STRUCTURE AND DERIVED LENGTH OF FINITE $p$-GROUPS
POSSESSING AN AUTOMORPHISM OF $p$-POWER ORDER
HAVING EXACTLY $p$ FIXED POINTS.

IAN KIMING

1. 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 $p$ and having exactly $p^n$ fixed points 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 $p$
fixed points. 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 3 we derive a more useful description of the groups in question and
we show that the theory of these objects is similar to the theory of finite $p$-groups
of maximal class. We illustrate the ideas in abelian $p$-groups.

In section 4 we study $p$-power and commutator structure.

Based on the results of section 4 we prove the main theorems in section 5. The
method leading to the proof of our main theorems does not resemble Alperin’s
method. Our 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 used by Leedham-Green and McKay in [5], and is of ‘combinatorial’
nature.

2. 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
\[ [x, yz] = [x, z][x, y][x, y, z] \quad \text{and} \quad [xy, z] = [x, z][x, z, y][y, z] \]
(where $[x_1, ..., x_{n+1}] = [[x_1, ..., x_n], x_{n+1}]$).

If $\alpha$ is an automorphism of a group $G$ we write $x^\alpha$ for the image of $x$ under $\alpha$.

If $\alpha$ is an automorphism of a group $G$, and if $N$ is an $\alpha$-invariant, normal sub-
group of $G$, then we also write $\alpha$ for the automorphism induced by $\alpha$ on $G/N$.  


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

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

3.

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 $p$ fixed points.

**Definition 1.** Suppose that $G$ is a finite $p$-group. We say that $G$ is concatenated if and only if $G$ has:

(i) a strongly central series

\[ G = G_1 \geq G_2 \geq \ldots \geq G_n = \{e\} \]  

(putting $G_k = \{e\}$ for $k \geq n$, ‘strongly central’ means that $[G_i, G_j] \leq G_{i+j}$; for all $i, j$),

(ii) elements $g_i \in G_i$, $i = 1, \ldots, n$, and

(iii) an automorphism $\alpha$ such that

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

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

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

In the situation of definition 1 we shall also say that $G$ is $\alpha$-concatenated. It is easy to see that $\alpha$ has $p$-power order whenever $\alpha$ is an automorphism of the finite $p$-group $G$ such that $G$ is $\alpha$-concatenated.

If $G$ is a finite $p$-group, then the statement ‘$G$ is $\alpha$-concatenated’ means that $G$ possesses an automorphism $\alpha$ such that $G$ is $\alpha$-concatenated.

Whenever $G$ is given as an $\alpha$-concatenated $p$-group, we shall assume that a strongly central series $G = G_1 \geq G_2 \geq \ldots$ and elements $g_i \in G_i$ have been chosen so that conditions (1), (2) and (3) in definition 1 above are fulfilled; the symbols $G_i$ and $g_i$ then always refer to this choice.

**Proposition 1.** Suppose $G$ is an $\alpha$-concatenated $p$-group. Then for all $i \in \mathbb{N}$, $G_{i+1}$ is the image of $G_i$ under the mapping

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

and if $G_{i+1}$ is generated by $x G_{i+1}$, then the group $G_{i+1}/G_{i+2}$ is generated by $[x, \alpha] G_{i+2}$.

**Proof.** Suppose that $G$ has order $p^{n-1}$. Then $[g_{n-1}, \alpha] = e$ and so $[g_n^a, \alpha] = e$ for all $a$. This shows the assertions for all $i \geq n - 1$. Assume then that the enunciations have been proved for $i \geq k + 1$, where $1 \leq k < n - 1$. If then $x \in G_k - G_{k+1}$, we write $x = g_k^a y$, where $a \in \{1, \ldots, p - 1\}$ and $y \in G_{k+1}$. Then,

\[ [x, \alpha] = [g_k^a, \alpha] [g_k^a, \alpha, y] [y, \alpha] \]

whence

\[ [x, \alpha] \equiv [g_k, \alpha]^a \mod G_{k+2}, \]
since it is easy to see that $[g_k^r, \alpha] \equiv [g_k, \alpha]^r \mod G_{k+2}$ for all $r$. Thus we deduce

$$[x, \alpha] \equiv g_k^{a_{k+1}} \mod G_{k+2}.$$ 

As a consequence we have demonstrated the last enunciation for $i = k$ and that the image of $G_k$ under the mapping $x \mapsto [x, \alpha]$ is contained in $G_{k+1}$. It also follows that the group of fixed points of $\alpha$ in $G$ is $G_{n-1}$.

Then for $x, y \in G_k$,

$$[x, \alpha] = [y, \alpha] \iff yx^{-1} = (yx^{-1})^\alpha \iff yx^{-1} \in G_{n-1},$$

and since $G_{n-1} \leq G_k$, we see that the image of the mapping $x \mapsto [x, \alpha]$ restricted to $G_k$ has order

$$|G_k : G_{n-1}| = \frac{1}{p}|G_k| = |G_{k+1}|.$$ 

Thus this image must be all of $G_{k+1}$. $\square$

**Proposition 2.** Let $G$ be a finite $p$-group and let $\alpha$ be an automorphism of $p$-power order of $G$. Then the following statements are equivalent:

1. $G$ is $\alpha$-concatenated.
2. $\alpha$ has exactly $p$ fixed points in $G$.

**Proof.** (1) implies (2): If $G$ has order $p^{n-1}$ then Proposition 1 implies that $\alpha$’s group of fixed points in $G$ is $G_{n-1}$; but $|G_{n-1}| = p$.

(2) implies (1): We show by induction on $|G|$ that $G$ is $\alpha$-concatenated. Of course we may assume that $|G| > p$.

If $N$ is an $\alpha$-invariant, normal subgroup of $G$, it is well-known that $\alpha$ has at the most $p$ fixed points in $G/N$ ($xN$ is a fixed point if and only if $x^{-1}x^\alpha \in N$; $x^{-1}x^\alpha = y^{-1}y^\alpha$ if and only if $yx^{-1}$ is a fixed point of $\alpha$ in $G$). Since the order of $\alpha$ is a power of $p$, $\alpha$ must then have exactly $p$ fixed points in $G/N$.

Let $F$ be the group of fixed points of $\alpha$ in $G$. Since $\alpha$ has $p$-power order, and since $|F| = p$, $F$ is contained in the center of $G$. From the inductive hypothesis we deduce that $G/F$ is $\alpha$-concatenated. Therefore there exists a strongly central series

$$G/F = G_1/F \geq \ldots \geq G_n/F = \{e\}$$

and elements $g_i \in G_i$ such that

$$G_i/G_{i+1} \text{ has order } p,$$

$$G_i/G_{i+1} \text{ is generated by } g_iG_{i+1} \text{ for } i = 1, \ldots, n-1,$$

and

$$[g_iF, \alpha] \equiv g_i^{F+i} \mod G_{i+2}/F \text{ for } i = 1, \ldots, n-2.$$ 

Then

$$[g_i, \alpha] \equiv g_i^{F+1} \mod G_{i+2} \text{ for } i = 1, \ldots, n-2,$$

and $e \neq [g_{n-1}, \alpha] \in F$. Putting $g_n := [g_{n-1}, \alpha]$, we then have that $g_n$ generates $F$.

