^{\rho_t a_p} \in P_{i+j+2p-1} \leqq P_{i+j+p+k}$, as $k < p-1$. Obviously

$s_{i+j+p+k}^{\alpha(i,j+p)a_p} \cdot v_1 \in P_{i+j+p+k}$. Hence $d_\mu \in K_\mu(P_{i+j+p})$ implies that for $\mu \geqq 2$, $d_\mu \in P_{i+j+p+k}$. Therefore

(III) $$[s_i, s_{j+p}]^{a_p} \in P_{i+j+p+k}.$$

By similar calculations it is easy to show that for $2 \leqq t \leqq p-1$

$$c_t^{\binom{a_p}{t}} \in P_{i+j+p+k}.$$

But for $t \geqq p$ obviously $c_t \in P_{i+j+p+k}$. Hence (I), (II) and (III) imply that $[s_i, s_{j+p}^{a_p}] \in P_{i+j+p+k}$. This means:

(IV) $$[s_i, s_j^{p^n} s_{j+p-1}^{\binom{p^n}{p}} \cdots] \equiv [s_i, s_j^{p_n}]^{\sigma_{p-1}} \cdot [s_i, s_{j+p-1}^{a_{p-1}}]^{\sigma_p} \bmod P_{i+j+p+k}.$$

Now,

$$[s_i, s_j^{p^n}] = [s_i, s_j]^{p^n} \cdot c_2^{\binom{p^n}{2}} \cdots c_p^{\binom{p^n}{p}} \cdots c_{p^n},$$

by the collection formula, where $c_t \in K_t := K_t(\langle [s_i, [s_i, s_j]] \rangle) \leqq P_{i+j+i(t-1)} = P_{j+ti}$. Again, by the collection formula

$$\begin{aligned}[s_i, s_j]^{p^n} &= (s_{i+j}^{l_0} \cdot s_{i+j+1}^{l_1} \cdots s_{i+j+k-1}^{l_{k-1}} \cdot s_{i+j+k}^{\alpha(i,j)} u)^{p^n} \\ &= s_{i+j+2(p-1)}^{\bar{l}_0} \cdots s_{i+j+2(p-1)+t}^{\bar{l}_t} \cdots s_{i+j+k+p-1}^{\alpha(i,j)b} \cdot v\end{aligned}$$

where $p^{n-1} \mid \bar{l}_t$, $p \mid l_t$, $u \in P_{i+j+k+1}$, $v \in P_{i+j+k+p}$ and

$$b \equiv -\binom{p^n}{p} \equiv -p^{n-1} \bmod p^n.$$

Since by assumption $k < p-1$, $[s_i, s_j]^{p^n} \equiv s_{i+j+k+p-1}^{\alpha(i,j)b} \bmod P_{t+j+k+p}$. Also, as $c_t \in P_{i+j}$ a similar calculation shows that

$$c_2^{\binom{p}{2}} \cdots c_{p-1}^{\binom{p^n}{p-1}} \in P_{i+j+k+p}.$$

Since $c_p = s_\mu^{e_0} \cdots s_{\mu+2k}^{e_{2k}} s_{\mu+2k+1}^{\alpha} \cdot u_1$ for a certain $\mu \geqq j + ip$ and $u_1 \in P_{\mu+2k+2}$ where $p \mid e_t$ for $0 < t \leqq 2k$ (by Theorem 1(b)), $c_p^{p^{n-1}} \in P_{(i+j)+p-1+\nu}$ where $\nu = \min\{2k+1, p-1\}$. But $i+j+(p-1)+\nu \geqq i+j+p+k$ $(k < p-1)$. Hence $c_p^{p^{n-1}} \in P_{i+j+p+k}$ and

(V) $$[s_i, s_j^{p^n}]^{\sigma_{p-1}} \equiv s_{i+j+k+p-1}^{\alpha(i,j)b} \bmod P_{i+j+p+k}, \qquad \text{where } b \equiv p^{n-1} \bmod p^n.$$

By a similar argument

(VI) $$[s_i, s_{j+p-1}^{\binom{p^n}{p}}]^{\sigma_p} \equiv s_{i+j+k+p-1}^{\alpha(i,j+p-1)\cdot b_1} \bmod P_{i+j+p+k}, \quad \text{where } b_1 \equiv \binom{p^n}{p} \equiv p^{n-1} \bmod p^n.$$

Therefore (IV), (V) and (VI) imply that $(\alpha(i,j+p-1) - \alpha(i,j))p^{n-1} \equiv o(p^n)$, i.e., $\alpha(i,j+p-1) \equiv \alpha(i,j) \bmod p$. This proves Theorem 2.

The following theorem is the main result of this section:

THEOREM 3. *Let P be a p-group of type (m,n). Assume that P has p-degree of commutativity k. If $m > 3p-6+2k$ then $k \geqq p-1$.*

PROOF. Assume $k \leqq p-2$. Then the $\alpha(i,j)$'s defined in Theorem 2 satisfy the conditions of Shepherd's Theorem [12] (see also [7]). Hence $m < 3p-6+2k$, contradicting $m > 3p-6+2k$.

COROLLARY. *If $m \geqq 5p-10$ then $k \geqq p-1$.*

By the aid of Theorem 3 we may find the exponent of P_i for $m \geqq 5p-10$.

THEOREM 4. *Let P be a p-group of type (m,n) and assume that P has p-degree of commutativity $k \geqq p-1$. Let $m-1 = q(p-1)+r$, $1 \leqq r \leqq p-1$, $\exp(P_1) = p^e$ and let $x \equiv s_1^{\alpha_1} \cdot s_2^{\alpha_2} \cdots s_r^{\alpha_r} \bmod P_{r+1}$ be an element of P_1, where $0 \leqq \alpha_i < p^n$ for $1 \leqq i \leqq r$.*

(a) *If $p \mid \alpha_i$ for $1 \leqq i \leqq r$ then $x^{p^{e-1}} = 1$.*

(b) *If $p \nmid \alpha_i$ for at least one i, $1 \leqq i \leqq r$ and i_0 is the first such i, then $x^{p^{e-1}} = s_{m-r+i_0}^{a_0} \cdots s_{m-1}^{a_{r-i-1}}$, where $p^{n-1} \mid a_j$ for $0 < j \leqq r-i-1$.*

(c) *For $i \geqq 1$, $\exp(P_i) = |s_i|$.*

(d) *$\Omega_{e-1}(P_1) \geqq P_p \cdot \mho(P_1)$, $p \leqq |P_1/\Omega_{e-1}(P_1)| \leqq p^{p-1}$ and $P/\Omega_{e-1}(P)$ is regular.*

PROOF. Let us prove (a), (b) and (c) by induction on $\mathrm{cl}(P)$. If $\mathrm{cl}(P) = 2$ everything is trivial. Assume (a), (b) and (c) hold for P with $\mathrm{cl}(P) = j$ and prove (a), (b), and (c) for P with $\mathrm{cl}(P) = j+1$. By Lemma 0.1 we may assume that (a), (b) and (c) hold for $H_i = \langle P_i, s\rangle$, $i \geqq 2$ and prove them for P. Denote $x = s_1^{\alpha} u$ where $u \equiv s_2^{\alpha_2} \cdots s_r^{\alpha_r} \bmod P_{r+1}$.

