MATH. SCAND. 76 (1995), 35–49

# SOME REMARKS ON A CERTAIN CLASS OF FINITE $p$-GROUPS

IAN KIMING

**Abstract.**

First we extend the main result of our previous article [3] concerning finite $p$-groups possessing an automorphism of $p$-power order and with exactly $p$ fixed points, to the case $p = 2$. Secondly, we use our techniques to prove a generalisation of certain classical results of Blackburn concerning "exceptionality" in finite $p$-groups of maximal class.

## 1. Introduction.

In this article the symbol $p$ always denotes a prime number and "$p$-group" means "finite $p$-group".

The following theorem is the main result in [3].

THEOREM A (Corollary 3 in [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 $G$ is a finite $p$-group possessing an automorphism of order $p^k$ having exactly $p$ fixed points, then $G$ possesses a normal subgroup of index less than $u(p, k)$ having class less than $v(p, k)$.*

Theorem A can be seen as a generalisation of the fact proved in [4] that the derived length of a $p$-group of maximal class is bounded above by a function depending only on $p$. For the theory of finite $p$-groups of maximal class the reader is referred to [1] or [2], III, § 14.

In section 2 below we prove that the prime number $p = 2$ does not have to be excluded in theorem A.

In section 3 we use our techniques to prove a theorem which can be viewed as a generalisation of a theorem of Blackburn concerning "exceptional" $p$-groups of maximal class: Blackburn proved that if $G$ is an exceptional $p$-group of maximal class and order $p^n$ then $6 \leqq n \leqq p + 1$ and $n$ is even; see for example [2], III,

Received December 6, 1993.

Hauptsatz 14.6. Having proved our theorem we shall point out the connection to this result of Blackburn.

We shall use the following notation: Let $G$ be a $p$-group. If $x, y \in G$ we write

$$x^y = y^{-1}xy \quad \text{and} \quad [x, y] = x^{-1}y^{-1}xy.$$

If $x \in G$ and $\alpha$ is an automorphism of $G$, we write $x^\alpha$ for the image of $x$ under $\alpha$.

The terms of the lower central series of $G$ are written $\gamma_i(G)$ for $i \in \mathbf{N}$.

If $|G/G^p| = p^d$, we write $\omega(G) = d$.

A central series

$$G = G_1 \geq G_2 \geq \ldots \geq G_s \geq \ldots$$

is called *strongly central* if $[G_i, G_j] \leq G_{i+j}$ for all $i,j$.

The letter $e$ always denotes the neutral element in a given group.

We shall now recall some definitions and results from [3] which will be needed in the sequel.

DEFINITION. Let $G$ be a $p$-group. We say that $G$ is *concatenated* if $G$ possesses an automorphism $\alpha$, a strongly central series

$$G = G_1 \geq \ldots \geq G_{n+1} = e = G_{n+2} = \ldots$$

(for some $n \in \mathbf{N}$) and elements $g_i \in G_i$ for $i = 1, \ldots, n+1$ such that the following holds:

(1) $|G_i/G_{i+1}| = p$ for $i = 1, \ldots, n$,

(2) $G_i/G_{i+1}$ is generated by $g_i G_{i+1}$ for $i = 1, \ldots, n+1$,

(3) $[g_i, \alpha] := g_i^{-1} g_i^\alpha \equiv g_{i+1} \bmod G_{i+2}$ for $i = 1, \ldots, n$.

In this situation we shall also say that $G$ is $\alpha$-concatenated. Thus, when we say that $G$ is $\alpha$-concatenated we mean that $G$ possesses an automorphism $\alpha$, a strongly central series

$$(+) \qquad G_1 \geq G_2 \geq \ldots \geq G_s \geq \ldots$$

and elements $g_i \in G_i$ such that the conditions of the above definitions are fullfilled. Obviously then, $\alpha$ have $p$-power order and $(+)$ is completely determined by $G$ and $\alpha$. The symbols $G_i$ will then always refer to the terms of this strongly central series. When $G$ is $\alpha$-concatenated we shall also assume that the elements $g_i$ have been chosen, and the symbols $g_i$ will then always refer to these fixed choices.

The relevance of the above definition for our purposes is the fact that if $G$ is a $p$-group and $\alpha$ an automorphism of $p$-power order of $G$, then $G$ is $\alpha$-concatenated if and only if $\alpha$ has exactly $p$ fixed points in $G$; cf. Theorem 2 in [3].

DEFINITION. Suppose that $G$ is an $\alpha$-concatenated $p$-group. Let $t$ be a non-negative integer. We say that $G$ has *degree of commutativity* $t$ if

$$[G_i, G_j] \leqq G_{i+j+t} \quad \text{for all} \quad i,j \in \mathbf{N}.$$

Thus, $G$ has in any case degree of commutativity 0.