Put $G_{n+i} = \{e\}$ for $i \in \mathbb{N}$. Then we only have to show that the series

$$G = G_1 \geq G_2 \geq \ldots \geq G_n = F \geq G_{n+1} = \{e\}$$

is strongly central. Consider the semidirect product $H = G < \alpha >$. Since the terms of the series are all $\alpha$-invariant we get $\gamma_i(H) \leq G_i$ for $i \geq 2$. 

Since $[G_1, \alpha, \ldots, \alpha] \in G_i - G_{i+1}$ if $G_i \neq \{e\}$, we see that $\gamma_i(H) = G_i$ for $i \geq 2$.

Then $[G_i, G_j] \leq [\gamma_i(H), \gamma_j(H)] \leq \gamma_{i+j}(H) = G_{i+j}$

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

\textbf{Corollary 1.} If $G$ is a finite, $\alpha$-concatenated $p$-group, then the only $\alpha$-invariant, normal subgroups of $G$ are the $G_i$ for $i \in \mathbb{N}$.

\textbf{Proof.} Suppose that $N$ is an $\alpha$-invariant, normal subgroup of $G$. Since $\alpha$ has $p$-power order, $\alpha$ has exactly $p$ fixed points in $N$. Thus $\alpha$'s group of fixed points in $G$ is contained in $N$. By induction on $|G|$ the statement follows immediately.

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

\textbf{Proposition 3.} Let $G$ be a finite $p$-group.

Then $G$ is $\alpha$-concatenated for some automorphism $\alpha$ of order $p$, if and only if $G$ can be embedded as a maximal subgroup of a finite $p$-group of maximal class.

\textbf{Proof.} Suppose that $G$ is $\alpha$-concatenated where $O(\alpha) = p$. Then $G$ is embedded as a maximal subgroup of the semidirect product $H = G \triangleleft \alpha$. By Proposition 1 we see that $H$ has class $n - 1$ if $G$ has order $p^{n-1}$. Thus $H$ is a finite $p$-group of maximal class.

Suppose conversely that $H$ is a finite $p$-group of maximal class and order $p^n$. Let $U$ be a maximal subgroup of $H$. We have to show that $U$ is $\alpha$-concatenated for some automorphism $\alpha$ of order $p$ and may assume that $n \geq 4$.

Put $H_i = \gamma_i(H)$ for $i \geq 2$, and $H_1 = C_H(H_2/H_4)$. It is well-known that

$$H_1 = C_H(H_i/H_{i+2}) \quad \text{for } i = 2, \ldots, n - 3 ;$$

this is also true for $i = n - 2$ if $p = 2$ (see [4], p. 362). Since $H$ has $p + 1$ maximal subgroups, we deduce the existence of a maximal subgroup $U_1$ of $H$ such that $U_1$ is different from $U$ and from

$$C_H(H_i/H_{i+2}) \quad \text{for } i = 2, \ldots, n - 2 .$$

If $U = < u, H_2 >$ and $U_1 = < u_1, H_2 >$ then $H$ is generated by $u$ and $u_1$. Suppose that $s \in C_H(u_1) \cap U$ and write $s = u_1^a u^b x$ with $x \in H_2$. Then $u_1$ commutes with $u^b x$. Since $H$ is not abelian, we must have $b \not\equiv 0 \pmod{p}$. Then $s = u_1^a y$ where $y \in H_2$. Since $s \in U \neq U_1$ we must have $a \equiv 0 \pmod{p}$. Then $s \in H_2$. Since

$$u_1 \not\in C_H(H_i/H_{i+2}) \quad \text{for } i = 2, \ldots, n - 2$$

we deduce $s \in H_{n-1} = Z(H)$. If $\alpha$ denotes the restriction to $U$ of the inner automorphism induced by $u_1$, then consequently $\alpha$ has exactly $p$ fixed points in $U$.

Then $U$ is $\alpha$-concatenated according to Proposition 2. Furthermore,

$$u_1^p \in C_H(U_1) \cap H_2 \leq C_H(U_1) \cap U = Z(H)$$

so $\alpha$ has order $p$.

Next we determine the structure of finite abelian, concatenated $p$-groups. The purpose is to provide some simple examples that will display certain phenomena occurring quite generally.
Proposition 4. Let \( U \) be a finite abelian, concatenated \( p \)-group.

Then \( U \) has type

\[
(\mu^d+1, \ldots, \mu^d+1, \mu^s, \ldots, \mu^s) \quad \text{for some } \mu \in \mathbb{N}, \ s \geq 0, \ d > s .
\]

Proof. Suppose that \( U \) is \( \alpha \)-concatenated. Let \( \omega(U) = p^d \). Now, \( U/U^p \) is \( \alpha \)-concatenated so we deduce the existence of elements \( u_1, \ldots, u_d \in U \) and \( u \in U^p \) such that

\[
U = \langle u_1, \ldots, u_d \rangle \quad \text{and} \quad u^\alpha_u = u_{i+1} \quad \text{for } i = 1, \ldots, d - 1, \quad u_d^\alpha = u_{d+1} .
\]

If we put \( p^\mu_i = O(u_i) \) we deduce \( \mu_1 \geq \ldots \mu_d \). Let \( s \geq 0 \) and \( \mu \in \mathbb{N} \) 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

\[
(u_s^\mu s+1)^\alpha = u_s^\mu s+1 u_s^\mu s+1 = u_s^\mu s+1
\]

and so \( \mu_s - \mu_{s+1} = 1 \), since \( \alpha \) has exactly \( p \) fixed points in \( U \). Then \( \mu_{s+1} = \ldots = \mu_d \), since \( u_1, \ldots, u_d \) are independent generators. \( \Box \)

Proposition 5. For integers \( \mu, s, d \) with \( \mu, s, d \in \mathbb{N} \) and \( d > s \geq 0 \), we consider the finite, abelian \( p \)-group

\[
U = U(p, \mu, s, d) := (\mathbb{Z}/\mathbb{Z}p^\mu)^s \times (\mathbb{Z}/\mathbb{Z}p^\mu)^{d-s}
\]

with canonical basis \((u_1, \ldots, u_d)\) (so that \( O(u_i) = p^{\mu+1} \) for \( i = 1, \ldots, s \), and \( O(u_i) = p^\mu \) for \( i > s \)).

For any integers \( b_1, \ldots, b_d \) with \( b_i \neq 0 (p) \) we define the endomorphism \( \alpha \) of \( U \) by

\[
u_i^\alpha = u_i u_{i+1} \quad \text{for } i = 1, \ldots, d - 1, \quad u_d^\alpha = u_{d+1} ,
\]

where \( u := u_1^{b_1} \ldots u_d^{b_d} \).

Then \( \alpha \) is an automorphism of \( U \) and \( U \) is \( \alpha \)-concatenated.

For all \( i \in \mathbb{N} \) define: \( u_i := [u_1, \alpha, \ldots, \alpha] \) (for \( i \leq d \) this is of course not a definition, but rather a property of \( \alpha \)), and put \( U_i := \langle u_j \mid j \geq i \rangle \).

The order of \( \alpha \) is then determined as follows:

Let \( v \in \mathbb{Z} \), \( v \geq 0 \) be least possible such that \( d \leq p^v(p-1) \).

Case (1). \( d < p^v(p-1) \): If \( d \mu + s \leq p^v \) then \( O(\alpha) = p^\sigma \), where \( \sigma \) is least possible such that \( p^\sigma \geq d \mu + s \).

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

\[
k \geq \frac{d \mu + s - p^v}{d} .
\]

Case (2). \( d = p^v(p-1) \): If \( d \mu + s < p^{v+1} \), put \( r = d \mu + s \). Otherwise, there exists \( r \in \{p^{v+1}, \ldots, d \mu + s \} \) least possible such that

\[
X := u_2^{(p^{v+1})} \ldots u_{p^{v+1}-2}^{(p^{v+1})} u_{p^{v+1}-1}^{(p^{v+1})} u_{p^{v+1}} \in U_{r+1} .
\]
Then $O(\alpha) = p^{v+k+1}$ where $k \geq 0$ is least possible such that
\[ k \geq \frac{d\mu + s - r}{d}. \]

**Proof.** It is easily verified that $\alpha$ is an automorphism of $U$, that $\alpha$ has exactly $p$ fixed points, and that $\alpha$ has $p$-power order. So, $U$ is $\alpha$-concatenated by Proposition 2.

By an easy inductional argument (on the parameter $d\mu + s$) we see that for all $i$,
\[ u_i^p \equiv u_i^a \mod U_{i+d+1} \quad \text{with } a \neq 0 \quad (p). \]

By induction on $k$ we also see that for all $i$,
\[ u_i^{\alpha^k} = u_i^{(k)} \cdots u_i^{(k-1)} \cdot \]

From these facts we may conclude that
\[ u_i^{\sigma^v} \equiv u_i^{b} \mod U_{i+p^\sigma+1} \quad \text{for all } i \text{ and all } \sigma \leq v, \]

since $d > p^\sigma(p-1)$ for $\sigma \leq v$.

**Case (1).** $d < p^\sigma(p-1)$: By an easy induction on $k \geq 0$ we get
\[ u_i^{\sigma^{p+k}} \equiv u_i^{b} \mod U_{i+p^\sigma+kd+1} \]
where $b(k) \neq 0 \quad (p)$. Here we have used the inequality
\[ (1-k(p-1))d < p^{v+1} - p^v. \]

**Case (2).** $d = p^t(p-1)$: With the same technique as in Case (1) we see that
\[ X \in U_{p^{v+1}+1}. \]

If $r = d\mu + s$ the statement about the order of $\alpha$ is seen to be true, so we assume that $d\mu + s > p^{v+1}$, and also that $U_{r+1} \neq \{e\}$. Then we may write
\[ u_i^{p^{v+1}} \equiv u_i^{b} \mod U_{r+2} \]
where $b \neq 0 \quad (p)$. Letting $(a-1)^{i-1}$ operate on this congruence we obtain
\[ u_i^{\sigma^{p+1}} \equiv u_i^{b} \mod U_{i+r+1}. \]

Then, by using the inequality $r + kd < p(r + (k-1)d)$ for $k \geq 1$, we get by induction on $k \geq 1$
\[ u_i^{\sigma^{p+k}} \equiv u_i^{b} \mod U_{i+r+(k-1)d+1} \]
for all $i$ with some $b(k) \neq 0 \quad (p)$. □

**Remark 1.** In Case (1) of Proposition 5 we see that the order of $U$ 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 $G$ is an $\alpha$-concatenated $p$-group where $O(\alpha) = p^{k}$ then either $G_{s(p,k)}$ has order less than $t(p,k)$ or $\omega(G_{s(p,k)})$ has form $p^{v}(p-1)$.

This more than indicates that the concatenated $p$-groups $G$ with $\omega(G)$ of form $p^{v}(p-1)$ 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.
**Definition 2.** Let $G$ be an $\alpha$-concatenated $p$-group. Let $t \in \mathbb{Z}$, $t \geq 0$. We say that $G$ has degree of commutativity $t$ if

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

In the proof of our main theorem, we shall show that if $G$ is a finite, concatenated $p$-group, then for sufficiently large $s$ the group $G_s$ has high degree of commutativity (in comparison with $n$ if $|G_s| = p^n$). In this connection it will be useful to single out a certain class of finite, concatenated $p$-groups having ‘straight’ $p$-power structure.

**Definition 3.** Suppose that $G$ is a finite, $\alpha$-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 $i \in \mathbb{N}$.
2. $x \in G_r$ and $c \in G_s$ implies $x^{-p}(xc)^p \equiv c^p \mod G_{r+s+d}$, for all $r, s \in \mathbb{N}$.
3. For all $i \in \mathbb{N}$ we have: If $gG_{i+1}$ is a generator of $G_i/G_{i+1}$, then $g^pG_{i+d+1}$ generates $G_{i+d}/G_{i+d+1}$.

We now give a criterion for straightness.

**Proposition 6.** Let $G$ be a finite, $\alpha$-concatenated $p$-group with $\omega(G) = d$.

If $G$ is regular, or has degree of commutativity $\geq (d+1)/(p-1) - 1$, then $G$ is straight.

**Proof.** For the theory of finite, regular $p$-groups the reader is referred to [3], or [4], pp. 321–335.

Let $|G| = p^{n-1}$. We prove the theorem by induction on $n$. Thus we may assume that $G_2$ is straight. Put $\omega(G_2) = d_1$. We may also assume that $G$ does not have exponent $p$.

(a) We claim that if $r \leq s$, and if $x \in G_r$, $c \in G_s$, then:

$$x^{-p}(xc)^p \equiv c^p \mod G_{r+s}^p G_{r+s+d}.$$ 

For suppose that $G$ is regular. We then obtain

$$x^{-p}(xc)^p \equiv c^p \mod \gamma_2(<x, c>)^p,$$

and in any case we see, using the Hall-Petrescu formula (see [4], pp. 317–318), that

$$x^{-p}(xc)^p \equiv c^p \mod \gamma_2(<x, c>)^p \gamma_p(<x, c>).$$

Now, $\gamma_2(<x, c>) \leq G_{r+s}$, so if $G$ has degree of commutativity $\geq \frac{d_1+1}{p-1} - 1$ then

$$\gamma_p(<x, c>) \leq G_{s+(p-1)r+(p-1)t}.$$ 

(b) We claim that $d_1 \geq d$. We may assume $G_{d+2} = \{e\}$ and have to prove that $G_2^p = \{e\}$.

Suppose that $y \in G_i$, where $i \geq 2$. According to Proposition 1 there exists $x \in G_{i-1}$ such that $[x, \alpha] = y$.

Now, $G^p = G_{d+1}^p$: For $G^p$ is an $\alpha$-invariant, normal subgroup of index $p^d$. So, by Corollary 1 the claim follows (from now on we will use Corollary 1 without explicit reference).

In particular, $x^p \in G_{d+1}$, whence according to (a),

$$e = [x^p, \alpha] = x^{-p}(x^p)^p = x^{-p}[x, \alpha]^p \equiv [x, \alpha]^p = y^p \mod G_{2i-1}^p G_{2i-1+d}.$$
Now, \( G_{2i-1+d} = \{ e \} \), and since certainly \( d_1 \geq d - 1 \), \( G_{2i-1}^p = \{ e \} \). Hence, \( y^p = e \).

(c) We claim that \( G_i^p \leq G_{i+d} \) for all \( i \in \mathbb{N} \): This is clear from (b) and the inductive hypothesis.

(d) If \( r \leq s \), and if \( x \in G_r \), \( c \in G_s \), then:

\[
x^{-p}(xc)^p \equiv c^p \pmod{G_{r+s+d}}.
\]

This is clear from (a) and (c).

(e) We claim that \( d_1 = d \): We may assume \( G_{d+2} > \{ e \} \). Choose \( g \in G \) such that \( g^p \notin G_{d+2} \). Then

\[
[g^p, \alpha] = g^{-p}(g[\alpha])^p \equiv [g, \alpha]^p \pmod{G_{d+3}}
\]

because of (d). Since \([g^p, \alpha] \notin G_{d+3} \), we have \([g, \alpha]^p \notin G_{d+3} \). Since \([g, \alpha] \in G_2 \), this proves \( d_1 \leq d \).

(f) If \( gG_2 \) generates \( G_1/G_2 \), and if \( x \in G \), we have \( x = g^ay \) for some \( y \in G_2 \).

By (a) we then have

\[
g^{-pa}x^p \equiv y^p \equiv e \pmod{G_{d+2}}.
\]

Since \( G^p = G_{d+1} \), we must then have \( g^p \notin G_{d+2} \). Then \( g^pG_{d+2} \) generates \( G_{d+1}/G_{d+2} \).

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

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

\[
\mu_{\sigma,s} + s \equiv \sigma \pmod{2^i} \quad \text{and} \quad \mu_{\sigma,s} \in \{0, \ldots, 2^i - 1\}.
\]

Then the integer

\[
\nu := 2 \left( \frac{2^i - 1}{\sigma} \right) + \sum_{s=1}^{2^i-1} \left( \frac{2^i}{s} \right) \left( \frac{2^i - 1}{\mu_{\sigma,s}} \right)
\]

is divisible by 4.

**Proof.** Suppose that \( s \in \{0, \ldots, 2^i - 1\} \) and that \( \left( \frac{2^i}{s} \right) \) is not divisible by 4. Now,

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

hence \( 2^i \mid s \), and so \( s = 2^i - 1 \). We conclude that \( \nu \) differs from

\[
2 \left( \frac{2^i - 1}{\sigma} \right) + 2 \left( \frac{2^i - 1}{2^i - 1} \right) \left( \frac{2^i - 1}{\mu_{\sigma,2i-1}} \right)
\]

by a multiple of 4.

Now, the integer

\[
\left( \frac{2^i - 1}{\sigma} \right) + \left( \frac{2^i - 1}{2^i - 1} \right) \left( \mu_{\sigma,2^i-1} \right)
\]

is even for the following reasons: We have

\[
\left( \frac{2^i - 1}{\mu_{\sigma,2i-1}} \right) = \begin{cases} 
\left( \frac{2^i - 1}{\sigma - 2i - 1} \right) & \text{for } \sigma \geq 2i - 1 \\
\left( \frac{2^i - 1}{\sigma + 2i - 1} \right) & \text{for } \sigma < 2i - 1
\end{cases}
\]
and from well-known facts concerning the 2-powers dividing \( n! \) for \( n \in \mathbb{N} \), we see that
\[
\binom{2^i - 1}{\mu_{\sigma, 2^i - 1}}
\]
is divisible by exactly the same powers of 2 as is \( \binom{2^i - 1}{\sigma} \), and also that
\[
\binom{2^i - 1}{2^i - 1 - 1}
\]
is odd.

\[\Box\]

**Lemma 2.** Let \( F \) be the free group on free generators \( x \) and \( y \). Let \( p \) be a prime number and let \( n \) be a natural number. Then,
\[
x^{p^n} y^{p^n} = (xy)^{p^n} c_{p^n} ... c_{p^n},
\]
where \( c \in \gamma_2(F)^{p^n} \) and \( c_{p^i} \in \gamma_{p^i}(F)^{p^{n-i}} \) for \( i = 1, \ldots, n \).

Each \( c_{p^i} \) has form
\[
\prod_{j=1}^{p^i-1} v_{p^i}^{b_{p^i}^{p^i-j}} \mod \gamma_{p^i+1}(F)^{p^{n-i}} \gamma_{p^i+2}(F)^{p^{n-i-2}} \gamma_{p^i}(F)^{p^n},
\]
for certain integers \( a_i \) and \( b_{p^i} \), and certain group elements \( v_{p^i} \) which each has form:
\[
v_{p^i} = [y, z_1, \ldots, z_{p^i-1}]
\]
with \( z_k \in \{x, y\} \), and \( z_k = y \) for at least one \( k \) (in each \( v_{p^i} \)).

Furthermore, \( a_i \equiv -1 \) \( \pmod{p} \) for \( i = 1, \ldots, n \).

**Proof.** Let \( i \in \{1, \ldots, n\} \). If \( u, v \in \gamma_{p^i}(F) \) then the Hall-Petrescu formula ([4], pp. 317–318) implies
\[
(uv)^{p^n-i} \equiv u^{p^n-i} v^{p^n-i} \mod \gamma_{p^i+1}(F)^{p^{n-i}} \gamma_{p^i+2}(F)^{p^{n-i-2}} \gamma_{p^i}(F)^{p^n},
\]
From this, and from standard, elementary facts concerning commutators the result follows immediately from the Hall-Petrescu formula, except for the fact that \( a_i \equiv -1 \) \( \pmod{p} \) for \( i = 1, \ldots, n \).

Consider the abelian \( p \)-group \( U \) of type
\[
\left( p^{n-i+1}, \ldots, p^{n-i+1} \right)
\]
with basis \( u_1, \ldots, u_{p^i} \), and let \( G \) be the semidirect product \( G = U < \alpha > \) where \( \alpha \) is the automorphism of \( U \) given by
\[
u_{p^i}^a = u_{j+1}, \quad j = 1, \ldots, p^i - 1, \quad \text{and} \quad u_{p^i}^a = u_1.
\]
Then \( \alpha \) has order \( p^i \). Put \( u_s = u_r \) if \( r, s \in \mathbb{N}, r \in \{1, \ldots, p^i\} \), and \( s \equiv r \pmod{p} \).
Then for \( r = 1, \ldots, p^i \) we have
\[
[u_r, u_{p^i}, \ldots, u_{p^i}] = u_r^{(-1)^{p^i-1}} u_{r+1}^{(-1)^{p^i-2}(p^i-1)} \cdots u_{r+p^i-1}
\]
and

\[
[u_r, \alpha, \ldots, \alpha] = u_r^{1+(-1)^{p^i}} \cdot u_{r+1}^{(-1)^{p^i-1}(p^i)} \cdots u_{r+p^i-1}^{(-1)(p^i)}.
\]

Thus, \( \gamma_{p^i+1}(G) \leq U^p \). Using the same argument with \( u_r \) replaced by \( u_r^{p^i} \) we deduce

\[
\gamma_{sp^i+1}(G) \leq U^{sp^i} \quad \text{for } s \in \mathbb{N}.
\]

Since \( sp^i + 1 \leq p^{i+s-1} \) for \( s \geq 2 \) except when \( p = 2 \) and \( s = 2 \), we conclude that

\[
(\ast \ast \ast) \quad \gamma_{p^i+s-1}(G)^{p^{n-(i+s-1)}} = \{e\} \quad \text{for } s \geq 2,
\]

except possibly when \( p = 2 \) and \( s = 2 \).

If \( p = 2 \) we use (\ast) and (\ast\ast) to conclude that

\[
[u_r, \alpha, \ldots, \alpha] = \prod_{\sigma=0}^{2^i-1} u_{r+\sigma}^{b(r,\sigma)}
\]

where

\[
b(r, \sigma) = (-1)^{\sigma+1} \left( 2^i \binom{2^i-1}{\sigma} + \sum_{s=1}^{2^i-1} \binom{2^i}{s} \binom{2^i-1}{\mu_{\sigma,s}} \right)
\]

with \( \mu_{\sigma,s} \) determined by

\[
\mu_{\sigma,s} \in \{0, \ldots, 2^i-1\} \quad \mu_{\sigma,s} + s = \sigma \cdot (2^i).
\]

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

Now we compute

\[
x := (\alpha u_1)^p n (\alpha u_1^{-1}) \cdots (\alpha u_n^{-1} u_1^{-1}) \cdots (\alpha u_n^{-1} u_1) = (u_1 \cdots u_p)^{p^{n-i}}.
\]

Using the results obtained this far we conclude

\[
e = \alpha^{p^n} u_1^{p^n} = xc_{p^i} = x[u_1, \alpha, \ldots, \alpha]^{a_i} u_1^{p^{n-i}}
\]

\[
= \left( (u_1 \cdots u_p)(u_1^{(-1)p^{i-1}} \cdots u_2^{(-1)p^{i-2}(p^i)} \cdots u_1) a_i \right)^{p^{n-i}}
\]

which gives \( a_i \equiv -1 \pmod{p} \). \( \square \)

**Theorem 1.** Suppose that \( G \) is an \( \alpha \)-concatenated \( p \)-group of order \( p^{n-1} \) where \( O(\alpha) = p^k \).

If \( G \) centralizes \( G_i/G_{i+2} \) for \( i = 1, \ldots, p^k \), and if \( n \geq p^k + 2 \), then \( \omega(G) \leq p^k - 1 \).

**Proof.** Put \( d := \omega(G) \). The element \( \alpha g_1 \) belonging to the semidirect product \( H = G < \alpha > \) has the property that \( \alpha g_1 \notin C_H(G_i/G_{i+2}) \) for \( i = 2, \ldots, p^k \). Since \( (\alpha g_1)^{p^k} \) is an element of \( G_2 \) (confer Lemma 2 for instance) that commutes with \( \alpha g_1 \), we must have

\[
(\alpha g_1)^{p^k} \in G_{p^k+1}.
\]
Now assume that \(d \geq p^k\). Then \(G^p_1 \leq G_{p^{k+1}}\). By Lemma 2 we then deduce (note that \(\gamma_i(H) = G_i\) for \(i \geq 2\))

\[
eq \alpha g^p_k v_1 = (\alpha g_1)^p k \equiv c \mod G_{p^{k+1}},
\]

where \(c\) has form

\[
c \\equiv [g_1, \alpha, \ldots, \alpha]^{-1} \prod_{\mu} v_{\mu} \mod G_{p^{k+1}},
\]

with each \(v_{\mu}\) of the form \([g_1, z_1, \ldots, z_{p^k-1}]\), where \(z_j \in \{\alpha, g_1\}\) and \(z_j = g_1\) for at least one \(j\) (in each \(v_{\mu}\)). Since \(g_1 \in C_H(G_i/G_{i+2})\) for \(i = 2, \ldots, p^k\), we deduce \(v_{\mu} \in G_{p^{k+1}}\) for all \(\mu\). But then

\[
c \equiv [g_1, \alpha, \ldots, \alpha]^{-1} \not\equiv e \mod G_{p^{k+1}},
\]

a contradiction. \(\square\)

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

**Proof.** Put \(s = 1 + (1 + \ldots + p^{k-1})\). According to Theorem 1, either \(G_s\) has exponent \(p\) or \(\omega(G_s) \leq p^k - 1\). If \(G_s\) has exponent then \(G_s\) is trivially straight. Assume then that \(\omega(G_s) \leq p^k - 1\). As \(G_s\) has degree of commutativity at least

\[
s - 1 = (1 + \ldots + p^{k-1}) = \frac{p^k - 1}{p - 1} \geq \frac{p^k - p + 1}{p - 1} = \frac{p^k}{p - 1} - 1 \geq \frac{\omega(G_s) + 1}{p - 1} - 1,
\]

the statement now follows from Proposition 6. \(\square\)

**Theorem 2.** Let \(G\) be an \(\alpha\)-concatenated \(p\)-group of order \(p^{n-1}\), where \(O(\alpha) = p^k\). Suppose further that \(G\) is straight, that \(n \geq p^k + 2\), and that \(G\) centralizes \(G_i/G_{i+2}\) for \(i = 2, \ldots, p^k\).

Then \(\omega(G) = p^v(p - 1)\) for some \(v \in \{0, \ldots, k - 1\}\).

**Proof.** We wish to perform certain calculations in the semidirect product \(G < \alpha >\).

By the same argument as in the proof of Theorem 1 we see that the element \(\alpha g_1\) satisfies

\[
(\alpha g_1)^p k \in G_{p^{k+1}}.
\]

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

\[
\alpha^p g^p_k = (\alpha g_1)^p k c_{p^0} \cdots c_{p^k},
\]

where the \(c_i\)'s have the shapes given in Lemma 2. Notice that \(c_j \in G_{p^j + (k-j)d}\) and that \(c \in G_{2 + kd} \leq G_{s+1}\).

Suppose that \(i_0 = 0\): Then \(s = kd\), and we deduce \(G_{s+1} \not\equiv g^p_{s+1} \equiv e \mod G_{s+1}\), a contradiction.

Suppose then that \(i_0 > 0\): Here we get \(e \equiv g^p_{s+1} \equiv c_{p^{i_0}} \mod G_{s+1}\), and

\[
c_{p^{i_0}} = [g_1, \alpha, \ldots, \alpha]^{-p^{-i_0}} \equiv g^{-p^{-i_0}} \mod G_{s+1},
\]
but we have
\[ g_{p^{k-1_0}}^G \notin G_{s+1}, \]
a contradiction.

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

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

**Definition 4.** Suppose that \( G \) is an \( \alpha \)-concatenated \( p \)-group and that \( G \) has degree of commutativity \( t \). Then we define the integers \( a_{i,j} \) modulo \( p \) for \( i, j \in \mathbb{N} \) thus: If \( G_{i+j+t} = \{e\} \), we put \( a_{i,j} = 0 \). Otherwise, we let \( a_{i,j} \) be the unique integer modulo \( p \) determined by the condition:
\[ [g_i, g_j] \equiv g_{i+j+t}^{a_{i,j}} \mod G_{i+j+t+1}. \]

We refer to the \( a_{i,j} \) as the invariants of \( G \) 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 \( p \).

**Proposition 7.** Let \( G \) be a finite, \( \alpha \)-concatenated \( p \)-group of order \( p^n \). Suppose that \( G \) has degree of commutativity \( t \) and let \( a_{i,j} \) be the associated invariants. Then we have the following.

1. \( a_{i,j}a_{k,i+j+t} + a_{j,k}a_{i,j+k+t} + a_{k,i}a_{j,k+i+t} \equiv 0 \mod p \) for \( i + j + k + 2t + 1 \leq n \).
2. \( a_{i,j} \equiv a_{i+1,j} + a_{i,j+1} \mod p \) for \( i + j + t + 2 \leq n \).
3. If \( i_0 \in \mathbb{N} \) then we have for \( i, j \geq i_0 \):
   \[ a_{i,j} \equiv \sum_{s=0}^{i-i_0} (-1)^s \binom{i-i_0}{s} a_{i_0,j+s} \mod p \] if \( i + j + t + 1 \leq n \).
4. For \( r \in \mathbb{N} \) we have
   \[ a_{i,i+r} \equiv \sum_{s=1}^{\lceil (r+1)/2 \rceil} (-1)^{s-1} \binom{r-s}{s-1} a_{i+s-1,i+s} \mod p \] if \( 2i + r + t + 1 \leq n \).

**Proof.** We shall make use of Witt’s Identity
\[ (a, b^{-1}, c)[b, c^{-1}, a]c[a, a^{-1}, b]^a = e \]
for elements \( a, b, \) and \( c \) in a group.

1. Considering \( (*) \) modulo \( G_{i+j+k+2t+1} \) with \( a = g_i, b = g_j, \) and \( c = g_k \) gives us the congruence
   \[ g_{i+j+k+2t}^{-a_{i,j}a_{i+1,j+k}a_{j+k+i,s}a_{k,i}a_{k+i+t,j}} \equiv e \mod G_{i+j+k+2t+1}. \]
   But if \( i + j + k + 2t + 1 \leq n \) then \( g_{i+j+k+2t} \neq e \), and the claim follows.
2. Considering \( (*) \) modulo \( G_{i+j+t+2} \) with \( a = g_i, b = a^{-1}, \) and \( c = g_kj \) gives us the congruence
   \[ g_{i+j+t+1}^{-a_{i,j}a_{i+1,j}a_{i,j+1}^2} \equiv e \mod G_{i+j+t+2} . \]
But if \( i + j + t + 2 \leq n \), then \( g_{i+j+t+1} \neq e \), and the claim follows.

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

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

The next proposition reveals part of the purpose of the introduction of the idea of straight, concatenated \( p \)-groups.

**Proposition 8.** Let \( G \) be an \( \alpha \)-concatenated \( p \)-group of order \( p^{n-1} \). Suppose that \( G \) is straight and put \( d = \omega(G) \). Let \( a_{i,j} \) be \( G \)'s invariants with respect to a given degree of commutativity \( t \). Then for all \( i, j \) we have

\[
i + j + d + t + 1 \leq n \Rightarrow (a_{i,j} \equiv a_{i+d,j} \mod (p)) .
\]

**Proof.** If \( G_{i+d} \neq \{ e \} \), we have

\[
g_i^p \equiv g_{i+d} \mod G_{i+d+1} ,
\]

with \( b_i \neq 0 \) \( (p) \).

Suppose that \( i \in \mathbb{N} \) with \( G_{i+1+1} \neq \{ e \} \). Then \( g_i^p+1 = ([g_i, \alpha])p \) for some \( y \in G_{i+2} \). Then (by Lemma 2)

\[
[g_i, \alpha]^{-1} g_i^p \equiv y^p \mod G_{2i+3+d} ,
\]

so

\[
g_i^{b_i+1} \equiv g_i^p \equiv [g_i, \alpha]^p \equiv g_i^{-1}(g_i[\alpha])^p \equiv g_i^{-1} \mod G_{i+d+2} ,
\]

and since \( g_{i+d+1} \neq e \), we deduce \( b_{i+1} = b_i \) \( (p) \).

If \( i + j + d + t + 1 \leq n \) we get

\[
g_{i+j+d+t}^{b_i+a_{i+j}} \equiv [g_i, g_j]^p \equiv g_i^{-1}(g_i[\alpha])^p \equiv g_i^{-1} \mod G_{i+j+d+t+1} ,
\]

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

For straight, concatenated \( p \)-groups we have a stronger version of Proposition 7.

**Proposition 9.** Let \( G \) be a straight, \( \alpha \)-concatenated \( p \)-group of order \( p^{n-1} \) and with \( \omega(G) = p^r(p-1) \). Suppose that \( G \) has degree of commutativity \( t \) and let \( a_{i,j} \) be the associated invariants. Suppose that \( s \in \mathbb{N} \) is such that \( s + t \equiv 0 \) \( (p^n) \) and define \( a_{i,j}^{(r)} \) for \( r = 0, \ldots , v \) and \( i, j \in \mathbb{Z} \) such that \( s + ip^r, s + jp^r \geq 1 \) by

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

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

(1) Then for \( r = 0, \ldots , v \) we have the following congruences

\[
a_{i,j}^{(r)} a_{k,i+j+t(r)} + a_{j,k}^{(r)} a_{i,j+k+t(r)} + a_{k,i}^{(r)} a_{j,k+i+t(r)} \equiv 0 \mod (p)
\]

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

(2) \( a_{i,j}^{(r)} a_{i,j+p^r(p-1)} \equiv a_{i,j}^{(r)} \mod (2s + t + (i + j)p^r + p^n(p-1) + 1 \leq n .

(3) \( a_{i,j}^{(r)} \equiv a_{i,j+1}^{(r)} + a_{i,j+1}^{(r)} \mod (2s + t + (i + j + 1)p^r + 1 \leq n .

(4) If \( i_0 \in \mathbb{N} \) then for \( i, j \geq i_0 \) and \( 2s + t + (i + j)p^r + 1 \leq n \) we have:

\[
a_{i,j}^{(r)} \equiv \sum_{h=0}^{i-i_0} (-1)^h \binom{i-i_0}{h} a_{i_0,j+h}^{(r)} \mod (p)
\].
For \( w \in \mathbb{N} \) and \( 2s + (2i + w)p^r + t + 1 \leq n \),
\[
a_{i,i+w}^{(r)} = \sum_{h=1}^{\lceil w+1/2 \rceil} (-1)^{h-1} \binom{w-h}{h-1} a_{i+h-1,i+h}^{(r)} (p) .
\]

**Proof.** (1). Using Proposition 7 this follows immediately from the definitions.

(2). Using Proposition 8 this follows immediately from the definitions.

(3). Let \( r \in \{0, \ldots, v\} \) and let \( i \in \mathbb{N} \). We first claim that
\[
[g_i, \alpha^{p^r}] \equiv g_{i+p^r} \mod G_{i+p^r+1}.
\]
To see this we write, in accordance with Lemma 2,
\[
\alpha^{p^r} [\alpha^{p^r}, g_i] = (\alpha[\alpha, g_i])^{p^r} = \alpha^{p^r} [\alpha, g_i]^{p^r} c_{p^r} \cdots c_{p^r}
\]
where, with \( U := \langle \alpha, [\alpha, g_i] \rangle \) (a subgroup of the semidirect product \( G < \alpha \)),
\[
c \in \gamma_2(U)^{p^r}, \quad c_{p^r} \in \gamma_2(U)^{p^r-\mu}, \quad \mu = 1, \ldots, r ,
\]
and
\[
c_{p^r} \equiv [g_i, \alpha, \ldots, \alpha]^{-1} \equiv g_{i+p^r}^{-1} \mod G_{i+p^r+1}.
\]
Furthermore, since \( r \leq v \), we have
\[
G_{i+1}^{p^r} \leq G_{i+p^r+1} \quad \text{and} \quad \gamma_{p^r}(U)^{p^r-\mu} \leq G_{i+p^r+(r-\mu)d} \leq G_{i+p^r+1}
\]
for \( \mu = 1, \ldots, r-1 \). The claim follows from this.

Now suppose that \( i, j \in \mathbb{Z} \) such that \( s + ip^r, s + jp^r \geq 1 \) and \( z := 2s + t + (i + j + 1)p^r + 1 \leq n \). Then by considering Witt’s Identity
\[
[a, b^{-1}, c]^{b}[h, c^{-1}, a]^{c}[c, a^{-1}, b]^{a} = e
\]
modulo \( G_z \) with
\[
a = g_{s+ip^r}, \quad b = \alpha^{-p^r}, \quad \text{and} \quad c = g_{s+jp^r},
\]
and noting that \( g_{z-1} \neq e \), the result follows.

(4), (5): Using (3) these statements follow by easy inductions. \( \square \)

5.

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 \( a_{i,j} \) modulo \( p \), defined for \( i + j + t + 1 \leq n \). Suppose further that these integers satisfy the following relations:
\[
\begin{align*}
a_{i,j} & \equiv -a_{j,i} \pmod{p} \quad \text{for } i + j + t + 1 \leq n , \\
a_{i,i} & \equiv 0 \pmod{p} \quad \text{for } 2i + t + 1 \leq n , \\
a_{i,j} & \equiv a_{i+1,j} + a_{i,j+1} \pmod{p} \quad \text{for } i + j + t + 2 \leq n , \\
a_{i+d,j} & \equiv a_{i,j} \pmod{p} \quad \text{for } i + j + d + t + 1 \leq n .
\end{align*}
\]

Then the existence of a natural number \( s \) such that \( 2s + d + t \leq n \) and \( a_{s+h,s+h+1} \equiv 0 \pmod{p} \) for \( h = 0, \ldots, \lceil \frac{d}{2} \rceil - 1 \) implies \( a_{i,j} \equiv 0 \pmod{p} \) for all \( i, j \).
Proof. As in the proof of Proposition 7 we see that

\[ a_{r+r} \equiv \sum_{h=1}^{[r+1]/2} (-1)^{r-h-1} \binom{r-h}{h-1} a_{r+h-1} \pmod{p} \quad \text{if } 2i + r + t + 1 \leq n \]

and

\[ a_{i,j} \equiv \sum_{h=0}^{i-i_0} (-1)^{i-i_0} \binom{i-i_0}{h} a_{i_0,j+h} \pmod{p} \quad \text{if } i + j + t + 1 \leq n \text{ and } i, j \geq i_0. \]

(a) We have \( a_{s,s+j} \equiv 0 \pmod{p} \) for \( j \geq 0 \) and \( 2s + j + t + 1 \leq n \): This is clear from (*).

(b) \( a_{i,j} \equiv 0 \pmod{p} \) for \( i, j \geq s \) and \( i + j + t + 1 \leq n \): This is clear from (**) and (a).

(c) Suppose that \( \sigma \in \mathbb{N} \) and \( a_{i,j} \equiv 0 \pmod{p} \) for \( i + j + t + 1 \leq n \) and \( i, j > \sigma - 1 \). Then

\[ a_{s-\sigma,s+1-s-\sigma+1} \equiv -a_{s-\sigma+1,s-\sigma+1} \pmod{p} \]

whence

\[ a_{i,j} \equiv 0 \pmod{p} \quad \text{for } i + j + t + 1 \leq n \text{ and } i, j \geq s - 1. \]

We conclude that \( a_{i,j} \equiv 0 \pmod{p} \) for all \( i, j \).

\[ \square \]

**Theorem 3.** Let \( p \) be an odd prime number and let \( G \) be a straight, concatenated \( p \)-group of order \( p^{v-1} \) and with \( \omega(G) = p^v(p-1) \).

1. If \( n \geq 4p^{v+1} - 2p^v + 1 \) then \( G \) has degree of commutativity

\[ \left[ \frac{1}{2} (n - 4p^{v+1} + 2p^v + 1) \right] \]

2. If \( n \geq 4p^{v+1} - 2p^v + 1 \) then \( c(G) \leq 2p^{v+1} - p^v \).

3. \( c(G) \leq 4p^{v+1} - 2p^v - 2 \).

4. If \( n \leq 12p^{v+1} - 6p^v - 10 \) then \( c(G) \leq 3 \).

**Proof.** (1): Assume \( n \geq 4p^{v+1} - 2p^v + 1 \). Suppose that \( G \) has degree of commutativity \( t \), where \( t \leq \frac{1}{2} (n - 4p^{v+1} + 2p^v - 1) \). Let \( a_{i,j} \) be the associated invariants. We must show that \( a_{i,j} \equiv 0 \pmod{p} \) for all \( i, j \).

Let \( i_0 \in \{1, \ldots, p^v(p-1)\} \) be determined by the condition \( i_0 + t \equiv 0 \pmod{p^v(p-1)} \).

For \( r = 0, \ldots, v \) and \( i, j \in \mathbb{Z} \) such that \( i_0 + ip^r \), \( i_0 + jp^r \geq 1 \) we let \( a_{i,j}^{(r)} \) be the integers modulo \( p \) introduced in Proposition 9 (with \( i_0 = s \)).

We show by induction on \( v - r \) that if \( r \in \{0, \ldots, v\} \) then \( a_{i,j}^{(r)} \equiv 0 \pmod{p} \) for all \( i, j \).

So we suppose that \( r \in \{0, \ldots, v\} \) is given and that \( a_{i,j}^{(r)} \equiv 0 \pmod{p} \) for all \( i, j \) whenever \( r \in \{0, \ldots, v\} \) and \( r > r \).

By Proposition 9, (1), (2), we have the congruence

\[ a_{i,j}^{(r)} a_{k,i+j}^{(r)} + a_{j,k}^{(r)} a_{i,j+k}^{(r)} + a_{k,i}^{(r)} a_{j,k+i}^{(r)} \equiv 0 \pmod{p} \]

when \( 3i_0 + 2t + (i + j + k)p^r + 1 \leq n \). So, we may substitute \( (i, j, k) = (1, 2, 2s - 1) \) for \( 2 \leq s \leq \frac{1}{2} (p-1) \) in (*). If now \( 2 \leq s \leq \frac{1}{2} (p-1) \), and if we have proved
Lemma 3 (with \( a \)). Let \( 1 \leq s < t \leq n \) and the inductional hypothesis. Then

\[
\begin{align*}
a_{2s-1,3}^{(r)} &\equiv -a_{3,2s-1}^{(r)} \equiv (-1)^s \left( \begin{array}{c} s-2 \\ s-3 \end{array} \right) a_{s,s+1}^{(r)} \quad (p), \\
a_{2s-1,2}^{(r)} &\equiv (-1)^s a_{s,s+1}^{(r)} \quad (p), \\
a_{1,2s+1}^{(r)} &\equiv a_{1,2}^{(r)} + (-1)^s \left( \begin{array}{c} s \\ s-1 \end{array} \right) a_{s,s+1}^{(r)} \quad (p), \\
a_{2s-1,s}^{(r)} &\equiv -a_{2,2s-1}^{(r)} \equiv -a_{1,2}^{(r)} \quad (p), \\
a_{2,2s}^{(r)} &\equiv (-1)^s \left( \begin{array}{c} s-1 \\ s-2 \end{array} \right) a_{s,s+1}^{(r)} \quad (p),
\end{align*}
\]

where \( a_{2s-1,3}^{(r)} \) should be interpreted as 0 if \( s = 2 \). Combining these congruences with \((*)\) for \((i,j,k) = (1,2,2s-1)\) we obtain

\[
s(a_{s,s+1}^{(r)})^2 \equiv 0 \quad (p).
\]

So we may conclude that \( a_{s,s+1}^{(r)} \equiv 0 \quad (p) \) for \( s = 2, \ldots, \frac{1}{2}(p-1) \). As \( 2i_0 + t + p^{v+1} + 1 \leq n \), we can then use Proposition 9, (5), to deduce:

\[
(*) \quad a_{0,p}^{(r)} \equiv a_{0,1}^{(r)} + 2a_{1,2}^{(r)} \quad (p).
\]

If now \( r = u \), then \( a_{0,p}^{(r)} = a_{0,1}^{(r)} \quad (p) \) according to Proposition 9, (2). Since \( p \) is odd, \((*)\) then gives \( a_{1,2}^{(r)} \equiv 0 \quad (p) \). So, \( a_{s,s+1}^{(r)} \equiv 0 \quad (p) \) for \( s = 1, \ldots, \frac{1}{2}(p-1) \). Then Lemma 3 (with \( d = p-1 \)) implies \( a_{i,j}^{(r)} \equiv 0 \quad (p) \) for all \( i,j \).

So assume then that \( r < u \). Then \( a_{0,p}^{(r)} \equiv a_{0,1}^{(r+1)} \equiv 0 \quad (p) \) by definition of these numbers and the inductional hypothesis. Then \((*)\) reads:

\[
a_{0,1}^{(r)} + 2a_{1,2}^{(r)} \equiv 0 \quad (p).
\]

On the other hand, considering \((*)\) with \((i,j,k) = (0,1,3)\) gives us:

\[
a_{1,2}^{(r)}(a_{0,1}^{(r)} + a_{1,2}^{(r)}) \equiv 0 \quad (p),
\]

because \( a_{1,3}^{(r)} \equiv a_{1,2}^{(r)} \quad (p), a_{0,3}^{(r)} \equiv a_{0,1}^{(r)} - a_{1,2}^{(r)} \quad (p), \) and \( a_{0,4}^{(r)} \equiv a_{0,1}^{(r)} - 2a_{1,2}^{(r)} \quad (p) \), again by Proposition 9, (5). So, if \( a_{1,2}^{(r)} \neq 0 \quad (p) \) we would deduce \( a_{0,1}^{(r)} \equiv a_{1,2}^{(r)} \equiv 0 \quad (p) \), a contradiction. Hence, \( a_{1,2}^{(r)} \equiv 0 \quad (p) \), and so \( a_{0,1}^{(r)} \equiv 0 \quad (p) \) (again because \( p \) is odd).

Now we substitute \((i,j,k) = (0,1,2s)\) in \((*)\) for \( s = 1, \ldots, \frac{1}{2}p^{v-r}(p-1)-1 \).

If \( 2 \leq s \leq \frac{1}{2}p^{v-r}(p-1)-1 \), and if we have already proved \( a_{s,s+1}^{(r)} \equiv 0 \quad (p) \) for \( 1 \leq \sigma < s \), we use again Proposition 9, (5), as above to obtain the congruence:

\[
(-1)^{s+1} \left( \frac{2s-1}{s-1} \right)(\frac{2s+1}{s+1})(\frac{2s}{s})a_{s,s+1}^{(r)} \equiv 0 \quad (p).
\]

We conclude that \( a_{s,s+1}^{(r)} \equiv 0 \quad (p) \) for \( s = 1, \ldots, \frac{1}{2}p^{v-r}(p-1)-1 \), and hence for \( s = 0, \ldots, \frac{1}{2}p^{v-r}(p-1)-1 \). Noticing that \( 2i_0 + t + p^{v-r}(p-1)+1 \leq n \) we can again use Lemma 3 to deduce that \( a_{i,j}^{(r)} \equiv 0 \quad (p) \) for all \( i,j \). This concludes the induction step.
So, we have \( a_{i,j}^{(0)} \equiv 0 \ (p) \) for all \( i, j \), and hence \( a_{i,j} \equiv 0 \ (p) \) for all \( i, j \), as desired.

(2) Put \( f(v) = 4p^{v+1} - 2p^v - 1 \). Suppose that \( n \geq 4p^{v+1} - 2p^v + 1 \) and that \( n \) is odd. By (1) \( G \) has degree of commutativity \( \frac{1}{2}(n - f(v)) \). Then,

\[
\gamma_k(G) = \{e\} \quad \text{if} \quad k \geq \frac{3n - f(v) - 2}{n - f(v) + 2}
\]

However,

\[
\frac{3n - f(v) - 2}{n - f(v) + 2} \leq 1 + \frac{1}{2}(f(v) + 1) = 1 + (2p^{v+1} - p^v),
\]

when \( n \geq f(u) + 2 \).

If \( n \geq 4p^{v+1} - 2p^v + 2 \) and \( n \) is even, we see in a similar way that \( \gamma_k(G) = \{e\} \) if \( k = 2p^{v+1} - p^v + 1 \).

(3) If \( n \leq 4p^{v+1} - 2p^v \) then \( c(G) \leq 4p^{v+1} - 2p^v - 2 \). Since

\[
4p^{v+1} - 2p^v - 2 \geq 2p^{v+1} - p^v,
\]

the statement then follows from (2).

(4) \( n \geq 4p^{v+1} - 2p^v + 1 \) and

\[
4 \geq \frac{3n - f(v) - 3}{n - f(v) + 1}
\]

where \( f(u) := 4p^{v+1} - 2p^v - 1 \) then we deduce along lines similar to the above reasoning that \( c(G) \leq 3 \). But the second inequality holds for \( n \geq 12p^{v+1} - 6p^v - 10 \), and it is clear that

\[
12p^{v+1} - 6p^v - 10 \geq n \geq 4p^{v+1} - 2p^v + 1.
\]

The desired conclusion follows.

Theorem 4. 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 \( G \) has a normal subgroup of index less than \( u(p, k) \) and of 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 \( G \) is a finite \( p \)-group possessing an automorphism of order \( p^k \) having exactly \( p \) fixed points, then the derived length of \( G \) is less than \( f(p, k) \).

Proof. The first statement follows immediately from Proposition 6, Theorem 1, Theorem 2, and Theorem 3. The second statement follows trivially from the first.

\[
\square
\]

References
DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COPENHAGEN, UNIVERSITETSARKEN 5, DK-2100 COPENHAGEN Ø, DENMARK.

E-mail address: kiming@math.ku.dk