MATH. SCAND. 62 (1988), 153–172

STRUCTURE AND DERIVED LENGTH OF FINITE p-GROUPS POSSESSING AN AUTOMORPHISM OF p-POWER ORDER HAVING EXACTLY p FIXPOINTS

IAN KIMING

Introduction.

Everywhere in this paper p denotes a prime number.

In [1] Alperin showed that the derived length of a finite p-group possessing an automorphism of order p having exactly p^n fixpoints is bounded above by a function of the parameters p and n.

The purpose of this paper is to prove the same type of theorem for the derived length of a finite p-group possessing an automorphism of order p^n having exactly p fixpoints. However, we will restrict ourselves to the case where p is odd.

A strong motivation for the consideration of this class of finite p-groups is induced by the fact that the theory of these groups is strongly similar to certain aspects of the theory of finite p-groups of maximal class. For the theory of finite p-groups of maximal class the reader may consult [2] or [4, pp. 361–377].

In section 1 we derive a more useful description of the groups in question and we show that the theory of these objects is naturally connected to the theory of finite p-groups of maximal class. We illustrate the ideas in abelian p-groups.

In section 2 we study p-power- and commutators-structure.

Based on the results of section 2 we prove the main theorems in section 3. The method leading to the proof of our main theorems does not resemble Alperin's method. The former method may be described as a detailed analysis of commutator- and p-power-structure of the groups in question. The central method is a development of a method mentioned by Leedham-Green and McKay in [5] and is of "combinatorial" nature.

Received January 5, 1987.

Notation.

The letter E always denotes the neutral element of a given group.

If X and Y are elements of a group we write

$$X^Y = Y^{-1}XY \quad \text{and} \quad [X, Y] = X^{-1}Y^{-1}XY.$$

Then we have the formulas

$$[X, YZ] = [X, Z][X, Y][X, Y, Z] \quad \text{and} \quad [XY, Z] = [X, Z][X, Z, Y][Y, Z]$$

($[X_1, \ldots, X_{n+1}] = [[X_1, \ldots, X_n], X_{n+1}]$).

If α is an automorphism of a group we write X^α for the image of X under α.

If α is an automorphism of a group $\mathfrak{G}$, and $\mathfrak{N}$ is an α-invariant, normal subgroup of $\mathfrak{G}$, then we write α also for the automorphism induced by α on $\mathfrak{G}/\mathfrak{N}$.

For a given group, $\mathfrak{G}$, the terms of the lower central series of $\mathfrak{G}$ are written $\gamma_i(\mathfrak{G})$ for $i \in \mathsf{N}$.

If $\mathfrak{G}$ is a finite p-group, then $\omega(\mathfrak{G}) = k$ means that $|\mathfrak{G}/\mathfrak{G}^p| = p^k$.

1.

We now define a certain class of finite p-groups which turns out to be precisely the objects in which we are interested, that is the finite p-groups possessing an automorphism of p-power order having exactly p fixpoints.

Definition. Suppose that $\mathfrak{G}$ is a finite p-group. We say that $\mathfrak{G}$ is *concatenated* if and only if $\mathfrak{G}$ has

i) a strongly central series

$$\mathfrak{G} = \mathfrak{G}_1 \geqq \mathfrak{G}_2 \geqq \ldots \geqq \mathfrak{G}_n = \{E\}$$

(putting $\mathfrak{G}_k = \{E\}$ for $k \geqq n$, "strongly central" means that $[\mathfrak{G}_i, \mathfrak{G}_j] \leqq \mathfrak{G}_{i+j}$ for all i, j),

ii) elements $G_i \in \mathfrak{G}_i$, $i = 1, \ldots, n$, and

iii) an automorphism, α,

such that

1) $|\mathfrak{G}_i/\mathfrak{G}_{i+1}| = p$, $i = 1, \ldots, n-1$,

2) $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ is generated by $G_i\mathfrak{G}_{i+1}$, $i = 1, \ldots, n$,

3) $[G_i, \alpha] = G_i^{-1}G_i^\alpha \equiv G_{i+1} \mod \mathfrak{G}_{i+2}$, $i = 1, \ldots, n-1$.

In this situation we shall also say that $\mathfrak{G}$ is α-concatenated. It is easy to see that α has p-power order whenever α is an automorphism of the finite p-group $\mathfrak{G}$ such that $\mathfrak{G}$ is α-concatenated.

If $\mathfrak{G}$ is a finite p-group, then the statement "$\mathfrak{G}$ is α-concatenated" means that $\mathfrak{G}$ possesses an automorphism, α, such that $\mathfrak{G}$ is α-concatenated.

Whenever $\mathfrak{G}$ is given as an α-concatenated p-group, we shall assume that a strongly central series $\mathfrak{G} = \mathfrak{G}_1 \geqq \mathfrak{G}_2 \geqq \ldots$ and elements $G_i \in \mathfrak{G}_i$ have been chosen so that conditions 1), 2) and 3) in the definition above are fulfilled; the symbols $\mathfrak{G}_i$ and G_i always refer to this choice.

THEOREM 1. *Suppose $\mathfrak{G}$ is an α-concatenated p-group.*
For all $i \in \mathrm{N}$, $\mathfrak{G}_{i+1}$ is the image of $\mathfrak{G}_i$ under the mapping

$$X \mapsto X^{-1}X^{\alpha} = [X, \alpha]$$

and if $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ is generated by $X\mathfrak{G}_{i+1}$, then $\mathfrak{G}_{i+1}/\mathfrak{G}_{i+2}$ is generated by $[X, \alpha]\mathfrak{G}_{i+2}$.

PROOF. Suppose that $\mathfrak{G}$ has order p^{n-1}. Then $[G_{n-1}, \alpha] = E$ and so $[G_{n-1}^a, \alpha] = E$ for all a. Assume that the enunciations have been proved for $i \geqq k+1$, where $1 \leqq k < n-1$. If $X \in \mathfrak{G}_k - \mathfrak{G}_{k+1}$, we write $X = G_k^a Y$, where $a \in \{1, \ldots, p-1\}$ and $Y \in \mathfrak{G}_{k+1}$. Then,

$[X, \alpha] = [G_k^a, \alpha][G_k^a, \alpha, Y][Y, \alpha]$ whence
$[X, \alpha] \equiv [G_k, \alpha]^a \bmod \mathfrak{G}_{k+2}$ sinde it is easy to see that
$[G_k^r, \alpha] \equiv [G_k, \alpha]^r \bmod \mathfrak{G}_{k+2}$ fot all r. Thus we deduce
$[X, \alpha] \equiv G_{k+1}^a \bmod \mathfrak{G}_{k+2}$.

As a consequence we have demonstrated the last enunciation (for $i = k$) and that the image of $\mathfrak{G}_k$ under the mapping $X \mapsto [X, \alpha]$ is contained in $\mathfrak{G}_{k+1}$. It follows that the group of fixpoints of α on $\mathfrak{G}$ is $\mathfrak{G}_{n-1}$.

Now, for $X, Y \in \mathfrak{G}_k$,

$$[X, \alpha] = [Y, \alpha] \Leftrightarrow YX^{-1} = (YX^{-1})^{\alpha} \Leftrightarrow YX^{-1} \in \mathfrak{G}_{n-1},$$

and since $\mathfrak{G}_{n-1} \leqq \mathfrak{G}_k$, we see that the image of the mapping $X \mapsto [X, \alpha]$ restricted to $\mathfrak{G}_k$ has order

$$|\mathfrak{G}_k : \mathfrak{G}_{n-1}| = \frac{1}{p}|\mathfrak{G}_k| = |\mathfrak{G}_{k+1}|.$$

Thus this image must be all of $\mathfrak{G}_{k+1}$.

THEOREM 2. *Let $\mathfrak{G}$ be a finite p-group and let α be an automorphism of p-power order in $\mathfrak{G}$. Then the following statements are equivalent:*

1) $\mathfrak{G}$ *is α-concatenated.*
2) *α has exactly p fixpoints on $\mathfrak{G}$.*

PROOF. 1) *implies* 2): If $\mathfrak{G}$ has order p^{n-1} then Theorem 1 implies that α's fixpoint group on $\mathfrak{G}$ is $\mathfrak{G}_{n-1}$; but $|\mathfrak{G}_{n-1}| = p$.

2) *implies* 1: We show by induction on $|\mathfrak{G}|$ that $\mathfrak{G}$ is α-concatenated. Of course we may assume that $|\mathfrak{G}| > p$.

If $\mathfrak{N}$ is an α-invariant, normal subgroup of $\mathfrak{G}$, it is well-known that α has at the most p fixpoints on $\mathfrak{G}/\mathfrak{N}$ ($X\mathfrak{N}$ is a fixpoint if and only if $X^{-1}X^{\alpha} \in \mathfrak{N}$; $X^{-1}X^{\alpha} = Y^{-1}Y^{\alpha}$ if and only if YX^{-1} is a fixpoint of α on $\mathfrak{G}$). Since the order of α is a power of p, α must have exactly p fixpoints on $\mathfrak{G}/\mathfrak{N}$.

Let $\mathscr{F}$ be the group of fixpoints for α on $\mathfrak{G}$. Since α has p-power order, $\mathscr{F}$ is contained in the center of $\mathfrak{G}$. From the inductional hypothesis we conclude that $\mathfrak{G}/\mathscr{F}$ is α-concatenated. Therefore there exists a strongly central series

$$\mathfrak{G}/\mathscr{F} = \mathfrak{G}_1/\mathscr{F} \geqq \ldots \geqq \mathfrak{G}_n/\mathscr{F} = \{E\}$$

and elements $G_i \in \mathfrak{G}_i$ such that $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ has order p,

$\mathfrak{G}_i/\mathfrak{G}_{i+1}$ is generated by $G_i\mathfrak{G}_{i+1}$ for $i = 1,\ldots,n-1$ and
$[G_i\mathscr{F}, \alpha] \equiv G_{i+1}\mathscr{F} \mod \mathfrak{G}_{i+2}/\mathscr{F}$, $i = 1,\ldots,n-2$.

Then

$$[G_i, \alpha] \equiv G_{i+1} \mod \mathfrak{G}_{i+2} \text{ for } i = 1,\ldots,n-2 \text{ and } E \neq [G_{n-1}, \alpha] \in \mathscr{F}.$$

Putting $G_n = [G_{n-1}, \alpha]$, G_n generates $\mathscr{F}$. Put $\mathfrak{G}_{n+i} = \{E\}$ for $i \in \mathrm{N}$.

Then we only have to show that the series

$$\mathfrak{G} = \mathfrak{G}_1 \geqq \mathfrak{G}_2 \geqq \ldots \geqq \mathfrak{G}_n = \mathscr{F} \geqq \mathfrak{G}_{n+1} = \{E\}$$

is strongly central. Consider the semidirect product $\mathfrak{H} = \mathfrak{G}\langle\alpha\rangle$. Since the terms of the series are all α-invariant we get $\gamma_i(\mathfrak{H}) \leqq \mathfrak{G}_i$ for $i \geqq 2$. Since $[G_1, \alpha, \ldots, \alpha] \in \mathfrak{G}_i - \mathfrak{G}_{i+1}$ if $\mathfrak{G}_i \neq \{E\}$, we see that $\gamma_i(\mathfrak{H}) = \mathfrak{G}_i$ for $i \geqq 2$. Then

$$[\mathfrak{G}_i, \mathfrak{G}_j] \leqq [\gamma_i(\mathfrak{H}), \gamma_j(\mathfrak{H})] \leqq \gamma_{i+j}(\mathfrak{H}) = \mathfrak{G}_{i+j}$$

for all $i, j \in \mathrm{N}$.

COROLLARY 1. *If $\mathfrak{G}$ is a finite, α-concatenated p-group, then the only α-invariant, normal subgroups of $\mathfrak{G}$ are the $\mathfrak{G}_i$ for $i \in \mathrm{N}$.*

PROOF. Suppose that $\mathfrak{N}$ is an α-invariant, normal subgroup of $\mathfrak{G}$. Since α has p-power order, α has exactly p fixpoints on $\mathfrak{N}$. Thus α's fixpoint group on $\mathfrak{G}$ is contained in $\mathfrak{N}$. By induction on $|\mathfrak{G}|$ the statement follows immediately.

The next theorem shows that the theory of finite, concatenated p-groups is connected to certain aspects of the theory of finite p-groups of maximal class.

THEOREM 3. *Let $\mathfrak{G}$ be a finite p-group.*
Then $\mathfrak{G}$ is α-concatenated for an automorphism, α, of order p if and only if $\mathfrak{G}$ can be imbedded as a maximal subgroup of a finite p-group of maximal class.

PROOF. Suppose that $\mathfrak{G}$ is α-concatenated, where $O(\alpha) = p$. Then $\mathfrak{G}$ is imbedded as a maximal subgroup of the semidirect product $\mathfrak{H} = \mathfrak{G}\langle\alpha\rangle$. From Theorem 1 we see that $\mathfrak{H}$ has class $n-1$ if $\mathfrak{G}$ has order p^{n-1}. Thus $\mathfrak{H}$ is a finite p-group of maximal class.

Suppose $\mathfrak{H}$ is a finite p-group of maximal class and order p^n. Let $\mathfrak{U}$ be a maximal subgroup of $\mathfrak{H}$. We have to show that $\mathfrak{U}$ is α-concatenated for some automorphism, α, of order p and may assume that $n \geqq 4$.

Put $\mathfrak{H}_i = \gamma_i(\mathfrak{H})$ for $i \geqq 2$ and $\mathfrak{H}_1 = C_{\mathfrak{H}}(\mathfrak{H}_2/\mathfrak{H}_4)$. It is well-known that

$$\mathfrak{H}_1 = C_{\mathfrak{H}}(\mathfrak{H}_i/\mathfrak{H}_{i+2}) \quad \text{for} \quad i = 2, \ldots, n-3;$$

this is also true for $i = n-2$ if $p = 2$ (see [4, p. 362]). Since $\mathfrak{H}$ has $p+1$ maximal subgroups we deduce the existence of a maximal subgroup, $\mathfrak{U}_1$, of $\mathfrak{H}$ such that $\mathfrak{U}_1$ is different from $\mathfrak{U}$ and from

$$C_{\mathfrak{H}}(\mathfrak{H}_i/\mathfrak{H}_{i+2}) \quad \text{for} \quad i = 2, \ldots, n-2.$$

If $\mathfrak{U} = \langle U, \mathfrak{H}_2\rangle$ and $\mathfrak{U}_1 = \langle U_1, \mathfrak{H}_2\rangle$, then $\mathfrak{H}$ is generated by U and U_1. Suppose that $S \in C_{\mathfrak{H}}(U_1) \cap \mathfrak{U}$ and write $S = U_1^a U^b X$ with $X \in \mathfrak{H}_2$. Then U_1 commutes with $U^b X$. Since $\mathfrak{H}$ is not abelian, we must have $b \equiv 0\,(p)$. Then $S = U_1^a Y$, where $Y \in \mathfrak{H}_2$. Since $S \in \mathfrak{U} \neq \mathfrak{U}_1$ we must have $a \equiv 0\,(p)$. Then $S \in \mathfrak{H}_2$. Since

$$U_1 \notin C_{\mathfrak{H}}(\mathfrak{H}_i/\mathfrak{H}_{i+2}) \quad \text{for} \quad i = 2, \ldots, n-2$$

we deduce $S \in \mathfrak{H}_{n-1} = Z(\mathfrak{H})$.

If α denotes the restriction to $\mathfrak{U}$ of the inner automorphism induced by U_1, then, consequently, α has exactly p fixpoints on $\mathfrak{U}$. Then $\mathfrak{U}$ is α-concatenated according to Theorem 2. Furthermore,

$$U_1^p \in C_{\mathfrak{H}}(U_1) \cap \mathfrak{H}_2 \leqq C_{\mathfrak{H}}(U_1) \cap \mathfrak{U} = Z(\mathfrak{H})$$

so α has order p.

Now we compute the structure of finite, abelian, concatenated p-groups. The purpose is to provide some simple examples that will display certain phenomena occuring quite generally.

THEOREM 4. *Let $\mathfrak{U}$ be a finite, abelian, concatenated p-group.*
Then $\mathfrak{U}$ has type

$$(\underbrace{p^{\mu+1},\ldots,p^{\mu+1}}_{s},\underbrace{p^{\mu},\ldots,p^{\mu}}_{d-s}) \quad \text{for some} \quad \mu\in\mathbf{N},\ s\geqq 0,\ d>s.$$

PROOF. Suppose that $\mathfrak{U}$ is α-concatenated. Let $\omega(\mathfrak{U}) = p^d$. Now, $\mathfrak{U}/\mathfrak{U}^p$ is α-concatenated so we deduce the existence of elements $A_1,\ldots,A_d\in\mathfrak{U}$ and $A\in\mathfrak{U}^p$ such that

$$A_i^\alpha = A_iA_{i+1} \quad \text{for} \quad i = 1,\ldots,d-1, \quad A_d^\alpha = A_dA \quad \text{and} \quad \mathfrak{U} = \langle A_1,\ldots,A_d\rangle.$$

If we put $p^{\mu_i} = O(A_i)$ we deduce $\mu_1 \geqq \ldots \geqq \mu_d$. Let $s\geqq 0$ and $\mu\in\mathbf{N}$ be determined by the conditions $\mu_1 = \ldots = \mu_s = \mu+1$ and $\mu_s > \mu_{s+1}$; if $\mu_1 = \ldots = \mu_d$ we put $s = 0$ and $\mu = \mu_1$.

If $s > 0$, then

$$(A_s^{p^{\mu_{s+1}}})^\alpha = A_s^{p^{\mu_{s+1}}} A_{s+1}^{p^{\mu_{s+1}}} = A_s^{p^{\mu_{s+1}}}$$

and so $\mu_s-\mu_{s+1} = 1$, since α has exactly p fixpoints on $\mathfrak{U}$. Then $\mu_{s+1} = \ldots = \mu_d$, since $A_1,\ldots,A_d$ are independent generators.

THEOREM 5. *For integers μ,s,d with $\mu,d\in\mathbf{N}$ and $d > s \geqq 0$, we consider the finite, abelian p-group*

$$\mathfrak{U}(p,\mu,s,d) = (\mathbf{Z}/\mathbf{Z}p^{\mu+1})^s\times(\mathbf{Z}/\mathbf{Z}p^{\mu})^{d-s}$$

with canonical basis $(A_1,\ldots,A_d)$ (so $O(A_i) = p^{\mu+1}$ for $i = 1,\ldots,s$ and $O(A_i) = p^\mu$ for $i > s$).

For any integers $b_1,\ldots,b_d$ with $b_1 \not\equiv 0\,(p)$ we define the endomorphism α in $\mathfrak{U}(p,\mu,s,d)$ by

$$A_i^\alpha = A_iA_{i+1} \ \textit{for} \ i = 1,\ldots,d-1 \quad \textit{and} \quad A_d^\alpha = A_dA,$$

where $A = A_1^{pb_1}\ldots A_d^{pb_d}$.

Then α is an automorphism of $\mathfrak{U}$ and $\mathfrak{U}$ is α-concatenated.

Put $A_i = [A_1,\underbrace{\alpha,\ldots,\alpha}_{i-1}]$ and $\mathfrak{U}_i = \langle A_j | j\geqq i\rangle$ for $i\in\mathbf{N}$.

Then the order of α is determined as follows:

Let $u\geqq 0$ be least possible such that $d\leqq p^u(p-1)$, $(u\in\mathbf{Z})$.

1°. *$d < p^u(p-1)$: If $d\mu+s \leqq p^u$, then $O(\alpha)$ is p^σ, where σ is least possible such that $p^\sigma \geqq d\mu+s$.*

Otherwise, $O(\alpha) = p^{u+k}$, where $k\geqq 1$ is least possible such that

$$k \geqq \frac{d\mu+s-p^u}{d}.$$

2°. $d = p^u(p-1)$: *Let* $r \in \{p^{u+1}, \ldots, d\mu+s\}$ *be least possible such that*

$$X = A_2^{\binom{p^{u+1}}{1}} \cdots A_{p^{u+1}-1}^{\binom{p^{u+1}}{p^{u+1}-2}} A_{p^{u+1}}^{\binom{p^{u+1}}{p^{u+1}-1}} A_{p^{u+1}+1} \in \mathfrak{U}_{r+1};$$

if $d\mu+s < p^{u+1}$, *we put* $r = d\mu+s$. *(Part of the statement is that such an* r *exists.)*

Then $O(\alpha) = p^{u+k+1}$, *where* $k \geqq 0$ *is least possible such that*

$$k \geqq \frac{d\mu+s-r}{d}.$$

PROOF. It is easily verified that α is an automorphisms of $\mathfrak{U}$, that α has exactly p fixpoints and that α has p-power order. So, $\mathfrak{U}$ is α-concatenated by Theorem 2.

By an easy inductional argument (on the parameter $d\mu+s$) we see that, for all i,

$$A_i^p \equiv A_{i+d}^a \bmod \mathfrak{U}_{i+d+1} \quad \text{for some } a \not\equiv 0\,(p).$$

By induction on k we get

$$A_i^{\alpha^k} = A_i A_{i+1}^{\binom{k}{1}} \cdots A_{i+k-1}^{\binom{k}{k-1}} A_{i+k} \quad \text{for all } i.$$

From this we see that

$$A_i^{\alpha^{p^\sigma}} \equiv A_i A_{i+p^\sigma} \bmod \mathfrak{U}_{i+p^\sigma+1} \quad \text{for all } i \text{ and all } \sigma \leqq u,$$

since $d > p^\sigma(p-1)$ for $\sigma < u$.

1°. $d < p^u(p-1)$: By an easy induction on $k \geqq 0$ we get

$$A_i^{\alpha^{p^{u+k}}} \equiv A_i A_{i+p^u+kd}^{b(k)} \bmod \mathfrak{U}_{i+p^u+kd+1}$$

where $b(k) \not\equiv 0\,(p)$. Here we have used the ineqaulity

$$(1-k(p-1))d < p^{u+1}-p^u.$$

2°. $d = p^u(p-1)$: With the same technique as in 1° we see that

$$X \in \mathfrak{U}_{p^{u+1}+1}.$$

If $r = d\mu+s$, then the statement is obviously true so we assume that $d\mu+s > p^{u+1}$ and $\mathfrak{U}_{r+1} \neq \{E\}$. Then we may write

$$A_1^{\alpha^{p^{u+1}}} \equiv A_1 A_{r+1}^b \bmod \mathfrak{U}_{r+2}$$

where $b \not\equiv 0\,(p)$. Letting $(\alpha-1)^{i-1}$ operate on this congruence we obtain

$$A_i^{\alpha^{p^{u+1}}} \equiv A_i A_{i+r}^b \bmod \mathfrak{U}_{i+r+1}.$$

Then using the inequality $r+kd < p(r+(k-1)d)$ for $k \geqq 1$ we get by induction on $k \geqq 1$

$$A_i^{\alpha p^{u+k}} \equiv A_i A_{i+r+(k-1)d}^{b(k)} \bmod \mathfrak{A}_{i+r+(k-1)d+1}$$

for all i with some $b(k) \not\equiv 0\,(p)$.

REMARK. In case 1° of Theorem 5 we see that the order of $\mathfrak{U}$ is bounded above by a function of p and $O(\alpha)$. This fact is easily seen to imply the existence of functions, $s(x,y)$ and $t(x,y)$, such that whenever $\mathfrak{G}$ is an α-concatenated p-group where $O(\alpha) = p^k$ then either $\mathfrak{G}_{s(p,k)}$ has order less than $t(p,k)$ or $\omega(\mathfrak{G}_{s(p,k)})$ has form $p^u(p-1)$.

It is thus clear that the concatenated p-groups, $\mathfrak{G}$, with $\omega(\mathfrak{G})$ of form $p^u(p-1)$ must play an important role in the study of the derived length of finite, concatenated p-groups. In the sequel we shall get another explanation of this fact.

2.

DEFINITION. Let $\mathfrak{G}$ be an α-concatenated p-group. For $t \geqq 0$ we say that $\mathfrak{G}$ has *degree of commutativity* t if and only if

$$[\mathfrak{G}_i, \mathfrak{G}_j] \leqq \mathfrak{G}_{i+j+t} \quad \text{for all } i,j \in \mathbb{N}.$$

In the proof of our main theorem, we shall show that if $\mathfrak{G}$ is a finite, concatenated p-group, then for sufficiently large s, $\mathfrak{G}_s$ has high degree of commutativity (in comparison with n if $|\mathfrak{G}_s| = p^n$).

In this connection it will be useful to single out a certain class of finite, concatenated p-groups having "straight" p-power structure.

DEFINITION. Suppose that $\mathfrak{G}$ is a finite, α-concatenated p-group with $\omega(\mathfrak{G}) = d$. We say that $\mathfrak{G}$ is *straight*, if and only if the following conditions are fulfilled:

1) $\mathfrak{G}_i^p = \mathfrak{G}_{i+d}$ for all $i \in \mathbb{N}$.
2) $X \in \mathfrak{G}_r$ and $C \in \mathfrak{G}_s$ implies $X^{-p}(XC)^p \equiv C^p \bmod \mathfrak{G}_{r+s+d}$ for all $r,s \in \mathbb{N}$.
3) If $G\mathfrak{G}_{i+1}$ is a generator of $\mathfrak{G}_i/\mathfrak{G}_{i+1}$, then $G^p\mathfrak{G}_{i+d+1}$ generates $\mathfrak{G}_{i+d}/\mathfrak{G}_{i+d+1}$.

We now give a criterion for straightness.

THEOREM 6. *Let $\mathfrak{G}$ be a finite, α-concatenated p-group with $\omega(\mathfrak{G}) = d$.*
If $\mathfrak{G}$ is regular or has degree of commutativity $\geqq (d+1)/(p-1)-1$, then $\mathfrak{G}$ is straight.

PROOF. For the theory of finite, regular p-groups the reader is refered to [3] or [4], pp. 321–335].

Let $|\mathfrak{G}| = p^{n-1}$. We prove the theorem by induction on n. Thus we may assume that $\mathfrak{G}_2$ is straight. Put $\omega(\mathfrak{G}_2) = d_1$. We may assume that $\mathfrak{G}$ does not have exponent p.

a) If $X \in \mathfrak{G}_r$ and $C \in \mathfrak{G}_s$, $r \leqq s$, then

$$X^{-p}(XC)^p \equiv C^p \mod \mathfrak{G}_{r+s}^p \mathfrak{G}_{r+s+d}.$$

If $\mathfrak{G}$ is regular then

$$X^{-p}(XC)^p \equiv C^p \mod \gamma_2(\langle X, C\rangle)^p$$

and generally we get, using the Hall-Petrescu formula (see [4, pp. 317–318]),

$$X^{-p}(XC)^p \equiv C^p \mod \gamma_2(\langle X, C\rangle)^p \gamma_p(\langle X, C\rangle).$$

Now, $\gamma_2(\langle X, C\rangle) \leqq \mathfrak{G}_{r+s}$ and if $\mathfrak{G}$ has degree of commutativity

$$t \geqq \frac{d+1}{p-1} - 1, \quad \text{then} \quad \gamma_p(\langle X, C\rangle) \leqq \mathfrak{G}_{s+(p-1)r+(p-1)t} \leqq \mathfrak{G}_{r+s+d}.$$

b) $d_1 \geqq d$: We may assume $\mathfrak{G}_{d+2} = \{E\}$ and have to prove $\mathfrak{G}_2^p = \{E\}$. Let $Y \in \mathfrak{G}_i$ for some $i \geqq 2$. According to Theorem 1 there exists $X \in \mathfrak{G}_{i-1}$ such that $[X, \alpha] = Y$. Since $X^p \in \mathfrak{G}_{d+1}$ (from now on we will use Corollary 1 without explicit reference) we have according to a)

$$E = [X^p, \alpha] = X^{-p}(X^\alpha)^p = X^{-p}(X[X, \alpha])^p \equiv [X, \alpha]^p = Y^p \mod \mathfrak{G}_{2i-1}^p \mathfrak{G}_{2i-1+d}.$$

Now, $\mathfrak{G}_{2i-1+d} = \{E\}$ and since certainly $d_1 \geqq d-1$, $\mathfrak{G}_{2i-1}^p = \{E\}$.

c) $\mathfrak{G}_i^p \leqq \mathfrak{G}_{i+d}$ for all $i \in \mathrm{N}$: This is clear from b) and the inductional hypothesis.

d) If $X \in \mathfrak{G}_r$ and $C \in \mathfrak{G}_s$, $r \leqq s$, then

$$X^{-p}(XC)^p \equiv C^p \mod \mathfrak{G}_{r+s+d}.$$

This is clear from a) and c).

e) $d_1 = d$: We may assume $\mathfrak{G}_{d+2} > \{E\}$. Choose $G \in \mathfrak{G}$ such that $G^p \notin \mathfrak{G}_{d+2}$. Then

$$[G^p, \alpha] = G^{-p}(G[G, \alpha])^p \equiv [G, \alpha]^p \mod \mathfrak{G}_{d+3}$$

because of d). Since $[G^p, \alpha] \notin \mathfrak{G}_{d+3}$, $[G, \alpha]^p \notin \mathfrak{G}_{d+3}$. Since $[G, \alpha] \in \mathfrak{G}_2$, this proves $d_1 \leqq d$.

f) If $G\mathfrak{G}_2$ generates $\mathfrak{G}_1/\mathfrak{G}_2$ and $X \in \mathfrak{G}$ we may write $X = G^a Y$ with $Y \in \mathfrak{G}_2$. Then

$$G^{-pa} X^p \equiv Y^p \equiv E \mod \mathfrak{G}_{d+2}.$$

Since $\mathfrak{G}^p = \mathfrak{G}_{d+1}$ we must have $G^p \notin \mathfrak{G}_{d+2}$. Then $G^p \mathfrak{G}_{d+2}$ generates $\mathfrak{G}_{d+1}/\mathfrak{G}_{d+2}$.

We shall be needing some information about $\omega(\mathfrak{G})$ in case $\mathfrak{G}$ is a concatenated p-group and in particular in case $\mathfrak{G}$ is a straight, concatenated p-group. First we need some lemmas.

LEMMA 1. *Let $i \in \mathbf{N}$. Suppose that $\sigma \in \{0, \ldots, 2^i - 1\}$. For $s \in \{1, \ldots, 2^i - 1\}$, we let $\mu_{\sigma,s}$ be the integer determined by the conditions*

$$\mu_{\sigma,s} + s \equiv \sigma\,(2^i) \quad \textit{and} \quad \mu_{\sigma,s} \in \{0, \ldots, 2^i - 1\}.$$

Then the integer

$$2\binom{2^i-1}{\sigma} + \sum_{s=1}^{2^i-1} \binom{2^i}{s}\binom{2^i-1}{\mu_{\sigma,s}}$$

is divisible by 4.

PROOF. We may clearly assume $i \geqq 2$. Suppose tnat $s \in \{1, \ldots, 2^i - 1\}$ and that $(2^i/s)$ is not divisible by 4. Now,

$$\binom{2^i}{s} = \binom{2^i-1}{s} + \binom{2^i-1}{s-1} = \binom{2^i-1}{s-1}\left(1 + \frac{2^i-s}{s}\right) = \binom{2^i-1}{s-1}\frac{2^i}{s},$$

so $2^{i-1}|s$ whence $s = 2^{i-1}$. Furthermore, the integer

$$\binom{2^i-1}{\sigma} + \binom{2^i-1}{2^{i-1}-1}\binom{2^i-1}{\mu_{\sigma,2^{i-1}}}$$

is even for the following reasons: We have

$$\binom{2^i-1}{\mu_{\sigma,2^{i-1}}} = \begin{cases} \binom{2^i-1}{\sigma-2^{i-1}} & \text{for } \sigma \geqq 2^{i-1} \\ \binom{2^i-1}{\sigma+2^{i-1}} & \text{for } \sigma < 2^{i-1} \end{cases}$$

and from the well-known facts concerning the 2-powers dividing $n!$ for $n \in \mathbf{N}$, we see that

$$\binom{2^i-1}{2^{i-1}-1}$$

is odd and that

$$\binom{2^i-1}{\mu_{\sigma,2^{i-1}}}$$

is divisible by exactly the same powers of 2 as is $(2^i - 1/\sigma)$ (use $\sigma \leqq 2^i - 1$).

LEMMA 2. *Let $\mathscr{F}$ be the free group on free generators X and Y. Let p be a* *prime number and let n be a natural number. Then,*

$$X^{p^n} Y^{p^n} = (XY)^{p^n} C C_p \dots C_{p^n},$$

where $C \in \gamma_2(\mathscr{F})^{p^n}$ *and* $C_{p^i} \in \gamma_{p^i}(\mathscr{F})^{p^{n-i}}$ *for* $i = 1, \dots, n$. *Each* C_{p^i} *has the form*

$$C_{p^i} \equiv [Y, \underbrace{X, \dots, X}_{p^i - 1}]^{a_i p^{n-i}} \prod V_\mu^{b_\mu p^{n-i}}$$

$$\bmod \gamma_{p^i+1}(\mathscr{F})^{p^{n-i}} \gamma_{p^{i+1}}(\mathscr{F})^{p^{n-i-1}} \dots \gamma_{p^n}(\mathscr{F}),$$

where each V_μ *has the form* $V_\mu = [Y, S_1, \dots, S_{p^i-1}]$ *with* $S_k \in \{X, Y\}$ *and* $S_k = Y$ *for at least one* k *(in each* V_μ*). Furthermore,* $a_i \equiv -1\ (p)$ *for* $i = 1, \dots, n$.

Proof. Let $i \in \{1, \dots, n\}$. If $U, V \in \gamma_{p^i}(\mathscr{F})$, then the Hall-Petrescu formula implies

$$(UV)^{p^{n-i}} \equiv U^{p^{n-i}} V^{p^{n-i}} \bmod \gamma_2(\langle U, V\rangle)^{p^{n-i}} \prod_{\mu=1}^{n-i} \gamma_{p^\mu}(\langle U, V\rangle)^{p^{n-i-\mu}}.$$

From this and from the standard, elementary facts concerning commutators the result follows immediately from the Hall-Petrescu formula, except for the fact that $a_i \equiv -1\ (p)$ for $i = 1, \dots, n$.

Consider the abelian p-group

$$\mathfrak{U} \text{ of type } (\underbrace{p^{n-i+1}, \dots, p^{n-i+1}}_{p^i})$$

with basis $A_1, \dots, A_{p^i}$ and let $\mathfrak{G}$ be the semidirect product $\mathfrak{G} = \mathfrak{U}\langle\alpha\rangle$, where α is the automorphism in $\mathfrak{U}$ given by

$$A_j^\alpha = A_{j+1},\ j = 1, \dots, p^i - 1, \quad \text{and} \quad A_{p^i}^\alpha = A_1.$$

Then α has order p^i. If $r, s \in \mathsf{N}$, $r \in \{1, \dots, p^i\}$, and $r \equiv s(p^i)$ we put $A_s = A_r$. Then for $r = 1, \dots, p^i$ we have

$$(+) \qquad [A_r, \underbrace{\alpha, \dots, \alpha}_{p^i-1}] = A_r^{(-1)^{p^i-1}} A_{r+1}^{(-1)^{p^i-2}\binom{p^i-1}{1}} \dots A_{r+p^i-1}$$

and

$$(++) \qquad [A_r, \underbrace{\alpha, \dots, \alpha}_{p^i}] = A_r^{1+(-1)^{p^i}} A_{r+1}^{(-1)^{p^i-1}\binom{p^i}{1}} \dots A_{r+p^i-1}^{(-1)\binom{p^i}{p^i-1}}.$$

Thus, $\gamma_{p^i+1}(\mathfrak{G}) \leqq \mathfrak{U}^p$. Using the same argument with A_r replaced by $A_r^{p^{s-1}}$ we deduce

$$\gamma_{sp^i+1}(\mathfrak{G}) \leqq \mathfrak{U}^{p^s} \quad \text{for} \quad s \in \mathsf{N}.$$

Since $sp^i + 1 \leqq p^{i+s-1}$ for $s \geqq 2$ except when $p = 2$ and $s = 2$, we conclude that

$$(+++) \qquad \gamma_{p^{i+s-1}}(\mathfrak{G})^{p^{n-(i+s-1)}} = \{E\} \quad \text{for } s \geqq 2$$

except possibly when $p = 2$ and $s = 2$.

If $p = 2$, we use $(+)$ and $(++)$ to conclude that

$$[A_r, \underbrace{\alpha, \ldots, \alpha}_{2^{i+1}-1}] = \prod_{\tau=0}^{2^i-1} A_{r+\tau}^{b(r,\tau)}$$

where

$$b(r,\tau) = (-1)^{\tau+1}\left(2\binom{2^i-1}{\tau} + \prod_{s=1}^{2^i-1}\binom{2^i}{s}\binom{2^i-1}{\mu_{\tau,s}}\right)$$

where

$$\mu_{\tau,s} \in \{0, \ldots, 2^i-1\} \quad \text{and} \quad \mu_{\tau,s}+s \equiv \tau\,(2^i).$$

Using Lemma 1, we then see that $(+++)$ is true also in the case $p = 2$ and $s = 2$.

Now we compute

$$X = (\alpha A_1)^{p^n} = (\alpha A_1 \alpha^{-1}) \ldots (\alpha^{p^n} A_1 \alpha^{-p^n})\alpha^{p^n} = (A_1 \ldots A_{p^i})^{p^{n-i}}.$$

Using the results obtained this far we get

$$E = \alpha^{p^n} A_1^{p^n} = X C_{p^i} = X[A_1, \underbrace{\alpha, \ldots, \alpha}_{p^i-1}]^{a_i p^{n-i}}$$

$$= ((A_1 \ldots A_{p^i})(A_1^{(-1)^{p^i-1}} A_2^{(-1)^{p^i-2}\binom{p^i-1}{1}} \ldots A_{p^i})^{a_i})^{p^{n-i}},$$

which gives $a_i \equiv -1\ (p)$.

THEOREM 7. *Suppose that $\mathfrak{G}$ is an α-concatenated p-group of order p^{n-1}, where $O(\alpha) = p^k$.*

If $\mathfrak{G}$ centralizes $\mathfrak{G}_i/\mathfrak{G}_{i+2}$ for $i = 1, \ldots, p^k$ and $n \geqq p^k+2$, then $\omega(\mathfrak{G}) = d \leqq p^k - 1$.

PROOF. The element αG_1 belonging to the semidirect product $\mathfrak{H} = \mathfrak{G}\langle\alpha\rangle$ has the property that $\alpha G_1 \notin C_{\mathfrak{H}}(\mathfrak{G}_i/\mathfrak{G}_{i+2})$ for $i = 2, \ldots, p^k$. Since $(\alpha G_1)^{p^k} \in \mathfrak{G}_2$, we must have

$$(\alpha G_1)^{p^k} \in \mathfrak{G}_{p^k+1}.$$

Now assume that $d \geqq p^k$. Then $\mathfrak{G}_1^p \leqq \mathfrak{G}_{p^k+1}$. From Lemma 2 we deduce (note that $\gamma_i(\mathfrak{H}) = \mathfrak{G}_i$ for $i \geqq 2$)

$$E \equiv \alpha^{p^k} G_1^{p^k} \equiv (\alpha G_1)^{p^k} C \equiv C \mod \mathfrak{G}_{p^k+1},$$

where C has the form

$$C \equiv [G_1, \alpha, \underset{p^k-1}{\ldots}, \alpha]^{-1} \prod_{\mu} V_{\mu}^{b_{\mu}} \bmod \mathfrak{G}_{p^k+1},$$

where each V_μ has the form $[G_1, X_1, \ldots, X_{p^k-1}]$, where $X_s \in \{\alpha, G_1\}$ and $X_s = G_1$ for at least one s (in each V_μ). Since $G_1 \in C_{\mathfrak{H}}(\mathfrak{G}_i/\mathfrak{G}_{i+2})$ for $i = 2, \ldots, p^k$, we deduce $V_\mu \in \mathfrak{G}_{p^k+1}$ for all μ. But then

$$C \equiv [G_1, \alpha, \underset{p^k-1}{\ldots}, \alpha]^{-1} \not\equiv E \bmod \mathfrak{G}_{p^k+1}$$

a contradiction.