If $G$ has degree of commutativity $t$ and order $p^n$, then we introduce certain invariants associated with this degree of commutativity. The invariants $a_{i,j}$ for $i,j \in \mathbf{N}$ are integers defined modulo $p$ by the following requirements:

$$[g_i, g_j] \equiv g_{i+j+t}^{a_{i,j}} \bmod G_{i+j+t+1} \quad \text{for} \quad i+j+t \leqq n$$

and

$$a_{i,j} \equiv 0 \quad (p) \quad \text{for} \quad i+j+t \geqq n+1.$$

Thus, if $G$ has degree of commutativity $t$ and if the associated invariants are all congruent to 0 modulo $p$, then $G$ has degree of commutativity $t+1$.

THEOREM B (Theorem 9 in [3]). *Let $G$ be an $\alpha$-concatenated $p$-group of order $p^n$. Suppose that $G$ has degree of commutativity $t$ and let $a_{i,j}$ for $i,j \in \mathbf{N}$ be the associated invariants. Then the following holds:*

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

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

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

(4) *For $r \in \mathbf{N}$ we have:*

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

DEFINITION. Suppose that $G$ is a ($\alpha$)-concatenated $p$-group with $\omega(G) = d$. We say that $G$ is *straight* if the following conditions are fulfilled.

(1) $G_i^p = G_{i+d}$ for all $i \in \mathbf{N}$.

(2) $x \in G_r$ and $c \in G_s$ implies

$$x^{-p}(xc)^p \equiv c^p \bmod G_{r+s+d} \quad \text{for all} \quad r,s \in \mathbf{N}.$$

(3) If $gG_{i+1}$ is a generator of $G_i/G_{i+1}$ then $g^pG_{i+d+1}$ is a generator of $G_{i+d}/G_{i+d+1}$.

THEOREM C (Theorem 10 in [3]). *Let $G$ be a concatenated $p$-group of order $p^n$. Suppose that $G$ is straight with $\omega(G) = d$. Suppose further that $G$ has degree of commutativity $t$ and let $a_{i,j}$ be the associated invariants. Then we have for all $i,j$*

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

THEOREM D (Corollary 2 in [3]). *Let $G$ be an $\alpha$-concatenated $p$-group with $\alpha$ of order $p^k$. Put*

$$s = 1 + (1 + p + \ldots + p^{k-1}).$$

*Then $G_s$ is a straight, $\alpha$-concatenated $p$-group.*

Finally we shall need the following technical lemma, which is a refinement of the Hall-Petrescu formula (cf. [2], III, Satz 9.4, Hilfsatz 9.5).

LEMMA E (Lemma 2 in [3]). *Let $F$ be the free group on free generators $x$ and $y$. Let $p$ be a prime number and $n$ a natural number. Then we have*

$$x^{p^n} y^{p^n} = (xy)^{p^n} c c_p \ldots c_{p^n},$$

*with certain elements*

$$c \in \gamma_2(F)^{p^n} \quad \text{and} \quad c_{p^i} \in \gamma_{p^i}(F)^{p^{n-i}}$$

*for $i = 1, \ldots, n$, where each $c_{p^i}$ has the form*

$$c_{p^i} \equiv [y, \underbrace{x, \ldots, x}_{p^i - 1}]^{a_i p^{n-i}} \prod_{\mu} v_\mu^{b_\mu p^{n-i}}$$

*modulo*

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

*for certain integers $a_i$ and $b_\mu$, and where each $v_\mu$ has the form*

$$v_\mu = [y, s_1, \ldots, s_{p^i - 1}]$$

*with $s_k \in \{x, y\}$ and $s_k = y$ for at least one $k$ in each $v_\mu$. Furthermore,*

$$a_i \equiv -1 (p) \quad \text{for} \quad i = 1, \ldots, n.$$

## 2.

In this section we shall prove the extension of theorem A to the case $p = 2$. First we need a result which will also be usefull in the next section.

PROPOSITION 1. *Let $G$ be an $\alpha$-concatenated straight $p$-group of order $p^n$ with $\alpha$ of order $p^k$. Let $d = \omega(G)$, and let $a_{i,j}$ for $i, j \in \mathbf{N}$ denote $G$'s invariants with respect to degree of commutativity 0. Then the following holds.*

(1) *If $n \geqq 1 + p^k$ then $d$ has the form*

$$d = p^r(p - 1) \quad \text{for some} \quad r \in \{0, \ldots, k - 1\}.$$

(2) *Suppose that $s$ is a non-negative integer such that $d > p^s(p - 1)$. Define*

$$a_{i,j}^{(v)} = a_{ip^v, jp^v}$$

*for* $v = 1, \ldots, s+1$ *and* $i, j \in \mathbf{N}$. *Then*

$$a_{i,j}^{(v)} \equiv a_{i+1,j}^{(v)} + a_{i,j+1}^{(v)} (p),$$

*for* $v = 1, \ldots, s+1$ *and all* $i, j \in \mathbf{N}$ *such that* $p^v(i+j+1) \leqq n$.

PROOF. Let $i \in \mathbf{N}$. Using Lemma E for computation in the semi-direct product $G\langle\alpha\rangle$, we see that

$$(++) \qquad \alpha^{p^v}[\alpha^{p^v}, g_i] = (\alpha[\alpha, g_i])^{p^v} = \alpha^{p^v}[\alpha, g_i]^{p^v} c_{p^v}^{-1} \ldots c_p^{-1} c^{-1},$$

for given $v \in \mathbf{N}$, where putting $U = \langle \alpha, [\alpha, g_i] \rangle$ we have

$$[\alpha, g_i]^{p^v} \in G_{i+1+vd},$$

$$c \in \gamma_2(U)^{p^v} \leq G_{i+2+vd},$$

$$c_{p^\mu} \in \gamma_{p^\mu}(U)^{p^{v-\mu}} \leq G_{i+p^\mu+(v-\mu)d}$$

for $\mu = 1, \ldots, v$, and where $c_p, \ldots, c_{p^v}$ have the forms given in Lemma E.

Proof of (1): Suppose that $n \geqq 1 + p^k$ and let

$$m = \min\{p^\mu + (k-\mu)d \mid \mu = 0, \ldots, k\}.$$

Let $v \in \{0, \ldots, k\}$ be such that

$$m = p^v + (k-v)d,$$

and suppose that $v$ is *unique* with this property in $\{0, \ldots, k\}$. Using $(++)$ for $v = k$ we see that

$$e = [\alpha^{p^k}, g_1] \equiv g_2^{-p^k} \bmod G_{m+2} \quad \text{if} \quad v = 0,$$

and

$$e \equiv c_{p^v} \bmod G_{m+2} \quad \text{if} \quad v > 0.$$

In the first case we deduce $2 + kd \geqq n + 1 \geqq 2 + p^k$ and so

$$m = 1 + kd \geqq 1 + p^k > p^k,$$

which is impossible. In the case $v > 0$ we note that $c_{p^v}$ according to Lemma E satisfies

$$c_{p^v} \equiv [g_1, \underbrace{\alpha, \ldots, \alpha}_{p^v}]^{-p^{k-v}} \equiv g_{1+p^v}^{-p^{k-v}} \bmod G_{m+2}.$$

From this we deduce that $1 + p^v + (k-v)d \geqq n + 1 \geqq 2 + p^k$, and so

$$m = p^v + (k-v)d \geqq 1 + p^k > p^k,$$

which is impossible. Consequently, there exist two different numbers $\mu$, $\nu$ in $\{0,\dots,k\}$ such that

$$m = p^{\mu} + (k-\mu)d = p^{\nu} + (k-\nu)d.$$

Since $m$ is minimal, we then easily see that $|\mu - \nu| = 1$, and so $d$ has the form $p^r(p-1)$ with $r \in \{0,\dots,k-1\}$.

Proof of (2): Suppose that $s$ is a non-negative integer with $d > p^s(p-1)$, and let $v \in \mathbf{N}$ be such that $1 \leqq v \leqq s+1$. Then

$$p^{\mu-1} + (v-\mu+1)d > p^{\mu} + (v-\mu)d \quad \text{for} \quad \mu = 1,\dots,v,$$

and from $(++)$ we conclude that

$$[\alpha^{p^v}, g_i] \equiv c_{p^v}^{-1} \bmod G_{i+1+p^v} \quad \text{for} \quad i \in \mathbf{N},$$

since

$$p^s(p-1) + 1 \geqq \frac{1}{s+1} p^{s+1} \quad \text{for} \quad s \geqq 0.$$

According to Lemma E we have

$$c_{p^v}^{-1} \equiv [[\alpha, g_i], \underbrace{\alpha,\dots,\alpha}_{p^v-1}] \equiv [g_i, \underbrace{\alpha,\dots,\alpha}_{p^v}]^{-1} \equiv g_{i+p^v}^{-1} \bmod G_{i+1+p^v},$$

and so

$$(+++) \qquad [g_i, \alpha^{p^v}] \equiv g_{i+p^v} \bmod G_{i+p^v+1} \quad \text{for} \quad i \in \mathbf{N}.$$

Now suppose that $i, j \in \mathbf{N}$ are such that $p^v(i+j+1) \leqq n$, and put

$$m = p^v(i+j+1) + 1.$$

Consider Witt's identity

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

modulo $G_m$ with

$$A = g_{ip^v}, \; B = a^{-p^v} \quad \text{and} \quad C = g_{jp^v}.$$

Using $(+++)$ and noting that $g_{m-1} \neq e$, it then follows that:

$$a_{i,j}^{(v)} \equiv a_{i+1,j}^{(v)} + a_{i,j+1}^{(v)} \; (p)$$

THEOREM 1. *Let $G$ be a concatenated, straight 2-group of order $2^n$ and with $\omega(G) = 2^k$. Put $d = 2^k$.*

*Then $G$ is metabelian, and if $n \geqq 2d$ then $G$ has degree of commutativity $n - 2d$.*

PROOF. If $d = 1$ then $|G/G^2| = 2$, and so $G$ is cyclic. But then the statements of the theorem are clear. So, we assume that $k > 0$.

We now suppose that $n \geqq 2d$ and will show that $G$ has degree of commutativity $n - 2d$. If $n = 2d$ this is obviously the case, so we assume that $n > 2d$ and that $G$ has degree of commutativity $t$ with $t \leqq n - 2d - 1$. Let $a_{i,j}$ be the associated invariants.

For $s = 1, \ldots, \frac{1}{2}d$ we have $2s + d + t + 1 \leqq n$, and using Theorem B and Theorem C we then find modulo 2

$$(2) \qquad a_{s,s+1} \equiv a_{s,s+d+1} \equiv \sum_{h=1}^{\frac{1}{2}d+1} (-1)^{h-1} \binom{d+1-h}{h-1} a_{s+h-1,s+h}$$

$$\equiv \sum_{h=0}^{\frac{1}{2}d} (-1)^h \binom{d-h}{h} a_{s+h,s+h+1}$$

and

$$(2) \qquad a_{s+1,s} \equiv a_{s+1,s+1+(d-1)} \equiv \sum_{h=1}^{\frac{1}{2}d} (-1)^{h-1} \binom{d-h-1}{h-1} a_{s+h,s+h+1}.$$

Now, for $h = 1, \ldots, \frac{1}{2}d$ we have

$$\binom{d-h}{h} = \binom{d-h-1}{h-1} \frac{d-h}{h},$$

and since $d$ is a power of 2 and $h \leqq \frac{1}{2}d$, we see that $\binom{d-h}{h}$ and $\binom{d-h-1}{h-1}$ have the same parity. Using Theorem B (1) we then conclude that

$$0 \equiv a_{s,s+1} + a_{s+1,s} \equiv a_{s,s+1} + \sum_{h=1}^{\frac{1}{2}d} \left( \binom{d-h}{h} + \binom{d-h-1}{h-1} \right) a_{s+h,s+h+1}$$

$$\equiv a_{s,s+1} \qquad (2)$$

for $s = 1, \ldots, \frac{1}{2}d$. Then Theorem B (4) shows that

$$a_{1,1+r} \equiv 0 \quad (2) \quad \text{for} \quad r = 0, \ldots, d.$$

Hence Theorem C gives

$$a_{1,j} \equiv 0 \quad (2) \quad \text{for all} \quad j.$$

Using this and Theorem B (3) we easily see by induction on $i$ that

$$a_{i,j} \equiv 0 \quad (2) \quad \text{for all } i,j.$$

Consequently, $G$ has degree of commutativity $t + 1$.

So, $G$ has degree of commutativity $n - 2d$.

The group $G/G_{1+d}$ has exponent 2, hence is abelian. If $n \leqq 2d$ the same holds for the group $G_{1+d}$. If $n \geqq 2d$ then $G_{1+d}$ is abelian since $G$ has then degree of commutativity $n - 2d$. Thus, $G$ is metabelian in any case.

THEOREM 2. *Let $G$ be an $\alpha$-concatenated, straight 2-group of order $2^n$ with $\alpha$ of order $2^k$. Then the following holds.*
(1) *If $n \geqq 1 + 2^k$ then $G$ has class at the most $2^{k-1}$.*
(2) *If $n \geqq 2^{k+1} - 3$ then $G$ has class at the most 2.*
(3) *$G$ has class at the most $2^k - 1$.*

PROOF. Let $d = \omega(G)$. If $n \geqq 1 + 2^k$ then according to Proposition 1, $d$ has the form $d = 2^r$ for some $r \in \{0, \ldots, k-1\}$. Hence, if $k = 1$ and $n \geqq 3$ then $G$ is cyclic. If $n \leqq 2$ then $G$ is abelian. We may consequently assume that $k \geqq 2$.

Suppose that $n \geqq 1 + 2^k$. According to Theorem 1, $G$ has then degree of commutativity $t = n - 2d$. Now, it is easily seen by induction on $i$ that if $i \in \mathbf{N}$ and $i \geqq 2$ then

$$\gamma_i(G) \leqq G_{i+1+(i-1)t}.$$

So, $\gamma_i(G) = \{e\}$ if

$$(+) \qquad i \geqq \frac{2n - 2d}{n - 2d + 1}.$$

Using $n \geqq 1 + 2^k$ and $d = 2^r$ with $r \in \{0, \ldots, k-1\}$, an easy calculation shows ithat $(+)$ is satisfied if $i \geqq 1 + 2^{k-1}$. $(+)$ is also satisfied if $i \geqq 3$, provided that $n \geqq 2^{k+1} - 3$ (note that then $n \geqq 2^{k+1} - 3 \geqq 2^k + 1$, since $k \geqq 2$, whence $d \leqq 2^{k-1}$). This proves (1) and (2).