CLAIM. $x^{p^{e-1}} = s_1^{\alpha p^{e-1}} \cdot u^{p^{e-1}}$

PROOF. $(s_1^{\alpha} u)^{p^{e-1}} = s_1^{\alpha \cdot p^{e-1}} c_2^{\binom{p^{e-1}}{2}} \cdots c_i^{\binom{p^{e-1}}{i}} \cdots c_{p^{e-1}}$, by the collection formula, where $c_i \in K_i(\langle s_1^{\alpha}, u\rangle) \leqq P_{i+2}$. Hence, if $|s_{i+2}| = p^{e_i}$ then $c_i^{p^{e_i}} = 1$ by hypothesis (c). If $r+(k-1)(p-1) \leqq i+2 < r+k(p-1)$ then $|s_{i+2}| = p^{e-k}$ by Theorem 2.6.

Hence, $\exp(P_{i+2}) = p^{e-k}$ by hypothesis (c) and $c_i^{p^{e-k}} = 1$. Denote

$$\nu_p\left(\binom{p^{e-1}}{i}\right) = \mu_i - 1.$$

If $p^{\alpha} \leqq i < p^{\alpha+1}$ then $\mu_i - 1 \geqq e-1-\alpha$. Now, for $\alpha \geqq 2$

$$k > \frac{i+2-r}{p-1} \geqq \frac{p^{\alpha}+3-p}{p-1} \geqq \frac{p^{\alpha}-1}{p-1} - 1 \geqq \alpha$$

hence $\mu_i - 1 \geqq e - 1 - \alpha \geqq e - k$. Therefore

$$c_i^{\binom{p^{e-1}}{i}} = 1 \quad \text{for } p^2 \leqq i.$$

Assume $\alpha \leqq 1$. Since P has p-degree of commutativity $k \geqq p-1$, $c_i \equiv s_{i+2}^{a_0^i} \cdots a_{i+p}^{a_{p-2}^i} \bmod P_{i+p+1}$, where $p \mid a_j^i$ for $0 \leqq j \leqq p-2$. As for $i \geqq 2$, $c_i \in P_4$,

$$c_i^{\binom{p^{e-1}}{i}} = 1, \quad \text{for } 2 \leqq i \leqq p-1$$

by the induction hypothesis (c). Hence assume $\alpha = 1$. For $p \leqq i$, $c_i \in P_{p+2}$, hence by hypothesis (c) and Theorem 2.6, $c_i^{p^{e-2}} = 1$ for $p \leqq i < p^2$. This proves our Claim.

(a) By hypothesis (c) $u^{p^{e-1}} = 1$ and by Theorem 2.6, $s_1^{\alpha \cdot p^{e-1}} = 1$. Hence (a) follows from our last Claim.

(b) If $i_0 \geqq 2$ then $u^{p^{e-1}} = s_{m-r+i_0-1}^{a_0} \cdots a_{m-1}^{a_{r-i_0}}$ by the induction hypothesis. Since $p \mid \alpha$, $s_1^{\alpha p^{e-1}} = 1$ and (b) follows from the last Claim. If $i_0 = 1$ then

$$x^{p^{e-1}} = (s_1)^{\alpha_{p^{e-1}}} u^{p^{e-1}} = (s_{m-r}^{a_0} \cdots s_{m-1}^{a_{r-1}})(s_{m-r+1}^{b_0} \cdots s_{m-1}^{b_{r-2}})$$

by Theorem 2.5 and the hypothesis, where $p^{r-1} \mid a_j, b_l$ for $0 \leqq j \leqq r-1$, $0 \leqq l \leqq r-2$. Since P_{m-r} is regular for $r \leqq p-1$, by Theorem 2.7 $x^{p^{e-1}} = s_{m-r}^{c_0} \cdots s_{m-1}^{c_{r-1}}$ where $p^{n-1} \mid c_j$ for $0 \leqq j \leqq r-1$.

(c) For $i \geqq 2$ (c) is just the induction hypothesis. For $i = 1$ (c) follows from (a) and (b).

(d) By (c), $\exp P_p = |s_p|$. Hence, by Theorem 2.6, $G_p \leqq \Omega_{e-1}(P_1)$. This implies that $P_1/\Omega_{e-1}(P_1) = \bar{P}_1$ is generated at most by the $p-1$ elements $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_{p-1}$. On the other hand $\Omega(P_1) \leqq \Omega_{e-1}(P_1)$, hence $P_p \cdot (P_1) \leqq \Omega_{e-1}(P_1)$ and every element $x \equiv s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_{p-1}^{\alpha_{p-1}} \bmod P_p$ s.t. $p \mid \alpha_t$ for $1 \leqq t \leqq p-1$ belongs to $\Omega_{e-1}(P_1)$. Therefore $p \leqq |P_1/\Omega_{e-1}(P_1)| \leqq p^{p-1}$. Finally $\bar{P} = P/\Omega_{e-1}(P_1) = \langle \bar{s} \rangle \cdot \bar{P}_1$. Since $[\bar{s}^p, \bar{P}_1] \leqq P_p \cdot \Omega(P_1)$ and $(\bar{s}^p) \leqq Z(P/\Omega_{e-1}(P_1))$, $\bar{P}$ has class $\leqq p-1$. Hence $\bar{P}$ is regular.

COROLLARY. *Let P be a p-group of type (m, n) and assume that $m \geqq 5p - 10$. Then* (a), (b), (c) *and* (d) *hold for P.*

PROOF. Follows from the corollary to Theorem 2.

PART B

4. p-local subgroups of finite groups with a Sylow p-subgroup of type (m, n)

For $n = 1$ the results appear in [10]. Hence we deal here only with the cases $n \geqq 2$. The main result is:

THEOREM 1. *Let G be a finite group with a Sylow p-subgroup P of type (m, n), $n \geqq 2$, $p \geqq 3$, $m \geqq (n+5)(p-1)+1$. For $H \leqq G$ denote $\bar{H} = HO_{p'}(G)/O_{p'}(G)$. If $O_p(G)$ is not cyclic and $P_1' \neq 1$ then $\bar{P} \triangle \bar{G}$ and $\bar{G} = \bar{P} \cdot \bar{T}$ is a semidirect product of $\bar{P}$ and $\bar{T}$, where $\bar{T}$ is cyclic of order τ, $\tau \mid p-1$.*

Briefly, the proof is this. Let G be a minimal counterexample. Then $O_{p'}(G) = 1$ and $C_G(O_p(G)) = C_P(O_p(G)) \leqq O_p(G)$. Also $N_G(P)/O^p(N_G(P)) \cong G/O^p(G)$. Hence if we find a normal subgroup N of G in $O_p(G)$ s.t. $|O_p(G)/N| = p$ then either $O_p(G)/N$ is noncentral in G/N, in which case G is not a minimal counterexample, or $O_p(G)/N$ is central in G/N. Since $N_G(P)/O^p(N_G(P)) \cong G/O^p(G)$ in this case G has a normal p-complement, again a contradiction to the minimality of G. In Propositions 1–3 we locate $O_p(G)$ in P and construct a normal subgroup $N_0 \triangle G$ in $O_p(G)$ s.t. $O_p(G)/N_0$ is elementary abelian of order $\leqq p^{p+1}$. Proposition 4 shows that $C_G(O_p(G)) = C_P(O_p(G))$ and in Proposition 5 we construct $N \triangle G$ with $|O_p(G)/N| = p$.

PROPOSITION 1. *Let H be an elementary abelian normal subgroup of P and assume that $\exp(P_1) = e \geqq 2n+1$. Then:*

(a) *If $H \leqq P_{n-i}$ then $|H| \leqq p^i$.*

(b) *$|H| \leqq p^{p^n}$ and if $H \leqq P_1$ then $|H| \leqq p^{p^{n-1}}$.*

(c) *If $H \leqq \mho_{e-i}(P)$ and $\varepsilon = e - i \geqq n$ then $|H| \leqq p^{i(p-1)}$.*

(d) *If $|H| = p^d$, $d \leqq p^\alpha$ then $\mho_\alpha(P) \leqq C_P(H)$ and $P_{p^\alpha} \leqq C_P(H)$.*

PROOF. (a) Since P_{i-1}/P_i is cyclic, $|H \cap P_{j-1}/H \cap P_j| = |(H \cap P_{j-1})P_j/P_j| \leqq p \Rightarrow |H| \leqq p^i$.

(b) Assume $H \leqq P_1$. Then by Proposition 0.2(b) we may assume that $H \not\leqq P_2$.

If $x \in P_1$ then we may write it uniquely by $x = \prod_{i=1}^{n-1} s_i^{\alpha_i}$, $0 \leqq \alpha_i < p^n$. If $\alpha = q \cdot p^t$, $(q, p) = 1$, denote $\nu_p(\alpha) = t$. Assume that $X = \{x_1, \cdots, x_d\}$ is a set of generators of H and $x_i = \prod_{j=1}^{m-1} s_j^{\alpha_j^{(i)}}$. If $x_1, \cdots, x_r$, $r \leqq d$, are all the generators of H in X s.t. $\alpha_1^{(i)} \neq 0$ and $\alpha_1^{(1)} = \min_i \nu_p(\alpha_1^{(i)})$, then there exist numbers $a_2, \cdots, a_r$ s.t. $\{x_1, x_2 x_1^{-a_2}, \cdots, x_r x_1^{-a_r}, x_{r+1}, \cdots, x_d\}$ is a set of generators of H and $x_i \cdot x_1^{-a_i} \in P_2$ for $2 \leqq i \leqq r$. If we continue this way we obtain a set of generators $\{y_1, \cdots, y_d\}$ of H, $y_i = \prod_{j=1}^{m-1} s_j^{\alpha_j^{(i)}}$ with $\alpha_j^{(i)} = 0$ for $i < j$ and $\nu_p(\alpha_i) \leqq \nu_p(\alpha_j)$ for $i > j$. If $x \in H$ and $x = \prod_{t=0}^{m-i-1} s_{i+t}^{\alpha_{i+t}}$, where $\alpha_i \neq 0$, $0 \leqq \alpha_{i+t} < p^n$ and $0 \leqq t \leqq m-i-1$, then $\nu_p(\alpha_i) = n-1$, otherwise $x^p \not\equiv 1 \bmod P_{i+1}$. Hence $\nu_p(\alpha_i^i) = n-1$ to every i, $1 \leqq i \leqq d$ in the set of generators $\{y_1, \cdots, y_d\}$ we have constructed above. Denote $t_i = [y_1, (i-1)s]$. Then

$$t_1^{p^n} \cdot t_2^{\binom{p^n}{2}} \cdots t_i^{\binom{p^n}{i}} \cdots t_{p^n} \equiv 1 \bmod P_{p^n+1}.$$

But $t_{p^n} = s_{p^n}^{p^{n-1}} u$, where $u \in P_{p^n+1}$. Hence $s_{p^n} = 1$ and H is generated by $p^n - 1$ elements. Finally if $H \leqq P$ then since P/P_1 is cyclic, $|H| \leqq p^{p^n}$.

(c) by Theorem 2.5,

$$s_i^{p^{n-1+t}} = \prod_{\mu=0}^{\mu_0} s_{i+t(p-1)+\mu}^{\alpha_{\mu+1}}, \quad \text{where } \mu_0 = m - i - 1 - t(p-1).$$

Hence if $t \geqq 1$ then $\mho_{m-1+t}(P_1) \leqq P_{1+t(p-1)}$. If $x = s^\alpha u$, $u \in P_1$, then by the collection formula

$$x^{p^\varepsilon} = (s^\alpha)^{p^\varepsilon} u^{p^\varepsilon} \cdots c_i^{\binom{p^\varepsilon}{i}} \cdots c_{p^\varepsilon}, \quad \text{where } c_i \in P_i.$$

Now, $s^{\alpha p^\varepsilon} \in P_{m-1}$ and $u^{p^\varepsilon} \in \mho_\varepsilon(P_1)$. If $p^\alpha \leqq i < p^{\alpha+1}$ and $1 + k(p-1) \leqq i \leqq (k+1)(p-1)$ then

$$p^{\varepsilon-\alpha} \,\Big|\, \binom{p^\varepsilon}{i}.$$

Since $k \geqq \alpha$,

$$c_i^{\binom{p^\varepsilon}{i}} \in \mho_{\varepsilon-k}(P_{1+k(p-1)}) \leqq P_{m-i(p-1)},$$

by Theorem 2.5. (Consider the subgroup $\langle P_{1+k(p-1)}, s\rangle$.) As $u^{p^\varepsilon} \in \mho_\varepsilon(P_1) \leqq P_{m-i(p-1)}$, hence $\mho_{e-i}(P) \leqq P_{m-i(p-1)}$. But then $H \leqq P_{m-i(p-1)}$. Therefore $|H| \leqq p^{i(p-1)}$, by (a).

(d) We may embed $P/C_p(H)$ in $\mathrm{GL}(d,p)$. Hence $\mho_\alpha(P) \leqq C_P(H)$ and $P_{p^\alpha} \leqq C_P(H)$ by theorems 16.3 and 16.5 respectively in [8, p. 382].

Proposition 2. *Let $A \triangle P$, $A \neq P$, $\exp(A) = p^e$. Let $H \leqq \mho_{e-1}(A)$, H ch A and assume that $C_P(K) \leqq A$ for every noncyclic characteristic subgroup $K \neq 1$ of A. If H is elementary abelian, $|H| > p$, and $\exp(P_1) \geqq p^{2n+3}$ then*

(a) *H is elementary abelian of order $\leqq p^{p-1}$. In particular $|\Omega(Z(\mho_{e-1}(A)))| \leqq p^{p-1}$.*

(b) $\mho(P) \leqq A$, $P_p \leqq A$.

(c) $\mho_{e-1}(P_1) \leqq \Omega(\mho_{e-2}(A)) \leqq \mho_{e-2}(P_1)$.

(d) $\mho_{n-1}(P_{m-p+1}) = \Omega(\mho_{e-2}(P_1)) = \Omega(\mho_{e-3}(A))$.

(e) *If $m \geqq (n+5)(p-1)$ then $A = P_1 \cdot \Phi(P)$.*

Proof. $H \leqq P$, H is elementary abelian. If $|H| \leqq p^d$ and $d \leqq p^\alpha$ then $\alpha \leqq n$ by Proposition 1(b). Hence $\mho_\alpha(P) \leqq A \leqq P$ by Proposition 1(d) and

$$\text{(0)} \qquad \mho_{e-1}(P) \leqq \mho_{e-1-\alpha}(A) \leqq \mho_{e-1-\alpha}(P).$$

Since $H \leqq \mho_{e-1}(A)$ obviously $H \leqq \mho_{e-1-\alpha}(A) \leqq \mho_{e-1-\alpha}(P)$ and $H \leqq$

$\mho_{e-1-\alpha}(P)$. Since $e \geqq 2n+3$, $\alpha \leqq n$ and $e-\alpha+1 \geqq n$, by Proposition 1(c) $d \leqq (\alpha+1)(p-1)$. Now, if $d > p^{\alpha-1}$ then $p^{\alpha-1}-1 < d \leqq (\alpha+1)(p-1)$, i.e., $p^{\alpha-1}-1 < (\alpha+1)(p-1)$. But for $\alpha \leqq 3$, $p^{\alpha}-1 \geqq (\alpha+1)(p-1)$. Hence $\alpha \leqq 2$ and by (0)

$$\mho_{e-1}(P) \leqq \mho_{e-3}(A) \leqq \mho_{e-3}(P). \tag{1}$$

Since $e \geqq 2n+3$, $\mho_{e-3}(P) = \mho_{e-3}(P_1)$, by Theorem 3.4, and $\mho_{e-3}(P)$ is regular. Moreover $|\Omega(\mho_{e-3}(P))| = |\Omega(\mho_{e-3}(P_1))| = |\mho_{e-3}(P_1)/\mho_{e-2}(P_1)| = p^{p-1}$. Hence

$$|\Omega(\mho_{e-3}(P))| = p^{p-1}. \tag{2}$$

On the other hand since $\mho_{e-2}(P_1)$ is regular, (1) implies that

$$1 < \mho_{e-1}(P) \leqq \Omega(\mho_{e-3}(A)) \leqq \Omega(\mho_{e-3}(P)) = \Omega(\mho_{e-3}(P_1)).$$

But $\Omega(\mho_{e-1}(A)) \leqq \Omega(\mho_{e-3}(A))$. Consequently

$$H \leqq \Omega(\mho_{e-1}(A)) \leqq \Omega(\mho_{e-3}(A)) \leqq \Omega(\mho_{e-3}(P)).$$

Therefore $|H| \leqq |\Omega(\mho_{e-3}(P))|$ and by (2), $|H| \leqq p^{p-1}$, as required.

(b) By *(a)* $\alpha = 1$. Hence (b) follows from Proposition 1(d).

(c) Since $\alpha = 1$ by (a), (c) follows from equation (0).

(d) Since $\mho(P) \leqq A$ by (b), $\mho_{e-2}(P_1) \leqq \mho_{e-3}(A) \leqq \mho_{e-3}(P_1)$. Hence $\Omega(\mho_{e-2}(P_1)) \leqq \Omega(\mho_{e-3}(A)) \leqq \Omega(\mho_{e-3}(P_1)$. But as $p \geqq 3$, $\Omega(\mho_{e-2}(P_1)) = \Omega(\mho_{e-3}(P_1))$. Therefore $\Omega(\mho_{e-2}(P_1)) = \Omega(\mho_{e-3}(A))$ and since $\mho_{n-1}(P_{m-p+1}) = \Omega(\mho_{e-2}(P_1))$, $\Omega(\mho_{e-3}(A)) = \mho_{n-1}(P_{m-p+1})$. Note that this means that $\mho_{n-1}(P_{m-p+1})$ is characteristic in A.

(e) Let $K = \mho_{n-1}(P_{m-p+1})$. Then $K \operatorname{ch} A$ by (d), K is elementary abelian of order p^{p-1} and hence $C_P(K) \leqq A$. On the other hand since $K = \langle s_{m-p+1}^{p^{n-1}}, \cdots, s_{m-1}^{p^{n-1}} \rangle$, $s_i \in C_P(K) \leqq A$ for $1 \leqq i \leqq p-1$, by Theorem 3.3. In particular $s_1 \in A$ and since $A \triangle P$, $P_1 \leqq A$. Since $\mho(P) \leqq A$ by (b) obviously $s^p \in A$. Hence $P_1 \cdot \langle s^p \rangle = P_1 \cdot \Phi(P) \leqq A$. But $P_1 \cdot \Phi(P)$ is a maximal subgroup of P and $A \neq P$. Hence $A = P_1 \cdot \Phi(P)$.

Proposition 3. *Let P be a p-group of type (m, n), $A = P_1 \cdot \Phi(P)$ and assume that* $\exp(P_1) = e \geqq 2n+1$. *Then*

(a) *To every $u \in P_1$ and to every $\alpha \geqq 1$, $(s^{p^\alpha} \cdot u)^{p^{e-1}} = s^{p^{\alpha+e-1}} \cdot u^{p^{e-1}}$. Hence $(s^{p^\alpha} \cdot u)^{p^{e-1}} = u^{p^{e-1}}$.*

(b) *If $u \in P_1$ and $|u| = p^e$ then $|s^{p^\alpha} \cdot u| = p^e$ for every $\alpha \geqq 1$.*

(c) *If $u \in P_1$ and $u^{p^{e-1}} = 1$ then $(s^{p^\alpha} u)^{p^{e-1}} = 1$ for every $\alpha \geqq 1$.*

(d) $\Omega_{e-1}(A) = \Omega_{e-1}(P_1) \cdot \langle s^p \rangle$.

(e) *$A/\Phi(A)$ is (elementary abelian) of order at most p^{p+1}.*

(f) *If $t \in N_G(P)$ and $s^t \equiv s^a \bmod P_2$, where $a \in \mathbf{Z}$, then $(s^p)^t \equiv (s^p)^a \bmod \Phi(A)$.*

(g) *$|\Omega_{e-1}(A) \cdot \Phi(A)/\Phi(A)| \leqq p^p$.*

PROOF. (a) $(s^{p\alpha} \cdot u)^{p^{e-1}} = s^{p\alpha+e-1} u^{p^{e-1}} c_2^{\binom{p^{e-1}}{2}} \cdots c_t^{\binom{p^{e-1}}{t}} \cdots c_{p^{e-1}}$ by the collection formula, where $c_t \in K_t(\langle s^{p\alpha}, u\rangle) \leqq P_t$. We show that

$$c_t^{\binom{p^{e-1}}{t}} = 1 \quad \text{for } t \geqq 2.$$

$$[s^{p\alpha}, s_i] = s_{i+1}^{p^\alpha} d_2^{\binom{p^\alpha}{2}} \cdots d_t^{\binom{p^\alpha}{t}} \cdots d_{p\alpha}, \quad \text{where } d_t \in K_t(\langle s, s_{i+1}\rangle) \leqq P_{t+i},$$

by the collection formula. Hence $[s^{p^\alpha}, s_i] \in \Gamma_{p-1}(P_{i+1})$. Since c_t is a product of commutators of $[s^{p^\alpha}, s_i]$ with x_j, where $x_j \in \{s^{p^\alpha}, s_i\}$, $c_t \in \Gamma_{p-1}(P_t)$, by Theorem 3.1. If $1 + k(p-1) \leqq t \leqq (k+1)(p-1)$ and $c_t \in \Gamma_{p-1}(P_t)$ then by Theorem 3.4, $c_t^{p^{e-k-1}} = 1$. If $p^\alpha \leqq t < p^{\alpha+1}$ then

$$p^{e-1-\alpha} \,\Big|\, \binom{p^{e-1}}{t}.$$

Now, by the computation in Theorem 3.4, $e - 1 - \alpha \geqq e - 1 - k$. Hence

$$c_t^{\binom{p^{e-1}}{t}} = 1$$

and since $e \geqq 2n + 1$, $(s^{p\alpha}u)^{p^{e-1}} = u^{p^{e-1}}$.

(b) and (c) are consequences of (a).

(d) Let $x = s^{p^\alpha}u$, where $u \in P_1$ and $\alpha \geqq 1$. By (a) $x^{p^{e-1}} = 1 \Leftrightarrow u^{p^{e-1}} = 1$. Hence $C = \{x \in A \mid x^{p^{e-1}} = 1\} = \{x \in A \mid x = s^{p^\alpha}u, u^{p^e} = 1\}$ is a set of generators for $\Omega_{e-1}(A)$. $\Omega_{e-1}(P_1) = \{u \in P_1 \mid u^{p^{e-1}} = 1\}$ by Theorem 3.4. Hence $C = \Omega_{e-1}(P_1) \cdot \langle s^p \rangle = \Omega_{e-1}(A)$.

(e) Since $\Phi(P_1) \leqq \Phi(A)$, to compute $A/\Phi(A)$ we may assume $\Phi(P_1) = 1$. Now, $[s^p, s_1] \in A' \leqq \Phi(A)$. On the other hand $[s^p, s_1] = s_{p+1}$ by the collection formula ($\Phi(P_1) = 1$) hence $[s^p, s_1] \equiv s_{p+1} \bmod \Phi(A)$, i.e., $s_{p+1} \in \Phi(A)$. Since $\Phi(A) \triangle P$ and $\Phi(P_1) \leqq A$, $A/\Phi(A) = \langle \bar{s}_p, \bar{s}_1, \cdots, \bar{s}_p \rangle$ where $\bar{x} = x \cdot \Phi(A)$ for $x \in P$.

(f) $(s^a s_2^{\alpha_2} \cdots s_{m-1}^{\alpha_{m-1}})^p = s^{ap} \cdots s_{m-1}^{\alpha_{m-1}} \cdot c_2^{\binom{p}{2}} \cdots c_p$, where $c_i \in K_i(\langle s^a, s_2^{\alpha_2}, \cdots, s_{m-1}^{\alpha_{m-1}}\rangle) \leqq P_{i+1}$. Hence

$$c_i^{\binom{p}{i}} \in \Gamma_{p-1}(P_{i+1}) \quad \text{and} \quad c_2^{\binom{p}{2}} \cdots c_p \in \Gamma_{p-1}(P_3).$$

In particular

$$c_2^{\binom{p}{2}} \cdots c_p \equiv s_3^{\beta_3} \cdots s_p^{\beta_p} \bmod P_{p+1}, \quad \text{where } p \mid \beta_t \text{ for } 3 \leqq t \leqq p.$$

Therefore by (e) and Theorem 3.1, $(s^a s_2^{\alpha_2} \cdots s_{m-1}^{\alpha_{m-1}})^p \equiv s^{ap} \bmod \Phi(A)$.

(g) $s_1 \notin \Omega_{e-1}(A)\cdot\Phi(A)$, by (c) and (e). Therefore (g) is a consequence of (c).

We now begin the proof of Theorem 1. Assume that G is a minimal counterexample. Then $O_{p'}(G) = 1$.

PROPOSITION 4. *Let $N \triangle P$ and assume that N is not cyclic. Then $C = C_G(N) = O_{p'}(C)\cdot C_P(N)$.*

PROOF. If $N \not\triangle G$ then by the minimality hypothesis $K = N_G(N) = O_{p'}(K)\cdot P\cdot T$, where $T\cdot O_{p'}(K)/O_{p'}(K)$ is cyclic of order $\tau, \tau \mid p-1$. Hence $C = C_G(N) = O_{p'}(C)\cdot C_p(N)$. So assume $N \triangle G$. If $K = C_G(N)\cdot P \neq G$ then $N_k(P) = P\cdot C_K(P)$ and $K = O_{p'}(K)\cdot P$, $[O_{p'}(K), N] \leqq O_{p'}(K)\cap N = 1$, hence $O_{p'}(K) \leqq O_{p'}(C_G(N))$, which proves the proposition. Assume therefore $G = C_G(N)\cdot P$ and $N_G(P) = P\cdot C_G(P)$ (since N is not cyclic, Theorem 0.2 implies that $\tau = 1$; hence $N_G(P) = P\cdot C_G(P)$) and prove that G has a normal p-complement. Since $L/O_p(G) = K_\infty(P/O_p(G)) \not\triangle G/O_p(G)$, $N_G(L) = O_{p'}(N_G(L))\cdot P$ and $G/O_p(G)$ has a normal p-complement $Q_0/O_p(G)$, by theorem 12.10 in [3, p. 37], where $Q_0 \cap P = O_p(G)$. If $O_p(G) \leqq \Phi(P)$, then by Tate's theorem [8, p. 431] Q_0 has a normal p-complement, hence G has a normal p-complement. Therefore $O_p(G) \not\leqq \Phi(P)$. If $s_1 \notin O_p(G)$ then there exists an $x \in P\setminus P_1\Phi(P)$ s.t. $x \in O_p(G)$. Since $O_p(G)\triangle P$, $P_2 \leqq O_p(G)$ and $Z_i(O_p(G)) = Z_i(P) = P_{m-i}$ for $1 \leqq i \leqq m-3$, by Proposition 0.2(c). Therefore $P_i \triangle G$ for $3 \leqq i \leqq m-1$ and in particular $P_3 \triangle G$. P/P_3 is of class 2, hence P/P_3 is regular. Consequently G/P_3 has a normal p-complement Q_1/P_3, $Q_1 \cap P = P_3$, by Wielandt's transfer theorem. But then by Tate's theorem Q_1 has a normal p-complement and hence G has. Therefore $s_1 \in O_p(G)$. Since $O_p(G)\triangle P$ obviously $P_1 \leqq O_p(G)$ and $\Omega_{e-1}(P_1) \leqq \Omega_{e-1}(O_p(G))$. This implies that $P/\Omega_{e-1}(O_p(G))$ is regular by Theorem 3.4, hence by Wielandt's transfer theorem for $\bar{P} = P/\Omega_{e-1}(O_p(G))$, $\bar{P}$ has a normal p-complement Q/Ω_{e-1} and

$$Q \cap P = \Omega_{e-1}(O_p(G)). \tag{1}$$

If $P = O_p(G)$ then $G = N_G(P) = P\cdot C_G(P)$ and G has a normal p-complement. Hence we may assume that $O_p(G) \neq P$. Now, $P_1 \leqq O_p(G) \leqq P_1\cdot\Phi(P)$, hence $\Omega_{e-1}(O_p(G)) \leqq \Omega_{e-1}(P_1\cdot\Phi(P))$ and by Proposition 3(d), $\Omega_{e-1}(O_p(G)) \leqq \Omega_{e-1}(P_1)\cdot\langle s^p\rangle$. By Theorem 3.4(d), $\Omega_{e-1}(P_1)\langle s^p\rangle \leqq \Phi(P)$. Hence

$$\Omega_{e-1}(O_p(G)) \leqq \Phi(P). \tag{2}$$

(1) and (2) imply that $Q \cap P \leqq \Phi(P)$. Hence Q has a normal p-complement by the theorem of Tate. But then G has a normal p-complement, as required.

COROLLARY 1. *If N is a noncyclic normal p-subgroup of G then $C_P(N) = C_G(N)$.*

PROOF. By Proposition 4, $C = C_G(N) = O_{p'}(G) \cdot C_P(N)$; $O_{p'}(G) \operatorname{ch} C \triangle G \Rightarrow O_{p'}(C) \triangle G$. Hence $O_{p'}(G) = 1$ and $C = C_P(N)$.

COROLLARY 2. $O_p(G) = P_1 \cdot \Phi(P)$.

PROOF. If $A = O_p(G)$ has no characteristic cyclic subgroup (c.c.s.) $K \neq 1$ then we are done by Proposition 2(e). Hence let K be a c.c.s. of A. Then $K \leqq Z(P) := Z$. Hence we may assume that K is the maximal c.c.s. of A and $K \leqq Z(G)$. If A/K has a c.c.s. then $s'_{m-2} \equiv s_{m-2} \bmod Z$ and $s'_{m-1} = s_{m-1}$ by Theorem 0.3(c). Therefore $t = 1$ and G has a normal p-complement. So A/K has no c.c.s. Let $\exp(A/Z) = e$ and $\Omega(Z(\mho_{e-1}(A/K))) = H/K$. Then $\bar{H} = HZ/Z \operatorname{ch} \bar{A}$. If $\bar{H}$ is cyclic then $H \leqq P_{m-2}$ and as H is not cyclic, $C_p(H) \leqq A$. But then $\Phi(P) \cdot P_1 \leqq C_p(\Omega(H))$ and $A = \Phi(P) \cdot P_1$. Consequently, $\bar{H}$ is a noncyclic elementary abelian subgroup of $\mho_{e-1}(\bar{A})$. Therefore by Proposition 2, $\bar{A} = \Phi(P) \cdot P_1/Z$ and $A = \Phi(P) \cdot P_1$, as required.

PROPOSITION 5. *Let $A = O_p(G)$ and to every $X \leqq G$ denote $\tilde{X} = X\Phi(A)/\Phi(A)$. Then $\langle \tilde{s}^p \rangle \triangle \tilde{G}$.*

PROOF. Let $M = \Omega_{e-1}(A)$, $K = F_p$. M is a $K\tilde{G}$-module which has dimension at most p over K, by Proposition 3(g). Also by Propositions 3(d) and 3(f) M decomposes, as a $K\tilde{N}$-module:

(1) $\qquad M_{K\tilde{N}} = U_1 \oplus U_2, \qquad$ where $U_1 = \langle \tilde{s}^p \rangle, \quad U_2 = \Omega_{e-1}(P_1)$.

M is not a projective $K\tilde{G}$ module, since then U_1 and U_2 have to be, which is clearly impossible as $\dim_K(U_i) < p$ for $i = 1, 2$. Therefore U_1 and U_2 have vertex $\tilde{P}$ and if M is an indecomposable $K\tilde{G}$ module, then M also has vertex $\tilde{P}$ (see [5]). But by Green's transfer theorem in [6] there exists a unique (up to isomorphism) indecomposable $K\tilde{N}$ module U s.t. $U \mid M_{K\tilde{N}}$ (i.e. U is isomorphic to a direct summand of $M_{K\tilde{N}}$) and U has vertex $\tilde{P}$. Consequently M is not indecomposable. By (1) if $M = M_1 \oplus M_2$ and $U_1 \mid M_{1K\tilde{N}}$ then again by Green's transfer theorem $U_1 = M_{1K\tilde{N}}$ and $\langle \tilde{s}^p \rangle$ is a $\tilde{G}$-invariant subspace of $\tilde{P}$, i.e., $\langle \tilde{s}^p \rangle \triangle \tilde{G}$.

PROOF OF THEOREM 1. Assume first that $\tau = 1$. Then $N_G(P) = P \cdot C_G(P)$, by Theorem 0.2; $\Omega_{e-1}(O_p(G)) \leqq \Phi(P)$, by Theorem 3.4 and Proposition 3(d). Since $P_1 \leqq O_p(G)$, $P/\Omega_{e-1}(O_p(G))$ is regular. Hence by Wielandt's transfer theorem for $P/\Omega_{e-1}(O_p(G))$ and Tate's theorem G has a normal p-complement. (We have stated these arguments in detail in Proposition 4.) Therefore assume that

$\tau \neq 1$. If $s^\tau \equiv s^a \bmod P_2$, $a \in \mathbf{Z}$ then $a \neq 1$. Since $(s^p)^\tau \equiv (s^p)^a \bmod \Phi(A)$ by Proposition 3(f) $\langle s^p \rangle \not\leqq Z(G)$. Hence $\tilde{C} := C_{\tilde{G}}(\tilde{s}^p) \triangle \tilde{G}$ and $1 < |\tilde{G} : \tilde{C}| = |G : C| \leqq p - 1$. But then, since the theorem is true for C by assumption, C has a normal p-complement and hence G is not a counterexample. This proves Theorem 1.

The following theorems are consequences of Theorem 1.

THEOREM 2. *Let G be a finite group with a Sylow p-subgroup P of type (m, n), $p > 2$. Assume that $m \geqq (n+5)(p-1)+1$. If $x, y \in P$ and $y = x^g$ for $g \in G$ then there exists an element $n \in N_G(P)$ s.t. $y = x^n$.*

PROOF. By induction on $|G : P| = \nu$. For $\nu = 1$, obvious. Assume $\nu \geqq 2$ and G is a minimal counterexample.

PROPOSITION 1. (a) *If $N \leqq P$, $N \triangle G$ then $N \leqq Z(P)$.*

(b) *Assume that $N \triangle P$, $N \not\!\triangle\, G$ and N is not cyclic. If $x, y \in P$ and there exists $h \in N_G(N)$ s.t. $y = x^h$ then there exists a $u \in N_G(P)$ s.t. $y = x^u$.*

PROOF. (a) Assume that $N \not\leqq Z(P)$. Then N is not cyclic hence by Theorem 1, $G = QPT$, $(|Q|, p) = 1$, $|TQ/Q| \mid p - 1$. If $x, y \in P$, $y = x^g$ for a certain $g \in G$ then $y \equiv x^g \bmod Q$. Since $G/Q \cong PT$, $x^g \equiv x^u \bmod Q$ for a certain $u \in PT$ and $x^g = x^u \cdot q$, where $q \in Q$. So $q = x^g \cdot (x^u)^{-1} = yx^{-u} \in P$, hence $q \in Q \cap P = 1$, i.e. $x^g = x^u$, contradicting our assumption on G. Therefore N is cyclic and $N \leqq Z(P)$.

(b) By Theorem 1, $N_G(N) = Q \cdot P \cdot T$. Hence by the above argument, but now with $N_G(N)$ in place of G, if $x, y \in P$, $g \in N_G(N)$ then there exists a $u \in N_G(P)$ s.t. $y = x^u$.

PROPOSITION 2. *If $Z \leqq Z(P)$ and Z is weakly closed in P w.r. to G then $Z \leqq Z(G)$.*

PROOF. Since Z is weakly closed in P w.r. to G:

(1) two elements $x, y \in P$ are conjugate in G iff they are conjugate in $N_G(Z)$.

Now Z ch (P) $(Z(P)$ is cyclic) hence $N_G(P) \leqq N_G(Z)$. If $N_G(P) \neq G$ then by the assumption on G:

(2) two elements $x, y \in P$ are conjugate in $N_G(Z)$ iff they are conjugate in $N_G(P)$.

Hence if $N_G(P) \neq G$, we are done by (1) and (2). So assume that $N_G(Z) = G$. If $Z \not\leqq Z(G)$ then $C_G(Z) \triangle G$, $|G : C_G(Z)| \mid p - 1$ and again by the induction hypothesis on G, two elements in P are conjugate in $C_G(Z)$ iff they are conjugate in $N_G(P) \cap C_G(Z)$. Since $G = C_G(Z)T$, $T \leqq N_G(P)$, if x and y are elements of P then x and y are conjugate in G iff they are conjugate in $N_G(P)$, contradicting our assumption on G (i.e. G is not a counterexample). Therefore $Z \leqq Z(G)$.

PROOF OF THE THEOREM. Denote by $J = J(P)$ the Thompson subgroup of P. By Proposition 1(a) and Theorem 1, $N_G(J) = QPT$, $(|Q|, p) = 1$ and $Q \leqq C_G(J)$. Therefore $\Omega_i(Z(P)) \triangle N_G(J)$ to every $1 \leqq i \leqq n-1$ and by theorem 14.5 in [3, p. 42] $\Omega_i(Z))$ is weakly closed in P w.r. to G for $1 \leqq i \leqq n-1$. Hence $\Omega_i(Z) \leqq Z(G)$ by Proposition 2 and in particular $s^t_{m-1} = s_{m-1}$ for every $t \in T(\leqq N_G(P))$. This implies that $Z(P) \leqq Z(N_G(J))$. But then by Theorem 14.10 in [3, p. 45]

(3) $Z(P) := Z$ is weakly closed in P w.r. to G.

Consequently, by Proposition 2,

(4) $Z = Z(P) \leqq Z(G)$.

Now, denote $\bar{X} = XZ/Z$ for $X \leqq G$. Let $J_1/Z = J(\bar{P})$. $J_1 \triangle P$ and by Theorem 1 and Proposition 1, $N_G(J_1) = Q_1PT$. Hence $N_{\bar{G}}(\bar{J}_1) = \bar{Q}_1\bar{P}\bar{T}$ $(|\bar{Q}_1|, p) = 1$ and $\mho_i(Z_2(P)) \cdot Z/Z \triangle N_{\bar{G}}(\bar{J}_1)$. Therefore by theorem 14.5 in [3, p. 42] $\mho_1(Z_2(P))Z/Z$ is weakly closed in P/Z w.r. to G/Z. Since $Z(P)$ is weakly closed in P by (3) and $\mho_1(Z_2(P))Z/Z$ is weakly closed in P/Z, $\Omega_i(Z_2(P)) \cdot Z = H_0$ is weakly closed in P. Moreover, since H_0/Z and Z are strongly closed in P/Z and P w.r. to G/Z and G respectively, H_0 is strongly closed in P w.r. to G. (Note that H_0/Z and Z are cyclic.) Now H_0 is an abelian subgroup of P which is strongly closed in P w.r. to G. Hence by theorem 6.1 in Glauberman [2], if x and y are elements of P and $y = x^g$ for a $g \in G$ then they are conjugate in $N_G(H_0)$. But H_0 is not cyclic. Hence by Proposition 1, if $x, y \in P$ are conjugate in $N_G(H_0)$, they are conjugate in $N_G(P)$. Consequently, if $x, y \in P$ are conjugate in G, they are already conjugate in $N_G(P)$, contradiction. Hence there is no counterexample to Theorem 2.

The following two theorems are trivial consequences of Theorems 1 and 2.

THEOREM 3. *Let G be a finite group, P a Sylow p subgroup as in Theorem 2. Denote* $N = N_G(P)$. *Then* $G/O^p(G) \cong N/O^p(N)$.

PROOF. By Theorem 1, $N = QPT$ $(|Q|, p) = 1$ and $Q \leqq C_G(P)$. Hence $N' = [QPT, QPT] = Q_0P'[P, T]$, $Q_0 \leqq Q$ and

$$P \cap N' = P'[P, T]. \tag{1}$$

By theorem 3.4 in [4, p. 250]

$$P \cap G' = \langle x^{-1}y \mid y = x^g, x, y \in P, g \in G \rangle$$
$$= \langle x^{-1}y \mid y = x^u, x, y \in P, u \in N \rangle$$
$$= \langle [x, u] \mid x \in P, u \in N \rangle = [P, N] = [P, QPT] = P'[P, T].$$

$$P \cap G' = P'[P, T]. \tag{2}$$

(1) and (2) imply that $P \cap G' = P \cap N'$, hence by Tate's theorem $G/O^p(G) \cong N/O^p(N)$.

REMARK. If P is a p-group of type (m, n) and $m \geqq p + 2$ then P may have many sections isomorphic to $\mathbf{Z}_p \operatorname{wr} \mathbf{Z}_p$ and may have homomorphic images of this type. Hence Theorem 3 cannot be derived from known theorems (such as Wielandt's [12] or Yoshida's [13]).

The following theorem describes the structure of p-local subgroups of G.

THEOREM 4. *Let G and P be as in Theorem* 1. *If $H \leqq D \leqq P$ and $H \triangle P$ but $H \not\leqq Z(P)$ then $N = N_G(D) = QBT_0$ where $Q = O_{p'}(N)$, $QB = O_{p',p}(N)$, B is a Sylow p-subgroup of N and $T_0 \leqq T$.*

PROOF. $H \triangle P$, $H \leqq D \Rightarrow H \triangle D$. By Theorems 1 and 2, H is weakly closed in P w.r. to G (in fact H is strongly closed in P), hence is weakly closed in B w.r. to N. Therefore $H^g = H$ for every $g \in N$, i.e., $H \triangle N$. But then $N \leqq N_G(H) = Q_0PT$ and N has the required form.

ACKNOWLEDGEMENT

This work is a part of my doctoral thesis done under the kind supervision of Professor A. Mann. I wish to express my thanks to Professor Mann for his aid during the preparation of this result.

REFERENCES

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

2. G. Glauberman, *A sufficient condition for p-stability*. Proc. London Math. Soc. **25** (1972), 253–287.

3. G. Glauberman, *Local and global properties of finite groups*, in *Finite Simple Groups* (M. B. Powell, ed.), Academic Press, 1971.

4. D. Gorenstein, *Finite Groups*, Harper Series in Modern Mathematics, 1967.

5. J. A. Green, *On the indecomposable representations of finite groups*, Math. Z. **70** (1959), 430–445.

6. J. A. Green, *A transfer theorem for modular representations*, J. Algebra **1** (1964), 73–84.

7. Leedham Green and Susan McKay, *p-groups of maximal class*, Quart. J. Math. Oxford Ser. **27** (1976), 1–28.

8. B. Huppert, *Endliche Gruppen I, Die Grundlehren der Math. Wissenschaften*, Band 134, Springer Verlag, Berlin and New York, 1967.

9. A. Juhász, *The automorphism group of a class of finite p-groups*, submitted.

10. A. Juhász, *Finite groups with a Sylow p-subgroup of maximal class*, submitted.

11. R. J. Miech, *Metabelian p-groups of maximal class*, Trans. Amer. Math. Soc. **152** (1960), 151–200.

12. R. Shepherd, *p-groups of maximal class*, Doctoral Thesis, Chicago, 1970.

13. T. Yoshida, *Character-theoretic transfer*, J. Algebra **52** (1978), 1–38.

INSTITUTE OF MATHEMATICS
THE HEBREW UNIVERSITY OF JERUSALEM
JERUSALEM, ISRAEL