Corollary 2. *Let $\mathfrak{G}$ be an α-concatenated p-group where $O(\alpha) = p^k$. Then $\mathfrak{G}_{1+(1+\ldots+p^{k-1})}$ is a straight, α-concatenated p-group.*

Proof. Put $s = 1+(1+\ldots+p^{k-1})$. According to Theorem 7, either $\mathfrak{G}_s$ has exponent p or $\omega(\mathfrak{G}_s) \leqq p^k - 1$. Using Theorem 6 and noting that $\mathfrak{G}_s$ has degree of commutatitivity $s-1$, the statement follows.

Theorem 8. *Let $\mathfrak{G}$ be an α-concatenated p-group of order p^{n-1}, where $O(\alpha) = p^k$. Suppose further that $\mathfrak{G}$ is straight, that $n \geqq p^k + 2$ and that $\mathfrak{G}$ centralizes $\mathfrak{G}_i/\mathfrak{G}_{i+2}$ for $i = 2, \ldots, p^k$.*
Then $\omega(\mathfrak{G}) = p^u(p-1)$ for some $u \in \{0, \ldots, k-1\}$.

Proof. We wish to perform certain calculations in the semidirect product $\mathfrak{G}\langle\alpha\rangle$. By the same argument as in the proof of Theorem 7 we see that the element αG_1 satisfies

$$(\alpha G_1)^{p^k} \in \mathfrak{G}_{p^k+1}.$$

Put $\omega(\mathfrak{G}) = d$. Assume that the minimum $\min\{p^i + (k-i)d \mid i = 0, \ldots, k\}$ is attained for exactly one value of i, say for $i = i_0 \in \{0, \ldots, k\}$. Put $s = p^{i_0} + (k - i_0)d$. Let

$$\alpha^{p^k} G_1^{p^k} = (\alpha G_1)^{p^k} C C_p \ldots C_{p^k},$$

where the C's have the form given in Lemma 2.

1°. $i_0 = 0$: Here we get $G_1^{p^k} \equiv E \bmod \mathfrak{G}_{s+1}$ contradiction.

2°. $i_0 > 0$: Here we get $E \equiv G_1^{p^k} \equiv C_{p^{i_0}} \bmod \mathfrak{G}_{s+1}$ and

$$C_{p^{i_0}} \equiv [G_1, \alpha, \underset{p^{i_0}-1}{\ldots}, \alpha]^{-p^{k-i_0}} \equiv G_{p^{i_0}}^{-p^{k-i_0}} \bmod \mathfrak{G}_{s+1}$$

and

$$G_{p^{i_0}}^{-p^{k-i_0}} \notin \mathfrak{G}_{s+1}$$

contradiction.

Consequently the minimum $\min\{p^i+(k-i)d \mid i = 0,\ldots,k\}$ is attained for two different values of i, say for $i = i_1$ and for $i = i_2$. Analysing the function $p^x+(k-x)d$ for $0 \leqq x \leqq k$ we deduce $|i_1-i_2| = 1$ whence, assuming $i_2 > i_1$, $d = p^{i_1}(p-1)$.

Our further investigations will concentrate on the analysis of certain invariants that will now be introduced.

Definition. Suppose that $\mathfrak{G}$ is an α-concatanated p-group and that $\mathfrak{G}$ has degree of commutativity t. Then we define the integers $a_{i,j}$ modulo p for $i,j \in \mathrm{N}$ thus:

$$[G_i, G_j] \equiv G_{i+j+t}^{a_{i,j}} \bmod \mathfrak{G}_{i+j+t+1}.$$

If $G_{i+j+t} = E$, we put $a_{i,j} = 0$.

We refer to the $a_{i,j}$ as the invariants of $\mathfrak{G}$ with respect to degree of commutativity t. (The $a_{i,j}$ depend on the choice of the G_i but choosing a different system of G_i's merely multiplies all the invariants with a certain constant incongruent to 0 modulo p.)

Theorem 9. *Let $\mathfrak{G}$ be a finite, α-concatenated p-group of order p^{n-1}. Suppose that $\mathfrak{G}$ has degree of commutativity t and let $a_{i,j}$ be the associated invariants.*

1) $a_{i,j}a_{k,i+j+t}+a_{j,k}a_{i,j+k+t}+a_{k,i}a_{j,k+i+t} \equiv 0(p)$ for $i+j+k+2t+1 \leqq n$.

2) $a_{i,j} \equiv a_{i+1,j}+a_{i,j+1}(p)$ for $i+j+t+2 \leqq n$.

3) If $i_0 \in \mathrm{N}$ then for $i,j \geqq i_0$

$$a_{i,j} \equiv \sum_{s=0}^{i-i_0} (-1)^s \binom{i-i_0}{s} a_{i_0,j+s}(p) \quad \text{for } i+j+t+1 \leqq n.$$

4) For $r \in \mathrm{N}$ we have

$$a_{i,i+r} \equiv \sum_{s=1}^{[(r+1)/2]} (-1)^{s-1} \binom{r-s}{s-1} a_{i+s-1,i+s}(p) \quad \text{for } 2i+r+t+1 \leqq n.$$

Proof. We shall make use of Witt's Identity:

$$(+) \qquad [A,B^{-1},C]^B[B,C^{-1},A]^C[C,A^{-1},B]^A = E$$

for elements A, B, and C in a group.

1) Considering $(+)$ modulo $\mathfrak{G}_{i+j+k+2t+1}$ with $A = G_i$, $B = G_j$, and $C = G_k$ gives us the congruence

$$G_{i+j+k+2t}^{-a_{i,j}a_{j+i+t,k}-a_{j,k}a_{j+k+t,i}-a_{k,i}a_{k+i+t,j}} \equiv E \text{ modulo } \mathfrak{G}_{i+j+k+2t+1}.$$

But if $i+j+k+2t+1 \leqq n$, then $G_{i+j+k+2t} \neq E$.

2) Considering $(+)$ modulo $\mathfrak{G}_{i+j+t+2}$ with $A = G_i$, $B = \alpha^{-1}$, and $C = G_j$ gives us the congruence

$$G_{i+j+t+1}^{-a_{i,j}+a_{i+1,j}+a_{i,j+1}} \equiv E \text{ modulo } \mathfrak{G}_{i+j+t+2}.$$

But if $i+j+t+2 \leqq n$, then $G_{i+j+t+1} \neq E$.

3) Using 2) this follows easily by induction on $i-i_0$.

4) Using 2) this follows easily by induction on r.

The purpose of the introduction of the idea of straight, concatenated p-groups will be clear from the next theorem.

THEOREM 10. *Let $\mathfrak{G}$ be an α-concatenated p-group of order p^{n-1}. Suppose that $\mathfrak{G}$ is straight with $\omega(\mathfrak{G}) = d$. Let $a_{i,j}$ be $\mathfrak{G}$'s invariants with respect to a given degree of commutativity t. Then for all i,j*

$$i+j+d+t+1 \leqq n \Rightarrow (a_{i,j} \equiv a_{i+d,j}(p)).$$

PROOF. If $\mathfrak{G}_{i+d} > \{E\}$, we have

$$G_i^p \equiv G_{i+d}^{b_i} \text{ mod } \mathfrak{G}_{i+d+1},$$

where $b_i \not\equiv 0(p)$.

Suppose that $i \in \mathrm{N}$ and $\mathfrak{G}_{i+d+1} > \{E\}$. Then $G_{i+1}^p = ([G_i, \alpha]Y)^p$ with $Y \in \mathfrak{G}_{i+2}$. Then

$$[G_i, \alpha]^{-p} G_{i+1}^p \equiv Y^p \text{ mod } \mathfrak{G}_{2i+3+d},$$

so

$$G_{i+d+1}^{b_{i+1}} \equiv G_{i+1}^p \equiv [G_i, \alpha]^p \equiv G_i^{-p}(G_i[G_i, \alpha])^p \equiv [G_i^p, \alpha] \equiv G_{i+d+1}^{b_i} \text{ mod } \mathfrak{G}_{i+d+2},$$

and since $G_{i+d+1} \neq E$, we deduce $b_{i+1} \equiv b_i(p)$.