Finally, (3) follows from (1) because $G$ obviously has class a the most $2^k - 1$ if $n \leqq 2^k$.

Our extension of Theorem A to the case $p = 2$ now follows immediately from Theorem D and Theorem 2: If $G$ is an $\alpha$-concatenated 2-group with $\alpha$ of order $2^k$, then the normal subgroup

$$G_{1+(1+2+\ldots+2^{k-1})}$$

has index at the most

$$2^{1+2+\ldots+2^{k-1}},$$

and has class at the most $2^k - 1$.

## 3.

We now turn our attention to our second objective described in the introduction. In what follows, $p$ will denote an *odd* prime number. The content of the main

result of this section, which is Theorem 3 below, is roughly speaking that if $G$ is an $\alpha$-concatenated, straight $p$-group of order $p^n$ with $\alpha$ of order $p^k$, if $a_{i,j}$ are the invariants associated with degree of commutativity 0, and if $a_{i,j}$ is congruent to 0 modulo $p$ whenever $i+j$ is less that a certain number, which is "small" compared with $p^k$, then $a_{i,j}$ can be incongruent to 0 modulo $p$ only if $i+j$ is "big" compared with $\min\{n, \omega(G)\}$. Furthermore, $G$ has degree of commutativity 1, if $n$ is sufficiently large compared with $p^k$.

This result will be a consequence of the following two propositions.

PROPOSITION 2. *Let $p$ be an odd prime number and let $n$, $r$ and $r_0$ be natural numbers. Assume that $3 \leqq r \leqq n-1$. Suppose that we are given integers $a_{i,j}$ for $i,j \in \mathbf{N}$ with $i+j \leqq n$. Suppose further that the following conditions are satisfied.*

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

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

(3) $a_{i,j}a_{k,i+j} + a_{j,k}a_{i,j+k} + a_{k,i}a_{j,k+i} \equiv 0 \quad (p) \quad for \quad i+j+k \leqq n.$

(4) $a_{i,j} \equiv 0 \quad (p) \quad for \quad i+j \leqq r.$

(5) $a_{pi,pj} \equiv 0 \quad (p)\ for \quad p(i+j) \leqq r_0.$

(6) $a_{1,r} \not\equiv 0 \quad (p).$

*Then the following assertions hold.*

*(I) Let $m$ be an integer such that $0 \leqq m \leqq \min\{n-r-1, r-2, p-1\}$. Let $i$ be an integer such that $1 \leqq i \leqq m+r$. Then*

$$a_{i,r-i+m+1} \equiv b_{i,m}a_{1,r} \quad (p),$$

*where*

$$b_{i,m} = 0 \quad for \quad 1 \leqq i \leqq m,$$

*and*

$$b_{i,m} = (-1)^{i+m+1}\binom{i-1}{m} \quad for \quad m+1 \leqq i \leqq m+r.$$

*(For $m = 0$, this also holds without the assumption (6)).*

(II) *The number $r$ is even.*

*If $r \leqq n-2$ then $r \equiv 0 \quad (p)$.*

*If $p+1 \leqq r \leqq n-p$ then $r \geqq r_0 - p + 1$.*

PROOF. Proof of (I): We prove the statement by induction on $m$.

Since

$$a_{i,r-i+1} + a_{i+1,r-i} \equiv a_{i,r-i} \equiv 0 \quad (p)$$

for $i = 1,\ldots,r-1$, because of (2) and (4), we deduce the statement for $m = 0$.

Let $\mu$ be a natural number such that $\mu \leqq \min\{n-r-1, r-2, p-1\}$. Assume that the statement in (I) has been proved for $0 \leqq m \leqq \mu - 1$. Since $\mu \leqq n-r-1$, we may consider the congruence (3) for $(i,j,k) = (1, \mu+1, r-1)$. This gives

$$(+) \qquad a_{\mu+1,r-1}a_{1,r+\mu} \equiv 0 \quad (p),$$

since $a_{r-1,1} \equiv 0 \quad (p)$ according to (4), and since

$$a_{1,\mu+1} \equiv 0 \quad (p)$$

according to (4) because $\mu \leqq r-2$. From the induction hypothesis we get

$$a_{\mu+1,r-1} \equiv -\mu a_{1,r} \quad (p),$$

and since we have $1 \leqq \mu \leqq p-1$, we then deduce from (6) and $(+)$ that

$$(++) \qquad a_{1,r+\mu} \equiv 0 \quad (p).$$

For $2 \leqq i \leqq \mu + r$, the induction hypothesis and (2) show that

$$(-) \qquad a_{i-1,r-i+\mu+2} + a_{i,r-i+\mu+1} \equiv a_{i-1,r-i+\mu+1} \equiv b_{i-1,\mu-1}a_{1,r} \quad (p);$$

from this and $(++)$ we find successively

$$a_{1,r+\mu} \equiv 0 \quad (p), \quad a_{2,r+\mu-1} \equiv 0 \quad (p), \ldots, a_{\mu,r+1} \equiv 0 \quad (p),$$

because

$$b_{i-1,\mu-1} \equiv 0 \quad (p) \quad \text{for} \quad i \leqq \mu.$$

Again, $(-)$ and the induction hypothesis show that

$$a_{i,r-i+\mu+1} \equiv (-1)^{i+\mu+1}\binom{i-2}{\mu-1}a_{1,r} - a_{i-1,r-i+\mu+2} \quad (p),$$

for $i = \mu+1,\ldots,\mu+r$, which together with $a_{\mu,r+1} \equiv 0 \quad (p)$ gives us successively

$$a_{i,r-i+\mu+1} \equiv (-1)^{i+\mu+1}\binom{i-1}{\mu}a_{1,r} \quad (p)$$

for $i = \mu+1,\ldots,\mu+r$.

Thus the statement in (I) holds for $m = \mu$.

This proves (I).

Proof of (II): Suppose that $r$ is odd and put $i = \dfrac{r+1}{2}$.

Using (I) for $m = 0$ we see that

$$a_{i,r-1+1} \equiv (-1)^{i+1} a_{1,r} \not\equiv 0 \quad (p).$$

Since $i = r - i + 1$, this contradicts (1) because $p$ is odd. So, $r$ is even.

Suppose that $r \leqq n - 2$. Then we may use (I) for ($m = 1, i = 1$) and for ($m = 1$, $i = r + 1$) (recall that $r \geqq 3$). Using (1) this gives

$$0 \equiv -a_{1,r+1} \equiv a_{r+1,1} \equiv (-1)^{r+1} r a_{1,r} \quad (p)$$

and so $r \equiv 0 \quad (p)$ because of (6).

Suppose that $p + 1 \leqq r \leqq n - p$. From the above it follows that $r \equiv 0 \quad (p)$. We may use (I) for $m = p - 1$ and $i = p$. This gives

$$a_{p,r} \equiv a_{1,r} \not\equiv 0 \quad (p).$$

Since $r \equiv 0$ (p), we then deduce from (5) that $p + r \geqq r_0 + 1$.

DEFINITION. We define the function $f(n)$ for natural numbers $n \geqq 2$ as follows. If $v$ is a non-negative integer such that:

$$2p^v \leqq n \leqq 2p^{v+1},$$

we put

$$f(n) = 2p^v \left[ \frac{n}{2p^v} \right].$$

PROPOSITION 3. *Let $G$ be a concatenated, straight $p$-group ($p$ odd) of order $p^n$. Let $d = \omega(G)$ and let $s$ be the largest non-negative integer such that $d > p^{s-1}(p-1)$. Let $a_{i,j}$ for $i, j \in \mathbf{N}$ be the invariants of $G$ associated with degree of commutativity 0. Assume that*

$$a_{i,j} \equiv 0 \quad (p) \quad fpr \quad i + j \leqq 3p^s.$$

*Then the following statements hold.*

(I) *If $n \leqq d + p^{s+1} + p^s - 1$ then*

$$a_{i,j} \equiv 0 \quad (p) \quad for \quad i + j \leqq f(n).$$

(II) *If $d = p^s(p-1)$ and $n \geqq p^{s+1} + p^s$ then $G$ has degree of commutativity 1.*

PROOF. Proof of (I): For $\mu = 0, \ldots, s$ we put

$$n_\mu = [np^{-\mu}],$$

and

$$a_{i,j}^{(\mu)} = a_{p^\mu i, p^\mu j} \quad \text{for} \quad i, j \in \mathbf{N}.$$

Then for $\mu = 0, \ldots, s$ we have

(1) $a_{i,j}^{(\mu)} \equiv -a_{j,i}^{(\mu)} \quad (p) \quad$ for $\quad i + j \leqq n_\mu$,

(2) $a_{i,j+1}^{(\mu)} + a_{i+1,j}^{(\mu)} \equiv a_{i,j}^{(\mu)} \quad (p) \quad \text{for} \quad i+j+1 \leqq n_\mu,$

(3) $a_{i,j}^{(\mu)} a_{k,i+j}^{(\mu)} + a_{j,k}^{(\mu)} a_{i,j+k}^{(\mu)} + a_{k,i}^{(\mu)} a_{j,k+i}^{(\mu)} \equiv 0 \quad (p) \quad \text{for} \quad i+j+k \leqq n_\mu.$

(1) and (3) follow for arbitrary $\mu$ from the fact that (1) and (3) hold for $\mu = 0$, cf. Theorem B(1) and B(2). (2) follows from Proposition 1.

We see from the definition of $f(n)$ that we may assume that $n$ has form

$$n = 2mp^l \quad \text{with} \quad 1 \leqq m \leqq p.$$

We may also assume that $n \geqq 3p^s$, which gives $l \geqq s$. Furthermore,

$$2p^{s+1} - 1 = p^s(p-1) + p^{s+1} + p^s - 1 \geqq d + p^{s+1} + p^s - 1 \geqq n = 2mp^l \geqq 2p^l,$$

whence $s \geqq l$. Thus we assume that

$$n = 2mp^s \quad \text{with} \quad 1 \leqq m \leqq p.$$

Then

$$n_\mu = 2mp^{s-\mu} \quad \text{for} \quad \mu = 0, \ldots, s.$$

Now we show by induction on $s - \mu$ that if $\mu \in \{0, \ldots, s\}$ then

$$a_{i,j}^{(\mu)} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq f(n_\mu).$$

For $\mu = 0$ this is precisely the statement in (I).

Suppose first that $\mu = s$. By assumption we have

$$a_{i,j}^{(s)} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq 3.$$

We also have $n_s = 2m \leqq 2p$ and so $f(n_s) = n_s$. Now assume that not all of the numbers

$$a_{i,j}^{(s)} \quad \text{with} \quad i+j \leqq n_s$$

are congruent to 0 modulo $p$. Let $r_s \in \mathbf{N}$ be largest possible such that

$$a_{i,j}^{(s)} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq r_s.$$

Then $3 \leqq r_s \leqq n_s - 1$. Now we see that we may use proposition 2 with $r = r_s$ and $r_0 = n_s$ (note that $n_s \leqq 2p$, and that we must have

$$a_{1,r_s}^{(s)} \not\equiv 0 \quad (p),$$

because of (2)). So, $r_s$ is even. If $r_s \leqq n_s - 2$ then $r_s$ is divisible by $p$ and so

$$r_s \geqq 2p \geqq n_s.$$

Consequently, we have $r_s \geqq n_s - 1$, and since $r_s$ and $n_s$ are both even, we get $r_s = n_s$, contradiction.

Suppose then that $\mu < s$ and that

$$a_{i,j}^{(\mu+1)} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq f(n_{\mu+1}).$$

Assume that not all of the numbers

$$a_{i,j}^{(\mu)} \quad \text{with} \quad i+j \leqq n_\mu$$

are congruent to 0 modulo $p$, and let $r_\mu \in \mathbf{N}$ be largest possible such that

$$a_{i,j}^{(\mu)} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq r_\mu.$$

Then we have $r_\mu \leqq n_\mu - 1$, and because of the assumptions of the theorem, we have $r_\mu \geqq 3p^{s-\mu} \geqq p+1$. Furthermore,

$$a_{pi,pj}^{(\mu)} = a_{i,j}^{(\mu+1)} \equiv 0 \quad (p) \quad \text{for} \quad p(i+j) \leqq pf(n_{\mu+1}) = pn_{\mu+1} = n_\mu.$$

Thus, we see that we may use Proposition 2 with $r = r_\mu$ and $r_0 = n_\mu$; note that we must have

$$a_{1,r_\mu} \not\equiv 0 \quad (p).$$

So, if $r_\mu \leqq n_\mu - p$ then $r_\mu \geqq n_\mu - p + 1$; so $r_\mu \geqq n_\mu - p + 1$. Since $\mu < s$, we have $n_\mu \equiv 0 \quad (p)$, and so $r_\mu \leqq n_\mu - 2$ is impossible since $r_\mu$ would then be divisible by $p$ and so $r_\mu = n_\mu$. Hence, $r_\mu \geqq n_\mu - 1$, and since $r_\mu$ and $n_\mu$ are both even, we deduce $r_\mu = n_\mu$, contradiction.

This proves (I).

Proof of (II): We use induction on $n$. For $n = p^{s+1} + p^s$ the statement follows from (I) since we have $f(n) = n$ in this case.

Thus we assume that $n > p^{s+1} + p^s$. Considering $G/G_n$ we deduce from the induction hypothesis that

$$a_{i,j} \equiv 0 \quad (p) \quad \text{for} \quad i,j \leqq n-1.$$

If not all of the numbers $a_{i,j}$ are divisible by $p$, we find (considering (2)) that

$$a_{1,n-1} \not\equiv 0 \quad (p).$$

But since $n - 1 > d$ we find using Theorem C that

$$a_{1,n-1} \equiv a_{1,n-1-d} \equiv 0 \quad (p);$$

contradiction.

THEOREM 3. *Let $G$ be an $\alpha$-concatenated, straight $p$-group ($p$ odd) of order $p^n$ and with $\alpha$ of order $p^k$. Let $a_{i,j}$ for $i,j \in \mathbf{N}$ be $G$'s invariants associated with degree of commutativity* 0, *and assume that*

$$a_{i,j} \equiv 0 \quad (p) \quad \textit{for} \quad i+j \leqq 3p^{k-1}.$$

*Put $d = \omega(G)$ and let $s$ be the largest non-negative integer with*

$$d > p^{s-1}(p-1).$$

*Then we have*

$$a_{i,j} \equiv 0 \quad (p) \quad \textit{for} \quad i+j \leqq f(\min\{n, d+p^{s+1}+p^s-1\}).$$

*Furthermore, if* $n \geqq p^k + p^{k-1}$ *then* $G$ *has degree of commutativity* 1.

PROOF. First note that $d \leqq p^k$: For if $n \geqq 1 + p^k$ then $d \leqq p^{k-1}(p-1)$ according to Proposition 1. And if $n \leqq p^k$ then $d \leqq n \leqq p^k$. So, $s \leqq k$.

If $s \leqq k-1$ then by using Proposition 3 on

$$G/G_{d+p^{s+1}+p^s},$$

we obtain

$$a_{i,j} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq f(\min\{n, d+p^{s+1}+p^s-1\}).$$

Suppose then that $s = k$. According to Proposition 1 we must then have $n \leqq p^k$. Using Proposition 3 on

$$G/G_{p^{k-1}(p-1)+1},$$

we find

$$a_{i,j} \equiv 0 \quad (p) \quad \text{for} \quad i+j \leqq p^{k-1}(p-1).$$

But since $p^{k-1}(p-1) < d \leqq n \leqq p^k$, we find

$$f(\min\{n, d+p^{k+1}+p^k-1\}) = f(n) = p^{k-1}(p-1).$$

Finally, suppose that $n \geqq p^k + p^{k-1}$. Then according to Proposition 1 we have

$$d = p^r(p-1) \quad \text{for some} \quad r \in \{0, \ldots, k-1\}.$$

Then $s = r \leqq k-1$. Then Proposition 3 and the assumption of the theorem imply that $G$ has degree of commutativity 1.

Suppose that $G$ is a finite $p$-group of maximal class of order $p^n$ where $p$ is an odd prime number and $n \geqq 4$. Then for any maximal subgroup of $G$ there exists an inner automorphism of $G$ which, when restricted to this subgroup, has order $p$ and exactly $p$ fixed points (see Theorem 3 in [3]). In particular, the group

$$G_1 = C_G(\gamma_2(G)/\gamma_4(G)),$$

which is a maximal subgroup of $G$, is $\alpha$-concatenated for some automorphism $\alpha$ of order $p$. Further, the concatenated $p$-group $G_1$ is straight (see Satz III, 14.16 in [2] and Theorem 6 in [3]). If $\alpha_{i,j}$ are the invariants of $G_1$ associated with degree of commutativity 0, then by definition of $G_1$ we have

$$a_{1,2} \equiv 0 \quad (p).$$

Note that the order of $G_1$ is $p^{n-1}$. We say that $G$ is exceptional if $G_1$ does not have degree of commutativity 1. We conclude from Theorem 3 that if $n \geqq p + 2$ then $G$ is not exceptional. Further, if $4 \leqq n \leqq p + 1$ then

$$a_{i,j} \equiv 0 \quad (p) \quad \text{for} \quad i + j \leqq f(n - 1).$$

But $f(n - 1) = n - 1$ if $n$ is odd, and $f(n - 1) = n - 2$ if $n$ is even.

Hence we see that if $G$ is exceptional then $n \leqq p + 1$ and $n$ is even. Furthermore, $G/G_{n-1}$, which is a finite $p$-group of maximal class, is never exceptional. These statements are classical results of Blackburn concerning finite $p$-groups ($p$ odd) of maximal class. Thus, Theorem 3 may be viewed as a generalisation of these results.

## REFERENCES

1. N. Blackburn, *On a special class of p-groups*. Acta Math. 100 (1958), 45–92.
2. B. Huppert: *Endliche Gruppen I*. Grundlehren Math. Wiss. 134, 1983.
3. I. Kiming, *Structure and derived length of finite p-groups possessing an automorphism of p-power order having exactly p fixpoints*, Math. Scand. 62 (1988), 153–172.
4. C. R. Leedham-Green, S. McKay, *On p-groups of maximal class* I, Quart. J. Math. Oxford Ser. (2) 27 (1976), 297–311.

INST. F. EXP. MATH.
UNIVERSITÄT ESSEN
ELLERNSTRASSE 29
45326 ESSEN
GERMANY