SOME REMARKS ON A CERTAIN CLASS OF FINITE p-GROUPS.

IAN KIMING

Abstract. First we extend the main result of our previous article (Math. Scand. **62** (1988), 153–172) 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 generalization 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 generalization 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 generalization 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 $6 \leq n \leq p + 1$ and n is even; see for example [2], III, 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

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

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

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

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 1. *Let G be a p-group. We say that G is concatenated if G possesses an automorphism α, a strongly central series*

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

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

$$|G_i/G_{i+1}| = p \quad \textit{for } i = 1, \ldots, n, \tag{1}$$

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

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

In this situation we shall also say that G is α-concatenated. Thus, when we say that G is α-concatenated we mean that G possesses an automorphism α, 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 fulfilled. Obviously then, α has p-power order and $(+)$ is completely determined by G and α. The symbols G_i will then always refer to the terms of this strongly central series. When G is α-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 α an automorphism of p-power order of G , then G is α-concatenated if and only if α has exactly p fixed points in G; cf. Theorem 2 in [3].

Definition 2. *Suppose that G is an α-concatenated p-group. Let t be a non-negative integer. We say that G has degree of commutativity t if*

$$[G_i, G_j] \leq G_{i+j+t} \qquad \textit{for all} \qquad i, j \in \mathbb{N}.$$

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 $i, j \in \mathbb{N}$ are integers defined modulo p by the following requirements:

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

and

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

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 α-concatenated p-group of order p^n. Suppose that G has degree of commutativity t and let $a_{i,j}$ for $i,j \in \mathbb{N}$ be the associated invariants. Then the following holds:*

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

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

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

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

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

Definition 3. *Suppose that G is a (α)-concatenated p-group with $\omega(G) = d$. We say that G is straight if the following conditions are fulfilled.*

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

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

$$x^{-p}(xc)^p \equiv c^p \mod G_{r+s+d} \qquad \textit{for all} \quad r,s \in \mathbb{N}.$$

(3) *If gG_{i+1} is a generator of G_i/G_{i+1} then the element 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*

$$i+j+d+t \leq n \qquad \Longrightarrow \qquad (a_{i,j} \equiv a_{i+d,j} \quad (p)).$$

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

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

Then G_s is a straight, α-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

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

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_μ, and where each v_μ 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_μ. Furthermore,

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

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 useful in the next section.

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

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

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

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

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

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

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

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

Proof. Let $i \in \mathbb{N}$. Using Lemma E for computation in the semi-direct product $G < \alpha >$, 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 $v \in \mathbb{N}$, where putting $U =< \alpha, [\alpha, g_i] >$ 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 $n \geq 1 + p^k$ and let

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

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

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

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

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

and

$$e \equiv c_{p^\nu} \quad \text{mod} \quad G_{m+2} \qquad \text{if} \quad \nu > 0.$$

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

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

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

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

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

$$m = p^\nu + (k-\nu)d \geq 1 + p^k > p^k,$$

which is impossible. Consequently, there exist two different numbers μ and ν 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 $v \in \mathbb{N}$ be such that $1 \leq v \leq s+1$. Then

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

and from (++) we conclude that

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

since

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

According to Lemma E we have

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

and so

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

Now suppose that $i, j \in \mathbb{N}$ are such that $p^v(i+j+1) \leq n$, 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:

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

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

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

□

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 $n \geq 2d$ 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 $n \geq 2d$ 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 $t \leq n - 2d - 1$. Let $a_{i,j}$ be the associated invariants.

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

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

and

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

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 $h \leq \frac{1}{2}d$, 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

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

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

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

Hence Theorem C gives

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

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

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

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 $n \leq 2d$ the same holds for the group G_{1+d}. If $n \geq 2d$ 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 α-concatenated, straight 2-group of order 2^n with α of order 2^k. Then the following holds.*

(1) *If $n \geq 1 + 2^k$ then G has class at the most 2^{k-1}.*

(2) *If $n \geq 2^{k+1} - 3$ then G has class at the most 2.*

(3) *G has class at the most* $2^k - 1$.

Proof. Let $d = \omega(G)$. If $n \geq 1 + 2^k$ 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 $n \geq 3$ then G is cyclic. If $n \leq 2$ then G is abelian. We may consequently assume that $k \geq 2$.

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

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

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

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

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

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

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

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

has index

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

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 α-concatenated, straight p-group of order p^n with α 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 $3 \leq r \leq n-1$. Suppose that we are given integers $a_{i,j}$ for $i, j \in \mathbb{N}$ with $i + j \leq n$. Suppose further that the following conditions are satisfied.*

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

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

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

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

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

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

Then the following assertions hold.