Then if $i+j+d+t+1 \leqq n$ we get

$$G_{i+j+d+t}^{b_i a_{i+d,j}} \equiv [G_i^p, G_j] = G_i^{-p}(G_i[G_i, G_j])^p \equiv [G_i, G_j]^p \equiv G_{i+j+d+t}^{b_{i+j+t} a_{i,j}} \text{ mod } \mathfrak{G}_{i+j+d+t+1}$$

and $a_{i+d,j} \equiv a_{i,j}(p)$.

For straight, concatenated p-groups we have a stronger version of Theorem 9.

THEOREM 11. *Let $\mathfrak{G}$ be a straight, α-concatenated p-group of order p^{n-1} and with $\omega(\mathfrak{G}) = p^u(p-1)$. Suppose that $\mathfrak{G}$ has degree of commutativity t and let $a_{i,j}$ be the associated invariants. Suppose that $s \in \mathrm{N}$ is such that $s+t \equiv 0\,(p^u)$ and define $a_{i,j}^{(r)}$ for $r = 0, \ldots, u$ and $i,j \in \mathrm{Z}$ such that $s+ip^r, s+jp^r \geqq 1$ by*

$$a_{i,j}^{(r)} = a_{s+ip^r, s+jp^r}.$$

Put $t(r) = (s+t)p^{-r}$ for $r = 0, \ldots, u$.

Then for $r = 0, \ldots, u$, *we have the following congruences*:

1) $a^{(r)}_{i,j} a^{(r)}_{k,i+j+t(r)} + a^{(r)}_{j,k} a^{(r)}_{i,j+k+t(r)} + a^{(r)}_{k,i} a^{(r)}_{j,k+i+t(r)} \equiv 0(p)$

   for $3s + 2t + (i+j+k)p^r + 1 \leqq n$.

2) $a^{(r)}_{i,j+p^{u-r}(p-1)} \equiv a^{(r)}_{i,j}(p)$ *for* $2s + t + (i+j)p^r + p^u(p-1) + 1 \leqq n$.

3) $a^{(r)}_{i,j} \equiv a^{(r)}_{i+1,j} + a^{(r)}_{i,j+1}(p)$ *for* $2s + t + (i+j+1)p^r + 1 \leqq n$.

4) *If* $i_0 \in \mathrm{N}$ *then for* $i, j \geqq i_0$ *and* $2s + t + (i+j)p^r + 1 \leqq n$

$$a^{(r)}_{i,j} \equiv \sum_{h=0}^{i-i_0} (-1)^h \binom{i-i_0}{h} a^{(r)}_{i_0,j+h}(p).$$

5) *For* $v \in \mathrm{N}$ *and* $2s + (2i+v)p^r + t + 1 \leqq n$

$$a^{(r)}_{i,i+v} \equiv \sum_{h=1}^{[(v+1)/2]} (-1)^{h-1} \binom{v-h}{h-1} a^{(r)}_{i+h-1,i+h}(p).$$

PROOF 1): Using Theorem 9 this follows immediately from the definitions.
2): Using Theorem 10 this follows immediately from the definitions.
3): Let $r \in \{0, \ldots, u\}$ and let $i \in \mathrm{N}$. We state that

$$[G_i, \alpha^{p^r}] \equiv G_{i+p^r} \mod \mathfrak{G}_{i+p^r+1}.$$

To see this we write, in accordance with Lemma 2,

$$\alpha^{p^r}[\alpha^{p^r}, G_i] = (\alpha[\alpha, G_i])^{p^r} = \alpha^{p^r}[\alpha, G_i]^{p^r} C_{p^r} \ldots C_p C$$

where, with $\mathfrak{U} = \langle \alpha, [\alpha, G_i] \rangle$ (a subgroup of the semidirect product $\mathfrak{G}\langle\alpha\rangle$),

$$C \in \gamma_2(\mathfrak{U})^{p^r}, \ C_{p^\mu} \in \gamma_{p^\mu}(\mathfrak{U})^{p^{r-\mu}}, \quad \mu = 1, \ldots, r,$$

and

$$C_{p^r} \equiv [G_i, \underbrace{\alpha, \ldots, \alpha}_{p^r}]^{-1} \equiv G^{-1}_{i+p^r} \mod \mathfrak{G}_{i+p^r+1}.$$

Furthermore, since $r \leqq u$, we have

$$\mathfrak{G}^{p^r}_{i+1} \leqq \mathfrak{G}_{i+p^r+1} \quad \text{and} \quad \gamma_{p^\mu}(\mathfrak{U})^{p^{r-\mu}} \leqq \mathfrak{G}_{i+p^\mu+(r-\mu)d} \leqq \mathfrak{G}_{i+p^r+1}$$

for $\mu = 1, \ldots, r-1$.

Now suppose that $i, j \in \mathrm{Z}$ such that $s + ip^r$, $s + jp^r \geqq 1$ and $v = 2s + t + (i+j+1)p^r + 1 \leqq n$. Then considering Witt's Identity

$$[A, B^{-1}, C]^B [B, C^{-1}, A]^C [C, A^{-1}, B]^A = E$$

modulo $\mathfrak{G}_v$ with

$$A = G_{s+ip^r}, \quad B = \alpha^{-p^r}, \quad \text{and} \quad C = G_{s+jp^r}$$

and noting that $G_{v-1} \neq E$ the result follows.

4), 5): Using 3) these statements follows by easy inductions.

3.

We are now ready to prove the main theorems. First a simple lemma.

LEMMA 3. *Let n, t, and d be natural numbers. Suppose that we are given integers modulo p, $a_{i,j}$, defined for $i+j+t+1 \leqq n$. Suppose further that these integers satisfies the relations*

$$\begin{aligned} a_{i,j} &\equiv -a_{j,i}(p) && \text{for } i+j+t+1 \leqq n, \\ a_{i,i} &\equiv 0(p) && \text{for } 2i+t+1 \leqq n, \\ a_{i,j} &\equiv a_{i+1,j}+a_{i,j+1}(p) && \text{for } i+j+t+2 \leqq n \text{ and} \\ a_{i+d,j} &\equiv a_{i,j}(p) && \text{for } i+j+d+t+1 \leqq n. \end{aligned}$$

Then the existence of a natural number s such that $2s+d+t \leqq n$ and $a_{s+v,s+v+1} \equiv 0(p)$ for $v = 0, \ldots, [\frac{1}{2}d]-1$ implies $a_{i,j} \equiv 0(p)$ for all i,j.

PROOF. As in the proof of Theorem 9 we see that

$$(+) \qquad a_{i,i+r} \equiv \sum_{v=1}^{[(r+1)/2]} (-1)^{v-1} \binom{r-v}{v-1} a_{i+v-1,i+v}(p) \quad \text{if} \quad 2i+r+t+1 \leqq n$$

and

$$(++) \quad a_{i,j} \equiv \sum_{v=0}^{i-i_0} (-1)^v \binom{i-i_0}{v} a_{i_0,j+v}(p) \quad \text{if} \quad i+j+t+1 \leqq n \quad \text{and} \quad i,j \geqq i_0.$$

a) $a_{s,s+j} \equiv 0(p)$ for $j \geqq 0$ and $2s+j+t+1 \leqq n$: This is clear from $(+)$.

b) $a_{i,j} \equiv 0(p)$ for $i,j \geqq s$ and $i+j+t+1 \leqq n$: This is clear from $(++)$ and a).

c) Suppose that $\sigma \in \mathrm{N}$ and $a_{i,j} \equiv 0(p)$ if $i+j+t+1 \leqq n$ and $i,j > s-\sigma$. Then $2(s-\sigma)+d+t+2 \leqq n$ and so

$$a_{s-\sigma,s-\sigma+1} \equiv -a_{s-\sigma+1,s-\sigma+d} \equiv 0(p)$$

whence

$$a_{i,j} \equiv 0(p) \quad \text{if} \quad i+j+t+1 \leqq n \quad \text{and} \quad i,j \geqq s-\sigma.$$

THEOREM 12. *Let p be an odd prime number and let $\mathfrak{G}$ be a straight, concatenated p-group of order p^{n-1} and with $\omega(\mathfrak{G}) = p^u(p-1)$.*

1) *If* $n \geqq 4p^{u+1}-2p^u+1$, *then* $\mathfrak{G}$ *has degree of commutativity* $[\frac{1}{2}(n-4p^{u+1}+2p^u+1)]$.

2) *If* $n \geqq 4p^{u+1}-2p^u+1$, *then* $c(\mathfrak{G}) \leqq 2p^{u+1}-p^u$.

3) $c(\mathfrak{G}) \leqq 4p^{u+1}-2p^u-2$.

4) *If* $n \geqq 12p^{u+1}-6p^u-10$, *then* $c(\mathfrak{G}) \leqq 3$.

PROOF. 1): Assume $n \geqq 4p^{u+1}-2p^u+1$. Suppose that $\mathfrak{G}$ has degree of commutativity t, where $t \leqq \frac{1}{2}(n-4p^{u+1}+2p^u-1)$. Let $a_{i,j}$ be the associated invariants. We must show that $a_{i,j} \equiv 0(p)$ for all i,j.

Let $i_0 \in \{1,\ldots,p^u(p-1)\}$ be determined by the condition $i_0+t \equiv 0(p^u(p-1))$. For $r = 0,\ldots,u$ and $i,j \in \mathbf{Z}$ such that $i_0+ip^r, i_0+jp^r \geqq 1$, we let $a_{i,j}^{(r)}$ be the integers (modulo p) introduced in Theorem 11 (with $i_0 = s$).

We show by induction on $u-r$ that if $r \in \{0,\ldots,u\}$ then $a_{i,j}^{(r)} \equiv 0(p)$ for all i,j. So we suppose that $r \in \{0,\ldots,u\}$ is given and that $a_{i,j}^{(\varrho)} \equiv 0(p)$ for all i,j whenever $\varrho \in \{0,\ldots,u\}$ and $\varrho > r$. Write $a_\mu^{(\varrho)}$ for $a_{\mu,\mu+1}^{(\varrho)}$ for brevity. In what follows we shall make use of Theorem 11 and Lemma 3 without explicit reference.

We have the congruence

$$(+) \qquad a_{i,j}^{(r)}a_{k,i+j}^{(r)}+a_{j,k}^{(r)}a_{i,j+k}^{(r)}+a_{k,i}^{(r)}a_{j,k+i}^{(r)} \equiv 0(p)$$

when $3i_0+2t+(i+j+k)p^r+1 \leqq n$.

So, we may substitute $(i,j,k) = (1,2,2s-1)$ for $2 \leqq s \leqq \frac{1}{2}(p-1)$ in $(+)$. Given $s \in \{1,\ldots,\frac{1}{2}(p-1)\}$ and having proved $a_\sigma^{(r)} \equiv 0(p)$ for $2 \leqq \sigma < s$ this gives us the congruence $s(a_s^{(r)})^2 \equiv 0(p)$.

So, $a_s^{(r)} \equiv 0(p)$ for $s = 2,\ldots,\frac{1}{2}(p-1)$. This gives us

$$a_{0,p}^{(r)} \equiv a_0^{(r)}+2a_1^{(r)}(p),$$

since $2i_0+t+p^{u+1}+1 \leqq n$.

If $r = u$, then $a_{0,p}^{(r)} \equiv a_0^{(r)}(p)$ and we deduce $a_s^{(r)} \equiv 0(p)$ for $s = 1,\ldots,\frac{1}{2}(p-1)$ and so $a_{i,j}^{(r)} \equiv 0(p)$ for all i,j.

So we assume that r $< u$. Then $a_{0,p}^{(r)} \equiv a_{0,1}^{(r+1)} \equiv 0(p)$. Now, the substitution $(i,j,k) = (0,1,3)$ in $(+)$ gives

$$a_1^{(r)}(a_1^{(r)}+a_0^{(r)}) \equiv 0(p).$$

So, if $a_1^{(r)} \not\equiv 0(p)$ we would deduce $a_1^{(r)} \equiv 0(p)$. Hence, $a_1^{(r)} \equiv 0(p)$ and so $a_0^{(r)} \equiv 0(p)$.

Now we substitute $(i,j,k) = (0,1,2s)$ in $(+)$ for $s = 1,\ldots,\frac{1}{2}p^{u-r}(p-1)-1$. Given $s \in \{1,\ldots,\frac{1}{2}p^{u-r}(p-1)-1\}$ and having $a_\sigma^{(r)} \equiv 0(p)$ for $1 \leqq {}^\sigma < s$ this gives us the congruence

$$(-1)^{s+1}\binom{(2s-1)-s}{s-1}(-1)^s\binom{(2s+1)-(s+1)}{s}(a_s^{(r)})^2 \equiv 0(p).$$

Hence, $a_s^{(r)} \equiv 0(p)$ for $s = 0,\dots,\frac{1}{2}p^{u-r}(p-1)-1$. Note that

$$2i_0+t+p^r(p^{u-r}(p-1)-1)+1 \leqq n.$$

2) Put $f(u) = 4p^{u+1}-2p^u-1$. If $n \geqq 4p^{u+1}-2p^u+1$ and n is odd, then $\mathfrak{G}$ has degree of commutativity $\frac{1}{2}(n-f(u))$. Then

$$\gamma_k(\mathfrak{G}) = \{E\} \quad \text{if} \quad k \geqq \frac{3n-f(u)-2}{n-f(u)+2}.$$

However,

$$\frac{3n-f(u)-2}{n-f(u)+2} \leqq 1+\tfrac{1}{2}(f(u)+1) = 1+(2p^{u+1}-p^u),$$

when $n \geqq f(u)+2$.

If $n \geqq 4p^{u+1}-2p^u+2$ and n is even, then we see in a similar way that $\gamma_k(\mathfrak{G}) = \{E\}$ with $k = 2p^{u+1}-p^u+1$.

3) If $n \leqq 4p^{u+1}-2p^u$, then $c(\mathfrak{G}) \leqq 4p^{u+1}-2p^u-2$. Since

$$4p^{u+1}-2p^u-2 \geqq 2p^{u+1}-p^u$$

the statement follows from 2).

4) If $n \geqq 4p^{u+1}-2p^u+1$ and

$$4 \geqq \frac{3n-f(u)-3}{n-f(u)+1} \quad \text{with} \quad f(u) = 4p^{u+1}-2p^u-1,$$

then $c(\mathfrak{G}) \leqq 3$. But the second inequality holds for $n \geqq 12p^{u+1}-6p^u-10$ and it is clear that

$$12p^{u+1}-6p^u-10 \geqq 4p^{u+1}-2p^u+1.$$

COROLLARY 3. *There exist functions of two variables, $u(x,y)$ and $v(x,y)$, such that whenever p is an odd prime number, k is a natural number and $\mathfrak{G}$ is a finite p-group possessing an automorphism of order p^k having exactly p fixpoints, then $\mathfrak{G}$ possesses a normal subgroup of index less than $u(p,k)$ having class less than $v(p,k)$.*

Thus there exists a function of two variables, $f(x,y)$, such that whenever p is an odd prime number, k is a natural number and $\mathfrak{G}$ is a finite p-group possessing an automorphism of order p^k having exactly p fixpoints, then the derived length of $\mathfrak{G}$ is less than $f(p,k)$.

PROOF. The first statement follows immediately from Theorem 6, Theorem 7, Theorem 8, and Theorem 12. The second statement follows trivially from the first.

REFERENCES

1. J. L. Alperin, *Automorphisms of solvable groups*, Proc. Amer. Math. Soc. 13 (1962), 175–180.
2. N. Blackburn, *On a special class of p-groups*, Acta Math. 100 (1958), 45–92.
3. P. Hall, *A contribution to the theory of groups of prime power orders*, Proc. London Math. Soc. 36 (1933), 29–95.
4. B. Huppert, *Endliche Gruppen* I (Grundlehren Math. Wiss. 134), Springer-Verlag, Berlin - Heidelberg - New York, 1967.
5. C. R. Leedham-Green and S. McKay, *On p-groups of maximal class* I, Quart. J. Math. Oxford Ser. (2) 27 (1976), 297–311.

MATEMATISK INSTITUT
KØBENHAVNS UNIVERSITET
UNIVERSITETSPARKEN 5
2100 KØBENHAVN Ø
DENMARK