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

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

where

$$b_{i,m} = 0 \qquad \textit{for} \quad 1 \leq i \leq m,$$

and

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

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

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

If $r \leq n-2$ then $r \equiv 0$ (p).

If $p+1 \leq r \leq n-p$ then $r \geq r_0 - p + 1$.

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

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

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 $\mu \leq r-2$. From the induction hypothesis we get

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

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

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

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

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

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

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

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 $i = \mu+1, \dots, \mu+r$, 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 $i = \mu+1, \dots, \mu+r$.

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

This proves (I).

Proof of (II): Suppose that r is odd and put $i = \frac{r+1}{2}$.
Using (I) for $m = 0$ we see that

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

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

Suppose that $r \leq n-2$. Then we may use (I) for $(m = 1,\ i = 1)$ and for $(m = 1,\ i = r+1)$ (recall that $r \geq 3$). 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 $p+1 \leq r \leq n-p$. 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 $r \equiv 0 \quad (p)$, we then deduce from (5) that $p + r \geq r_0 + 1$. □

Definition 4. *We define the function $f(n)$ for natural numbers $n \geq 2$ as follows. If v is a non-negative integer such that:*

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

we put

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

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 $i, j \in \mathbb{N}$ be the invariants of G associated with degree of commutativity 0. Assume that*

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

Then the following statements hold.

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

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

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

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

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

and

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

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

$$(1) \qquad a^{(\mu)}_{i,j} \equiv -a^{(\mu)}_{j,i} \quad (p) \qquad \text{for} \quad i + j \leq n_\mu,$$

(2) $$a^{(\mu)}_{i,j+1} + a^{(\mu)}_{i+1,j} \equiv a^{(\mu)}_{i,j} \quad (p) \qquad \text{for} \quad i+j+1 \le n_\mu,$$

(3) $$a^{(\mu)}_{i,j} a^{(\mu)}_{k,i+j} + a^{(\mu)}_{j,k} a^{(\mu)}_{i,j+k} + a^{(\mu)}_{k,i} a^{(\mu)}_{j,k+i} \equiv 0 \quad (p) \qquad \text{for} \quad i+j+k \le n_\mu.$$

(1) and (3) follow for arbitrary μ 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

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

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

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

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

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

Then

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

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

$$a^{(\mu)}_{i,j} \equiv 0 \quad (p) \qquad \text{for} \quad i+j \le f(n_\mu).$$

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

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

$$a^{(s)}_{i,j} \equiv 0 \quad (p) \qquad \text{for} \quad i+j \le 3.$$

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

$$a^{(s)}_{i,j} \qquad \text{with} \quad i+j \le n_s$$

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

$$a^{(s)}_{i,j} \equiv 0 \quad (p) \qquad \text{for} \quad i+j \le r_s.$$

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

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

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

$$r_s \ge 2p \ge n_s.$$

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

Suppose then that $\mu < s$ and that

$$a^{(\mu+1)}_{i,j} \equiv 0 \quad (p) \qquad \text{for} \quad i+j \le f(n_{\mu+1}).$$

Assume that not all of the numbers

$$a^{(\mu)}_{i,j} \qquad \text{with} \quad i+j \le n_\mu$$

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

$$a^{(\mu)}_{i,j} \equiv 0 \quad (p) \qquad \text{for} \quad i+j \le r_\mu.$$

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

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

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 $r_\mu \le n_\mu - p$ then $r_\mu \ge n_\mu - p + 1$; so, $r_\mu \ge n_\mu - p + 1$. Since $\mu < s$, we have $n_\mu \equiv 0 \quad (p)$, and so $r_\mu \le n_\mu - 2$ is impossible since r_μ would then be divisible by p and so $r_\mu = n_\mu$. Hence, $r_\mu \ge n_\mu - 1$, and since r_μ and n_μ 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

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

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

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

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

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

Then we have

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

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

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

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

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

we obtain

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

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

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

we find

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

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

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

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

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

Then $s = r \leq k-1$. 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 $n \geq 4$. 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 α-concatenated for some automorphism α 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 $a_{i,j}$ 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 $n \geq p+2$ then G is not exceptional. Further, if $4 \leq n \leq p+1$ then

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

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 $n \leq p+1$ 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 generalization 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 der mathematischen Wissenschaften **134**, Springer 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.

kiming@math.ku.dk

Dept. of math., Univ. of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark.