THE GROUP OF AUTOMORPHISMS OF
A CLASS OF FINITE $p$-GROUPS

BY

ARYE JUHÁSZ

Abstract. Let $G$ be a finite $p$-group and denote by $K_i(G)$ the members of the lower central series of $G$. We call $G$ of type $(m, n)$ if (a) $G$ has nilpotency class $m - 1$, (b) $G/K_2(G) \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ and $K_i(G)/K_{i+1}(G) \cong \mathbb{Z}_{p^n}$ for every $i, 2 \leq i \leq n - 1$. In this work we describe the structure of $\text{Aut}(G)$ and certain relations between $\text{Out}(G)$ and $G$.

Introduction. N. Blackburn considered in [1] a special class of finite $p$-groups, the $p$-groups of maximal class. Our aim here is to determine the structure of the automorphism group of a wider class of finite $p$-groups, groups $G$ with nilpotency class $m - 1$, such that $G/K_2(G) \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ and, for $2 \leq i \leq m - 1$, $K_i(G)/K_{i+1}(G) \cong \mathbb{Z}_{p^n}$. We call such groups $G$ of type $(m, n)$. Here $K_i(G)$ denotes the $i$th member of the descending central series of $G$ and $m, n$ are positive natural numbers, $m > 2$. (Thus a $p$-group of maximal class of order $p^m$ is of type $(m, 1)$.) Such groups were dealt with in [2] and independently in [5]. It becomes clear right at the beginning of our investigation that if $G$ is a $p$-group of type $(m, n)$ then $\text{Aut}(G)$ has a normal Sylow $p$-subgroup $P$ and $\text{Aut}(G)/P$ is isomorphic to a subgroup of $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}^2$ (Theorem 1.12). So, naturally, we focus on the structure of $P$ and prove that, roughly, in the splitting of $P$ to three parts by $G \triangle B \triangle P$, the size of $B/G$ is bounded from below by a number which depends on $\mathbb{Z}(G)$ and $G'$ (Theorem 2.3). Under certain conditions this means that $G$ has many outer automorphisms. Here $\overline{G}$ denotes the group of the inner automorphisms of $G$, $B$ stands for the subgroup of $\text{Aut}(G)$ of all automorphisms which fix $G/K_2(G)$ elementwise and $P/B$ is a subgroup of $\text{GL}(2, p^n)$ which is isomorphic to $\text{Aut}(G/K_2(G))$.

In §3 we deal with metabelian $p$-groups of type $(m, n)$. For these groups our results are more precise: We determine the upper and lower central series of $P$ under certain conditions (which are satisfied by metabelian $p$-groups of maximal class) and show that $B/\overline{G}$ has a very similar structure to that of a subgroup of $K_2(G)$. We also give a lower bound for $B/\overline{G}$ in terms of $m, n$ and $p$ (Theorem 3.2). Here we are working in the endomorphism ring of $K_2(G)$ generated by $G/K_2(G)$ and we use an idea of M. Lazard [8] exploited in [6].

We close by §4 with sharpening our results obtained in §§2 and 3 for $p$-groups of maximal class.
Acknowledgements. This work is a part of my doctoral thesis done under the kind supervision of Professor A. Mann. I wish to express my thanks to Professor Mann for his aid during the preparation of it. I am indebted to the referee for pointing out an error in the original version.

0. Notation. We follow the notation of [4, III]. Let $G$ be a finite group. For every $a, b \in G$ define $[a, 0b] = a$ and for every $0 < n \in Z$ define

$$[a, nb] = [[a, (n - 1)b], b].$$

Here $[c, b] = c^{-1}b^{-1}cb$ for every $c, b \in G$. For subsets $X$ and $Y$ of $G$ let $\langle X, Y \rangle$ be the subgroup of $G$ generated by $X$ and $Y$ in $G$ and $[x, y] = \langle [x, y] | x \in X, y \in Y \rangle$. For every $i > 1$ let $K_i(G)$ and $Z_i(G)$ be the $i$th member of the descending and ascending central series of $G$, respectively. Abbreviate $Z_i(G)$ by $Z(G)$ and the nilpotency class of $G$ by $cl(G)$. Denote by $F(G)$ and $\Phi(G)$ Fitting and the Frattini subgroup of $G$, respectively (see [4, III]). Let $p$ be a fixed prime number. For every natural $n$, $\Omega_n(G) = \langle x \in G | x^p^n = 1 \rangle$, $\Omega_n(G) = \langle x^p^n | x \in G \rangle$ and abbreviate the exponent of $G$ by $exp(G)$. $Aut(G)$ stands for the group of automorphisms of $G$ and if $G$ is abelian then $End(G)$ stands for the endomorphism ring of $G$. For every $\sigma \in Aut(G)$ and $x \in G$ we denote the action of $\sigma$ on $x$ by $x^\sigma$ and write $[x, \sigma]$ for $x^{-1}x^\sigma$. These commutators are defined in the semidirect product of $G$ by $Aut(G)$; hence all the rules for commutators hold for them. Write “$H \triangle G$” for “$H$ is a normal subgroup of $G$”.

For every element (subgroup) $x (X)$ of $G$ denote by $x (X)$ the inner automorphism (group) of $G$ induced by $x (X)$. We shall use freely the following identities of commutators [4, III, pp. 253, 254]: For every $a, b, c \in G$:

\begin{align*}
(\alpha) & [a, b^{-1}] = [a, b]^{-b^{-1}}, \\
(\beta) & [a, bc] = [a, c][a, b]c, \\
(\gamma) & [ab, c] = [a, c][b, c], \\
(\delta) & [a, b^{-1}, c][b, c^{-1}, a][c, a^{-1}b]^a = 1 \text{ (Witt’s identity).}
\end{align*}

Finally, we recall the collection formula [4, III, p. 317]: For every $a, b \in G$,

$$(ab)^p^n = a^{p^n}b^{p^n}c_2^{p^n}\ldots c_i^{p^n}\ldots c_{p^n}, \quad c_i \in K_i(\langle a, b \rangle).$$

1. Basic results. Let $G$ be a $p$-group of type $(m, n)$, $m \geq 4$. For $i \geq 2$ define $G_i = K_i(G)$ and for $i = 1$ define $G_1$ by $G_1/G_4 = C_{G_4/G_4}(G_2/G_4)$. If there exists a natural number $k$ such that, for every $i, j \geq 1$, $[G_i, G_j] \leq G_{i+j+k}$, then following N. Blackburn [1], we say that $G$ has degree of commutativity $k$.

We shall need the following basic properties of $p$-groups of type $(m, n)$, which we state without proof. They follow easily from the results of N. Blackburn in [1].

Let $G$ be a $p$-group of type $(m, n)$, $m \geq 4$. Then

(1.1) There exists an element $s_1 \in G$ such that $G_1 = G_2 \langle s_1 \rangle$ and $G = \langle s, s_1 \rangle$, for every $s \in G \setminus G_1\Phi(G)$. If for $i \geq 2$ we define $s_i = [s_{i-1}, s]$ then $G_i = \langle G_{i-1}, s \rangle$. Every element in $G$ can be expressed uniquely by $s^{a_0}s_1^{a_1}\ldots s_i^{a_i}\ldots s_m^{a_m}$, $a_i \in Z$, $0 \leq a_i < p^n$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(1.2) For every $x \in G \setminus G_1 \Phi(G)$, $x^{p^n} \in G_{m-1}$ and $C_G(x) = \langle x \rangle Z(G)$.

(1.3) For every $x \in G \setminus G_1 \Phi(G)$, $[x, G] = G_2$.

(1.4) $Z_i(G) = G_{m-i}$, for $1 \leq i < m - 1$.

(1.5) If $m \leq p + 1$, then $\exp(G_2) = \exp(G/G_{m-1}) = p^n$.

(1.6) If $m \geq p + 2$, then $\mathcal{U}_i(G_i) \leq G_{i+p-1}$ and, for $n = 1$, $\mathcal{U}_i(G_i) = G_{i+p-1}$.

(1.7) If $m \geq p + 2$, then

$$s_i^{p^n} \equiv s_{p^n}^{(p^n)} \mod(G_{p+1}).$$

(1.8) If $G$ is metabelian then $G$ has degree of commutativity $\geq 1$.

(1.9) Let $G$ be metabelian and let $s \in G \setminus G_1 \Phi(G)$ and for $i \geq 1$ let $s_i$ be as defined in (1.1). Then

(a) If $[s_1, s_2] = s_{m-k}^{x_k} \cdots s_{m-1}^{x_{m-1}}$ then $[s_1, s_j] = s_{m-k+i-2}^{x_k} \cdots s_{m-1}^{x_{m-1}}$, for every $i \geq 2$.

(b) The following are defining relations for $G_2$:

- $s_i^{p^n} \cdots s_{i+1}^{p^n} \cdots s_{i+p-1}^{p^n} = 1$, for $i \geq 2$.
- $s_{m+\mu} = 1$, for $\mu \geq 0$ and $[s_i, s_j] = 1$ for $i, j \geq 2$.

(1.10) For every $i \geq 1$, $H_i = \langle G_i, s \rangle$ is of type $(m - i + 1, n)$ and has degree of commutativity $i - 1$.

(1.11) In the sequel we shall work in metabelian $p$-groups of type $(m, n)$. In this case $G/G_2$ acts by conjugation on the abelian group $G_2$ and we have

**Lemma.** Let $G$ be a metabelian $p$-group of type $(m + 2, n)$, $m > 2$, $\phi$ the natural homomorphism $\phi: \text{Aut}(G) \to \text{Aut}(G_2)$. Let $s \in G \setminus G_1 \Phi(G)$ and denote $\alpha = \phi(s)$. Let $R$ be the subring of $\text{End}(G_2)$ generated by $\alpha$. Then

(a) $G_2$ is a cyclic $R$-module, isomorphic to $R$ (as an $R$-module) by $\theta: R \to G_2$, $\theta(r) = s_2^r$.

(b) $R \cong \mathbb{Z}[t]/\langle (t^{p^n} - 1)/(t - 1), (t - 1)^m \rangle$.

(c) $R$ is a completely primary ring with Jacobson radical $J = \langle \alpha - 1, p \rangle$, as the unique maximal ideal of $R$ and $R/J \cong F_p$.

(d) The multiplicative group $U$ of the units of $R$ has $1 + J$ as a Sylow $p$-subgroup.

(e) For every subring $K$ of $R$ which lies in $pJ$, $1 + K \equiv K$ as abelian groups.

(f) If $H$ is a subring of $J$ such that

- $\mathcal{U}_1(1 + H) \leq 1 + pH$ and
- $\mathcal{U}_1(1 + H) = |H/pH|$

then $H \cong 1 + H$.

**Proof.** (a) By (1.9) $G_2$ is a cyclic $R$-module generated by $s_2$. Since $R \subseteq \text{End}(G_2)$, $G_2$ is a faithful $R$-module. Hence $G_2 \cong R$ as $R$-modules.

(b) Since the defining relations of $G_2$ are $\prod_{\mu=0}^{p^n-1} s_i^{\mu} = 1$ for $i \geq 2$ and $s_{m+2} = 1$ by (1.9),

$$s_2^{\sum_{\mu=0}^{p^n-1}(\mu-1)^{p^n}} = 1$$
for every $j \geq 0$ and by part (a) the defining relations of $R$ are

$$
\sum_{\mu=0}^{p^n-1} \left( \frac{p^n}{\mu+1} \right) (\alpha - 1)^{\mu+j} = 0, \quad j \geq 0 \text{ and } (\alpha - 1)^n = 0.
$$

Therefore $R \cong \mathbb{Z}[t]/I$ where

$$
I = \left\langle (t-1)^m, \sum_{\mu=0}^{p^n-1} \left( \frac{p^n}{\mu+1} \right) (t-1)^{\mu+j}, j \geq 0 \right\rangle.
$$

But as

$$
\sum_{\mu=0}^{p^n-1} \left( \frac{p^n}{\mu+1} \right) (\alpha - 1)^{\mu+j} = \alpha \frac{p^n - 1}{\alpha - 1},
$$

$I = \langle (t-1)^m, (t^{p^n} - 1)/(t-1) \rangle$ and the result follows.

(c) and (d) are well-known facts.

(e) It follows by direct calculations that, for $u \in pJ$, $\exp(u)$ and $\ln(1 + u)$ defined in the usual manner are isomorphisms from $pJ$ to $1 + pJ$ and from $1 + pJ$ to $pJ$, respectively. (For a more general setting see [8].)

(f) Since $|1 + H| = |H|$, (B) implies that $|1 + pH| = |pH| = |\Omega_1(1 + H)|$. By (a) this means that $\Omega_1(1 + H) = 1 + pH$. But by part (e) $1 + pH \cong pH$, hence $\Omega_1(1 + H) \cong pH$. Thus $H$ and $1 + H$ are two finite abelian $p$-groups with the same number of generators and the same set of invariants. Consequently $H \cong 1 + H$ as abelian $p$-groups.

(1.12) Finally, we show that the only nontrivial component of $\text{Aut}(G)$ is its Sylow $p$-subgroup.

**Theorem.** Let $G$ be a $p$-group of type $(m, n)$, $m \geq 4$, $p \geq 3$. Denote $A = \text{Aut}(G)$ and let $B$ be a Sylow $p$-subgroup of $A$. Then

(a) $|A| \mid p^{2(\text{mn} - 2) + 1} \cdot (p - 1)^2$.

(b) $B \triangle A$ and $A$ is a splitting extension of $B$ by a $p'$-Hall subgroup $Q$, where $Q$ is isomorphic to a subgroup of $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$.

(c) $A' \leq B$.

(d) $A$ is solvable.

(e) $F(A) = B$.

(f) $m - 2 \leq \text{cl}(B) \leq mn - 1$.

**Proof.** We omit the proof of this theorem, as it is straightforward.

2. The structure of the Sylow $p$-subgroup of $\text{Aut}(G)$. It is well known (e.g. [7, Corollary 1]) that if $G$ is a finite $p$-group then $\text{Aut}(G)$ has the following normal series: $1 \triangle K \triangle \text{Aut}(G)$, where $K$ is the set of all the elements of $\text{Aut}(G)$ which fixes $G/K_2(G)$ elementwise and $\text{Aut}(G)/K$ is isomorphic to the subgroup of all elements $\text{Aut}(G)/K_2(G)$ which can be extended to an automorphism of $G$. Obviously $G \triangle K$.

In Theorem 2.3 we show that for $p$-groups of type $(m, n)$, $K$ is a splitting extension of $G$ by a subgroup of $\text{Aut}(G)$ which fixes a generator of $G$. Also, a lower bound for $|K|$ is given.
A CLASS OF FINITE $p$-GROUPS

(2.1) PROPOSITION. Let $G$ be a $p$-group of type $(m, n)$. Let $G'_1 \leq G_1$ and let $u \in G_{m-i+1} \cap Z(G_1)$, or $u \in G_2$ if $G_2$ is abelian. Define $\sigma: G \to G$ by $\sigma: s \mapsto s$, $\sigma: s_1 \mapsto s_1 u$ and if $x = s^b \prod_{i=1}^{m-1} s_i^{a_i}$, $0 \leq b$, $a_i < p^n$, then $\sigma: x \mapsto x \prod_{i=1}^{m-1} u_i^{a_i}$. Then $\sigma$ is an automorphism of $G$ iff $u_i = [u, (i - 1)s]$, for $i \geq 2$.

PROOF. $\sigma$ is a well-defined map of $G$ on itself. We prove, by induction on $|G|$, that $\sigma$ is an automorphism. Let $G_w$ be the first abelian $G_i$ and denote $H_w = \langle G_w, s \rangle$. Then $H_w$ is a $p$-group of type $(m - w + 1, n)$ by (1.10) and it follows easily from (1.9) that $\sigma_w$, the restriction of $\sigma$ to $H_w$, is an automorphism of $H_w$. Let $H_2 = \langle G_2, s \rangle$ and assume, by induction, that $\sigma_2$ is an automorphism of $H_2$. We prove that $\sigma$ is an automorphism of $G$. By induction $[s_i^o, s_j^o] = [s_i, s_j]^o$ for $i, j \geq 2$.

We show that $[s_i^o, s_j^o] = s_i^{o+1}$ and $[s_i^o, s_j^o] = [s_i, s_j]$. Since $u_i \in Z(G_2)$, $[s_i^o, s_j^o] = [s_i u_i, s_j] = s_i u_i [s_i u_i] = [s_i, u_i][s_i, s_i][s_i, s_i][u_i, u_i][u_i, s_i]$

On the other hand $[s_i, s_j]^o = [s_i, s_j]$. Hence we have to prove

$$[s_i, s_j, \sigma] = [s_i, s_j, \sigma].$$

Assume first that $G_2$ is not abelian. Then by assumption $[s_i, s_j, \sigma] \leq [G'_1, \sigma] \leq G_{1+m-l} = G_1 = 1$. So

$$[s_i, s_j, \sigma] = 1.$$  \hspace{1cm} (1)

On the other hand, if $x \in Z(G_1)$, then $[x, s] \in Z(G_1)$. Consequently $[u_i, s_i] = 1$ for $i > 1$ and

$$[s_i, \sigma, s_j] = 1.$$  \hspace{1cm} (2)

(1) and (2) imply (3).

Assume now that $G_2$ is abelian. Let notation be as in Lemma 1.11 and denote by $\sigma_2$ the restriction of $\sigma$ to $G_2$. Then $\sigma_2 \in R$, by the definition of $\sigma$. Since $s_i$, $[s_i, s_j] \in G_2$, Lemma 1.11(b) implies $[s_i, s_j, \sigma] = [s_i, \phi(s_i), \sigma_2] = s_i^{f(\alpha)g(\alpha)}$, where $f(t)$, $g(t) \in Z[t]$, and $[s_i, \sigma, s_j] = [s_i, \sigma_2, \phi(s_i)] = s_i^{f(\alpha)g(\alpha)}$. Since $R$ is commutative, (3) holds.

Finally, if $v \in G_1 \setminus G_2 \Phi(G_1)$ then by the collection formula

$$((sv)^o)^p = s^{p^n} v^{p^n} \prod_i d_i(s, v),$$

where $d_i(s, v)$ are certain commutators in $s$ and $v$. If $v_1 = v^o$, then since $d_i(s, v)$, $v^{p^n} \in G_2$,

$$((sv)^o)^p = \left( (sv_1)^p = s^{p^n} v^{p^n} \prod_i d_i(s, v_1) = s^{p^n} v^{p^n} \prod_i d_i(s, v), \right.$$

$$((sv)^o)^p = \left( s^{p^n} v^{p^n} \prod_i d_i(s, v) \right)^o = (s^{p^n})^o (v^{p^n})^o \prod_i d_i(s, v).$$

Since $[v, \sigma] = \bar{u} \in G_2$, $(sv)^o \neq (sv)^o \neq (sv)^p = (sv)^o$ and, as $(sv)^o \not\in Z(G)$, $(sv)^o \neq (sv)^o$. Hence $(sv)^o \neq (sv)^o$. But then by (4) $(v^{p^n})^o = (v^{o})^{p^n}$.
and since $G_1/G_2$ is cyclic, this proves that $\sigma \in \text{Aut}(G)$. The other direction follows from Witt's identity with $a = s_1$, $b = s^{-1}$ and $c = \sigma$ in formula (d) of §0.

(2.2) **Proposition.** Let $G$ be a finite $p$-group of type $(m, n)$, $m \geq 4$. Then to every $u \in G_2$ there exists a solution of the equation $[s, x]u[u, x] = 1$ in $x \in G_1$.

**Proof.** We have to prove $u^x = [s, x]$, for some $x \in G_1$. By (1.3) $u = [s, x^{-1}]$ for some $x \in G_1$. So $u^x = [s, x^{-1}]^x = [s, x]^{-x^{-1}}x = [s, x]$, by $0(\alpha)$.

I am indebted to the referee for this short proof.

(2.3) **Theorem.** Let $G$ be a $p$-group of type $(m, n)$, $m \geq 4$, and let $P$ be the Sylow $p$-subgroup of $\text{Aut}(G)$.

Let $A_3 = \{a \in \text{Aut}(G) | [s, a] = 1, [sx, a] \in G_3\}$ and let $B$ be the subgroup of $\text{Aut}(G)$ which fixes $G/G_2$ elementwise. Then

(a) $|A_3| \geq |G_{m-1}/Z(G_1)|$, where $G'_1 \leq G_1$ but $G'_1 \not\leq G_{1-1}$.

(b) $B$ is a splitting extension of $\overline{G}$ by $A_3$.

**Proof.** (a) follows from Proposition 2.1.

(b) It follows from the definitions of $A_3$ and $\overline{G}$ that $A_3 \cap \overline{G} = \{1\}$. Hence it remains to show that $A_3\overline{G} = B$. Obviously $\overline{A_3}\overline{G} \subseteq B$. Let $a \in B$, $[s, a] = u$, $[sx, a] = v$, $u, v \in G_2$. By Proposition 2.2 there is an element $x \in G_1$ such that $[s, x]u[u, x] = 1$. Hence $s^{ox} = (su)^x = s[s, x]u[x, x] = s$ and $s^{ox} = s_vv_1$, where $v_1 = [s, x]u[v, x] \in G_2$. Assume that $v_1 \equiv s_2 \mod G_3$, $0 \leq x < p^n$. Then $\sigma \tilde{x}^{-\alpha}$: $s \rightarrow s$ and $\sigma \tilde{x}^{-\alpha}$: $s \rightarrow [s_1, v_1]^{(s-\alpha)} \equiv s_1s_2^{\alpha}v_1 [v_1, s^{-\alpha}] \equiv s_1s_2^{\alpha} \equiv \mod G_3$, i.e. $\sigma \tilde{x}^{-\alpha} \in A_3$. Therefore $\sigma \in A_3G$. Consequently $B = A_3\overline{G}$, as required.

**Corollary.** Let notation be as in the theorem. If $G$ has degree of commutativity $l$ then $|\text{Aut}(G)/\overline{G}| \geq p^n$, where $t = \min\{m - l - 1, l + 3\}$.

3. **Metabelian $p$-groups of type $(m, n)$**. To prove the main result of this section (Theorem 3.2) we need the following:

(3.1) **Lemma.** Let $G$, $R$ and $\phi$ be as defined in Lemma 1.11. For every $i \geq 3$ let $A_i = \{a \in \text{Aut}(G) | [s, a] = 1, [s_1, a] \in G_1\}$ and let $B = \overline{G}A_3$ as in Theorem 2.3. Assume that $G$ has an automorphism $\sigma$ such that $s^x = ss_1^{-1}$ and $s_1^{-1} \equiv s_1 \mod G_3$ and which induces an automorphism on $R$ such that $x^\tau = x + y + xy$, where $x = \phi(s) - 1$ and $y = \phi(s)^{-1} - 1$. Then for every $i \geq 3$

(a) $\phi(A_i) = 1 + x^{i-1}R$.

(b) If $Z(G_1) = G_{m-k}$ then $C_{G_3}([1 + x^{i-1}, \tau]) \geq G_{m-k-i+2}$, $C_{G_2}([1 + x^{i-1}, \tau]) \not\geq G_{m-k-i+1}$.

(c) $[1 + x^{i-1}, \tau] \in 1 + x^{i+k-2}R \setminus 1 + x^{i+k-1}R$.

(d) If $a \in A_i \setminus A_i+1$ then $[\tau, a] \in \overline{G}_{i-1}A_{i+k-1} \setminus \overline{G}_{i-1}A_{i+k}$, for $i < m - k$ and $[\tau, a] \in \overline{G}_{i-1}$, for $i > m - k$.

**Proof.** (a) Let $a \in A_i$. Then by Proposition 2.1 there exists a $u \in G_{i+1}$ such that $[s_2, a] = u$. Since $G_2$ is a cyclic $R$-module by Lemma 1.11(a), there exists a polynomial $f(t) \in \mathbb{Z}[t]t^{i-1}$ such that $u = s_2^{f(x)}$. We claim that $\phi(a) - 1 + f(x)$. Since $1 + f(x)$ and $\phi(a)$ are $R$-endomorphisms of $G_2$, it suffices to show that
A CLASS OF FINITE $p$-GROUPS

475

\[ s_2^\phi(a) = s_2^{1+f(x)}. \]

But $s_2^\phi(a) = s_2^\alpha = s_2 \cdot s_2^{f(x)} = s_2^{1+f(x)}. \] Hence $\phi(a) = 1 + f(x)$ and $\phi(A_i) \subseteq 1 + x^{i-1}R$. Conversely, let $f(t) \in \mathbb{Z}[t]^{i-1}$ and let $u = s_2^{f(x)}$. Then $u \in G_{i+1}$ and $s_2^{1+f(x)} = s_2 u$. Since for every $u \in G_{i+1}$ there exists an $\alpha \in A_i$ such that $s_2^\alpha = s_2 u$ by Proposition 2.1, $1 + f(x) = \phi(\alpha)$ for some $\alpha \in A_i$. Consequently, $\phi(A_i) = 1 + x^{i-1}R$.

(b) It suffices to show that $j = m - k - i + 2$ is the smallest $j$ such that $s_j^{1+x^{i-1}, r} = s_j$. Denote $\sigma = 1 + x^{i-1}$ for brevity. Then since $\sigma^r \in R$, by definition, $[\sigma, \tau] = \sigma^{-1} \sigma^r = \sigma^{-1} \sigma^{r-1}$, as $R$ is commutative. Hence $s_j^{[\sigma, \tau]} = s_j \Leftrightarrow s_j^{[\sigma, \tau]^{-1}} = 1 \Leftrightarrow s_j^{\sigma^{-1} \sigma^{r-1}} = 1 \Leftrightarrow s_j^{\sigma^{-1} \sigma^{r-1}} = 1$, i.e. $s_j^{[\sigma, \tau]} = s_j \Leftrightarrow s_j^{\sigma^r} = 1$. Now

\begin{align*}
\sigma^r - \sigma &= (x + y + xy)^{i-1} - x^{i-1} = g(x, y)
\end{align*}

and $g(x, y) = y(x - 1) \sum_{\nu=0}^{x-2} \mu(x + y + xy)^\mu$.

To every $j \geq 2$ $s_j^{x^y} = [s_j + a, b_j]$, $a, b \in \mathbb{Z}$. Therefore, if $[s_1, s_2] \equiv s_y^x \mod G_{r+1}$ and $(8, p) = 1$ then $s_j^{x^y} \equiv s_j^{b_j + j+a} \mod G_{b r(r-2)+j+a+1}$, $(e, p) = 1$, by 1.9(b). Hence if $g(x, y) = \sum c_{a,b} x^y b$ and $b(r-2) + j + a$ attains its minimum for a unique pair $(a, b)$ such that $c_{a,b} \equiv o(p)$, then $s_j^{x^y} = s_j$ iff $s_j^{x^y} = s_j$. But in $g(x, y)$ of (*), $b(r-2) + j + a$ obtains its minimal value for $a = i - 2$ and $b = 1$, as $r \geq 4$ by the definition of $G_1$, and for this $(a, b)$, $c_{a,b} = -1$. Therefore $s_j^{[\sigma, \tau]} = s_j$ iff $s_j^{x^y} = s_j$, i.e. $s_j + i-2 \in \mathbb{Z}(G_1)$. Thus $s_{j+i-2} \in G_{m-k}$, $j + i - 2 \geq m - k$ and $j \geq m - k - i + 2$. By the choice of $j$, $j = m - k - i + 2$. Hence $G_{m-k-i+2} \subseteq C_{G_2}\{[1 + x^{i-1}, r]\}$ and $G_{m-k-i+2} \subseteq C_{G_3}\{[1 + x^{i-1}, r]\}$, as required.

(c) If $[1 + x^{i-1}, \tau] \in 1 + x^i R \setminus 1 + x^{i+1} R$ then the smallest $j$ such that $s_j^{1+x^{i-1}, r} = s_j$ is $j = m - l$. Hence by part (b) $m - k - i + 2 = m - l$, i.e. $l = k + i - 2$, as required.

(d) We prove (d) in four steps.

Step I. $[\alpha, \tau] \in G_2 A_3$. To prove this it suffices to show that $s_1^{[\alpha, \tau]} \equiv s \mod G_3$ and $s_1^{[\alpha, \tau]} \equiv s_1 \mod G_3$.

\begin{align*}
(s_1^{[\sigma, \tau]} - 1)^{r-1} &= s_1^{[\sigma, \tau]} - 1 = (s s_1^{-1})^{r-1} = (s s_1^{-1})^{r-1} = (s s_1^{-1} a^{-1})^{r-1} = s_1^{-1} a^{-1} r^{-1}.
\end{align*}

Since $[s, \tau^{-1}] = [s, \tau]^{-1} = s_1^{-1}$ we obtain

\begin{align*}
(s_1^{[\sigma, \tau]} - 1)^{r-1} &= s_1^{[\sigma, \tau]} - 1 = s s_1^{-1} a^{-1} r^{-1}.
\end{align*}

In particular $s_1^{[\sigma, \tau]} - 1 \equiv s \mod G_i$, $i$ defined by assumption.

Step II. $[\alpha, \tau] \in G_2 A_{i+k-1} A_{m-1} \setminus G_2 A_{i+k} A_{m-1}$ for $i + k \leq m - 1$ and $[\alpha, \tau] \in G_2 A_{i+k-1} A_{m-1}$ for $i + k > m - 1$. Let $\tau \in \text{Aut}(G)$ satisfying $[s, \tau] = s_1^{-1}$, $[s_1, \tau] \in G_3$. We show that $\tau$ induces an automorphism on $R$ by

\begin{align*}
\tau: \sum a_i x^i \to \sum a_i (x + y + xy)^i.
\end{align*}

Here $x$ and $y$ are as defined in the lemma. Obviously $\tau$ maps $R$ onto itself; hence by Lemma 1.11(b) it suffices to show that if $y = f(x), f(t) \in \mathbb{Z}[t]$, then

\begin{align*}
t + f(t) + tf(t) &\in I \quad \text{and} \quad \sum_{i=1}^p \left( f^p(t) (t + f(t) + tf(t))^{-1} \right) \in I.
\end{align*}
Here $I = \langle t^m, (1 + t)\rho^s - 1, t \rangle$ and we have written $t$ instead of $t - 1$ in Lemma 1.11(b). As $f(t) \in I^2 R$, by the definition of $s_i$, $t + f(t) + tf(t) \in I R$ and $(t + f(t) + tf(t))^m \in t^m R \leq I$. Finally let $s_i = [s_i, (i - 1)ss_i^{-1}]$ for $i \geq 2$. As $ss_i^{-1} \in G \setminus G_{\Phi}(G)$,

\[
\tilde{s}_2^p \tilde{s}_3^p \tilde{s}_4^p \cdots \tilde{s}_{\rho^n}^p \cdots \tilde{s}_{\rho^n + 1}^p = 1,
\]

by 1.9(a). Thus, if $R_1$ is the subring of $\text{End} G_2$ generated by $\phi(ss_i^{-1})$, then $G_2$ is a faithful cyclic $R_{I-}$ module generated by $s_2$ and

\[
\tilde{s}_2^p \tilde{s}_3^p \tilde{s}_4^p \cdots \tilde{s}_{\rho^n}^p \cdots \tilde{s}_{\rho^n + 1}^p = 1
\]

implies that

\[
\sum_{i=1}^{n} \left( \binom{p^n}{i} \left( \phi\left( ss_i^{-1}\right) - 1 \right)^{i-1} \right) = 0 \quad \text{in } R.
\]

Hence

\[
\left( \sum_{i=1}^{\rho^n} \binom{p^n}{i} x_i^{i-1} \right)^{\tau} = \sum_{i=1}^{\rho^n} \binom{p^n}{i} (x + y + xy)^{i-1}
\]

\[
= \sum_{i=1}^{\rho^n} \binom{p^n}{i} ((x + 1)(y + 1) - 1)^{i-1} = 0
\]

and $\sum_{i=1}^{\rho^n} \binom{p^n}{i} (x + y + xy)^{i-1} = 0$. Therefore by Lemma 1.11(b) the natural homomorphism $\theta: Z[t] \to Z[t]/I$ sends $\sum_{i=1}^{\rho^n} \binom{p^n}{i} (t + f(t) + tf(t))^{i-1}$ to the zero element of $Z[t]/I$ and $I' = I$. Thus, since $\tau$ induces a homomorphism on $Z[t]$, it induces an automorphism on $Z[t]/I$ and consequently on $R$. We claim that $\phi([\alpha, \tau]) \in x^{i+k-2}R \setminus x^{i+k-1}R$. Indeed, as $\tau$ induces an automorphism on $R$, $[1 + x^{i-1}, \tau] \in 1 + x^{i+k-2}R \setminus 1 + x^{i+k-1}R$ by part (c) and, for every $r \in R \setminus xR$, $[1 + x^{i-1}, \tau] \in 1 + x^{i+k-1}R$. (The last assertion follows by induction on $m = \deg f(t)$, where $f(x) = r$, $f(t) \in Z[t]$.) By the definition of $\tau$, $\phi([\alpha, \tau]) = [\phi(\alpha), \tau]$. Consequently $\phi([[\alpha, \tau]]) = [1 + x^{i+k-2}R \setminus 1 + x^{i+k-1}R]$ by parts (a) and (c) and $[\alpha, \tau] \in \phi^{-1}(1 + x^{i+k-2}R) \setminus \phi^{-1}(1 + x^{i+k-1}R) = \bar{G}_2 A_{i+k-1} A_{m-1} - \bar{G}_2 A_{i+k} A_{m-1}$ for $i + k \leq m - 1$ and $[\alpha, \tau] \in \bar{G}_2 A_{i+k-1} A_{m-1} - \bar{G}_2 A_{i+k} A_{m-1}$.

**Step III.** $[\alpha, \tau] \in \bar{G}_{i-1} A_{i+k-1} A_{m-1}$. Let $[\alpha, \tau] = \beta \bar{g}$, $\bar{g} \in \bar{G}_m$, $\beta \in A_{i+k-1} A_{m-1}$. Then $s^{[\alpha, \tau]} = s^{\beta \bar{g}} = s^{\bar{g}}$, as $s^{\beta} = s$. By (1) $s^{[\alpha, \tau]} \equiv s \text{ mod } G_i$. Hence $s^{\bar{g}} \equiv s \text{ mod } G_i$ and this means that $[s, g] \in G_i$. Consequently $g \in G_{i-1}$.

**Step IV.** $[\alpha, \tau] \in \bar{G}_{i-1} A_{i+k-1} \setminus \bar{G}_{i-1} A_{i+k}$ for $i \geq m - k$ and $[\alpha, \tau] \in \bar{G}_{i-1}$ for $i > m - k + 1$. If $i + k - 1 \leq m - 1$ then $A_{i+k-1} \supseteq A_{m-1}$ and nothing has to be proved, by Step III. Hence assume $i + k \geq m + 1$, i.e. $i \geq m - k + 1$. We show that $[A_{m-k+1}, \tau] \subseteq \bar{G}_2$. For this it suffices to show that if $\alpha \in A_{m-k+1}$ then $s^{[\alpha, \tau]} = s_1$; for $[\alpha, \tau] = \beta \bar{g}$, $\bar{g} \in \bar{G}_{m-k}$, and $\beta \in A_{m-1}$ by Step III. Hence $\beta = 1 \Leftrightarrow s^{\beta} = s_1 \Leftrightarrow s^{[\alpha, \tau]} = s_1$, as $g \in G_{m-k} = Z(G_i)$. Let $[s_1, \alpha] = \nu$ and $[s_1, \tau] = \mu$. It follows by induction on $j$ that $[s_j, \tau] = [u, (j - 1)s] \cdot \Pi[x_1, \ldots, x_j]$ where $x_h \in \{s, u, s_r, 1 \leq r \leq j\}$, $\mu \geq j$, and at least two of the $x_h$’s differ from $s$. Since $G$ is metabelian, if $[x_1, \ldots, x_\mu] \neq 1$ then at most one of the $x_h$ is an element of $G_2$. Hence at least one of
the $x_h$ is $s_1$ and as $G$ is metabelian, we may assume $x_\mu = s_1$. But if $\mu \geq m - k + 1$ then $[x_1, \ldots, x_m - 1] \in G_{m-k} = Z(G_1)$; consequently $[x_1, \ldots, x_\mu] = 1$. Therefore, $[s_j, \tau] = [u, (j-1)s]$ for $j \geq m - k + 1$. Consequently, $[v, \tau] = [u, \alpha] = s_1^{g(\alpha)}(x)$, where $f(t), g(t) \in \mathbb{Z}[t]$, $v = s_1^{g(\alpha)}$, $u = s_1^{g(\beta)}$ and $x = \phi(s) - 1$. This implies that $s_1^{\sigma \tau} = (s_1^{v})^{*} = s_1 \cdot v[v, \tau] = s_1 u [u, \alpha] = (s_1 u)^{\alpha} = s_1^{\sigma \tau}$ and $s_1^{[\alpha, \tau]} = s_1$, as required.

(3.2) Theorem. Let $G$ be a metabelian $p$-group of type $(m, n)$, $m \geq 4$, and for every $i \geq 3$ let $A_i = \{\sigma \in \text{Aut}(G) \mid [s, \sigma] = 1 \text{ and } [s_1, \sigma] \in G_1\}$, $A = \{\sigma \in \text{Aut}(G) \mid [s, \sigma] = 1\}$. Then

(a) $A = A_1 \times \langle s \rangle$ is abelian.
(b) $|A_3| = |G_3|$. 
(c) Let $H \triangleleft \mathcal{U}(G_3) \mathcal{U}_2(G_2)$ such that $H' = H$ and let $A_H = \{\sigma \in A \mid [s_2, \sigma] \in H\}$. Then $A_H/A_H \cap A_{m-1} \cong H$.
(d) The Sylow $p$-subgroup $P$ of $\text{Aut}(G)$ is generated by $p^n + 4$ elements.
(e) $K_1(B) = \overline{G}$ and $Z_1(B) = \overline{G}_{m-1} A_{m-1}$. Here $B = \overline{G} \cdot A$.
(f) Assume that $G$ can be embedded in a $p$-group $G_0$ of type $(m + 1, n)$ and let $B_0$ be the set of all the elements of $\text{Aut}(G_0)$ which fix $G_0/K_2(G_0)$ elementwise. If $Z(G_1) = G_1$ then $A_{i-1}(k) + 3 \mathcal{G}_i \leq A_{i-1}(k-1) \cdot \mathcal{G}_{i+1}$ and $Z_1(B_0) = \mathcal{G}_{m-i} - 1 \mathcal{G}_{m-1}$.

Proof. (a) $A = A_3 \times \langle s \rangle$ by the definitions of $A$, $A_3$ and by Theorem 2.3. Hence we show that $A_3$ is abelian. Let $\alpha, \beta \in A_3$, $[s, \alpha] = u$, $[s_2, \beta] = v$. Then $s_1^{\sigma \tau} = (s_1 u)^{\beta}$ and $s_1^{\sigma \tau} = (s_1 v)^{\alpha} = s_1 u \cdot v[v, \tau]$. Hence $s_1^{\sigma \tau} = s_1^{\sigma \tau}$ iff $v, \alpha = [u, \beta]$. We show $[v, \alpha] = [u, \beta]$. Let $R$ be the ring defined in Lemma 1.11; denote $x = \phi(s) - 1$, where $\phi$ is the canonical homomorphism from $\text{Aut}(G)$ to $\text{Aut}(G_2)$. Then for every element $a \in G_2$ there exists a polynomial $f_0(t) \in \mathbb{Z}[t]$ such that $a = s_1^{f_0(x)}$. In particular $v = s_1^{f_0(x)}, u = s_1^{g(\alpha)}$ for suitable $f(t), g(t) \in \mathbb{Z}[t]$. Now $[u, \beta] = [u, \phi(\beta)] = s_1^{g(\alpha)}(\phi(\beta)) = s_1^{g(\alpha)}(\phi(\beta)) = s_1^{g(\alpha)}(\phi(\beta)) = s_1^{[\alpha, \tau]} = [v, \alpha]$, as in the proof of Lemma 3.1(a).

(b) Follows from Theorem 2.3(a).
(c) Let notation be as in Lemma 1.11. Then $\theta(pJ) = \mathcal{U}_1(G_3) \cdot \mathcal{U}_2(G_2)$. Hence if $H \triangleleft \mathcal{U}_1(G_3) \cdot \mathcal{U}_2(G_2)$ then $\theta^{-1}(H) \subseteq 1 + pJ$ and, as $H$ is $s$-invariant, $\theta^{-1}(H) \cong H \cdot 1$ by Lemma 1.11(c). But $1 + \theta^{-1}(H) = \phi(A_H)$. Hence $A_H/\ker \phi \cap A_{m-1} \cong \ker(\phi)$ and $\overline{G}_2 A_{m-1}$ as $\ker(\phi)$. Since $\overline{G}_2 A_{m-1}$ and $\overline{G}_2 A_{m-1} \cong A$.

(d) It is not difficult to see that $A_3$ is generated by $\{s_i \mid s_i \rightarrow s_i, 3 \leq i \leq p^n + 2\}$. Hence $A_3$ is generated by $p^n - 1$ elements and $B = \overline{G} A_3$ is generated by $p^n + 1$ elements. Every $p$-subgroup of $\text{GL}(2, \mathbb{Z}_{p^n})$ can be generated by 3 elements. Hence $P$ is generated by $p^n + 4$ elements.

(e) By Theorem 2.3(b) $B/\overline{G}_1 \cong B$ and by part (a) of Theorem 3.2 $A$ is abelian. Hence $K_2(B) \cong \overline{G}_2$. On the other hand $[\phi(\overline{s}), \phi(A)] = 1$, i.e. $[\overline{s}, A] \cong \overline{G}_2 A_{m-1}$. Therefore as $A$ is abelian, $K_2(B) = [B, B] = [\overline{G}_1 A, \overline{G}_1 A] \cong \overline{G}_2 A_{m-1}$. But obviously $\overline{G}_2 \leq K_2(B)$. Consequently $K_2(B) = \overline{G}_2$. Since $\overline{G}_2, \overline{s}$, we get by induction on $i$ that $K_i(B) = \overline{G}_i$ for $2 \leq i \leq m - 2$. To determine the upper central series of $B$ determine first $Z(B)$. Let $\sigma \in Z(B), \sigma = \overline{g}$.
ARYE JUHASZ

Since $[\hat{s}, \sigma] = [\hat{s}, \hat{g}]\rho$, $[\hat{s}, \hat{g}] = 1$ and $g \in G_{m-2}$. Also, as $G$ has degree of commutativity $\geq 1$ by (1.8) and $\bar{g} \in G_{m-2}$, $[\hat{s}, \rho] = [\hat{s}, \rho] = 1$. This implies that $[s, \rho] \in G_{m-1}$. Consequently $\sigma \in G_{m-2}A_{m-1}$ and $Z(B) \leq G_{m-2}A_{m-1}$. But obviously $G_{m-2}A_{m-1} \leq Z(B)$. Thus $Z(B) = G_{m-2}A_{m-1}$. Since $Z(B)$ is the kernel of the natural homomorphism $\psi: \text{Aut}(G) \rightarrow \text{Aut}(G/G_{m-1})$, we get the results by induction on $cl(G)$.

(f) Since $G$ may be embedded in $G_0$ there exists a $\tau \in \text{Aut}(G)$ such that $s^\tau = ss_{i-1}^{-1}$ ($\tau$ plays here the role of $s_1$ in $G$). Since $\tau \not\in B$ and $B \triangle \text{Aut}(G)$ by Theorem 2.3(b), $\tau$ acts by conjugation on $B$ and

$B_0 = B\langle \tau \rangle$, \quad $[\hat{s}, \tau] = \hat{s}_1$ \quad and \quad $[\hat{s}, \tau] \in G_3$.

We compute $K_2(B_0)$ and then $K_3(B_0)$ for $i \geq 3$ by induction on $i$. Since $B_0/B$ is cyclic by (2), $K_2(B_0) = [B_0, B] = [B, A_3][B, A_3][\tau, A_3] \cdot [\tau, G] A_3 \leq G_1[\tau, A_3]$. By Lemma 3.1(d) $[\tau, A_3] \leq G_{2A_{k+2}}$. Hence $K_2(B_0) \leq G_{1A_{k+2}}$. Since $[\hat{s}, \tau] = \hat{s}_1$, $\hat{G}_1 \leq K_2(B_0)$. Now

$$G_iA_j, B_0 \equiv G_i(A_j, B_0) = [A_j, B_0]G_{i+1} = G_{i+1}[A_j, \langle \tau \rangle B]$$

by Lemma 3.1(d). Therefore,

$$K_{i+1}(B_0) = [K_i(B_0), B_0] = [G_{i-1}A_3 + (i-1)(k-1), B_0] \leq G_{i-1}A_3 + (i-1)(k-1) \wedge G_{i-1}A_3 + (i-1)(k-1)$$

Also, $\hat{G}_i \leq K_{i+1}(B_0)$, as $[\tau, i]$ $\in K_{i+1}(B_0)$.

(h) First we compute $Z(B_0)$. Obviously $Z(B_0) \leq \bar{Z}(B)$ as $Z(B_0) \leq B_0$. Hence $Z(B_0) \leq A_{m-2}\bar{G}_{m-2}$. We show that $Z(B_0) = \bar{G}_{m-2}$. Let $\sigma \in A_{m-1} \cap Z(B_0)$. Then $[s, \sigma] \in G_{m-1}$ and if $[s, \sigma] = z$ then $s = s_{i-1}^{-1}s_1^{-1} = s_{i-1}^{-1}s_1^{-1} = (s_{i-1}^{-1}s_1^{-1})^{-1} = s_{i-1}^{-1}s_1^{-1} = s$. Hence $z = 1$ and $[s, \sigma] = 1$, i.e. $\sigma = 1$. On the other hand $s_{m-2} \in Z(B_0)$ as $s_{m-2}A_{m-2} = s$ and $s_{m-2}A_{m-2} = s$. Consequently $Z(B_0) = \bar{G}_{m-2}$. Next we compute $Z_2(B_0)$. Let $\psi: \text{Aut}(G) \rightarrow \text{Aut}(G/G_{m-1})$ be the natural homomorphism and let $B_j = \psi(B_0)$. Then $\ker \psi = \bar{G}_{m-2}A_{m-1}$ and $\ker \psi \leq Z(B_0) = \psi^{-1}(Z(B_1))$. For, by Lemma 3.1(d) if $\sigma \in A_{m-1}$ then $[\sigma, \tau] \in \bar{G}_{m-2} = Z(B_0)$; hence $\ker \psi = \bar{G}_{m-2}A_{m-1} \leq Z_2(B_0)$. Also $Z_2(B_0) = \{\sigma \in B_0 | [\sigma, \rho] \in \bar{G}_{m-2} \text{ for every } \rho \in B_0\} = \{\sigma \in [\sigma, \rho] \in \bar{G}_{m-2}A_{m-1} = \psi^{-1}(Z(B_1))\}$. By direct calculation $[s_{m-3}, \tau] \in \bar{G}_{m-2} = Z(B_0)$. Hence as $s_{m-3} \in Z(B_0)$, $Z_2(B_0) = \bar{G}_{m-3}A_{m-1} = \psi^{-1}(Z(B_1))$ and $Z_2(B_0) = \psi^{-1}(Z(B_1))$. Thus $B_0/Z_2(B_0) = B_1/Z(B_1)$ and $Z_i(B_0/Z_2(B_0)) = Z_i(B_1/Z(B_1))$. Consequently $Z_i(B_0) = G_{m-1}A_{m-1}$.

4. $p$-groups of maximal class. By definition a $p$-group of maximal class is a $p$-group of type $(m,1)$. In this case $G_i/A_{i+1}$ is of order $p$ for $1 \leq i \leq m-1$ and also $A_i/A_{i+1}$ is of order $p$. This makes it possible to strengthen the results of the previous sections.

(4.1) Proposition. Let $G$ be a $p$-group of type $(m, n)$, $m \geq 4$.

(a) $G$ can be embedded in a $p$-group $H$ of type $(m+1, n)$ if and only if $G$ has an automorphism $\tau$ such that

1. $\tau: s \rightarrow ss_1^{\alpha}, \tau: s \rightarrow s_1u, \alpha \in \mathbb{Z}, 1 \leq \alpha \leq p-1, (\alpha, p) = 1$ and $u \in G_3$.

2. $\tau^{p^\gamma} \in \bar{G}, \tau^{p^\gamma} \not\in \bar{G}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(b) Assume that $G$ has degree of commutativity $k = 1$. If $m \leq p + 1$ and $\tau \in \text{Aut}(G)$ satisfies (1) of part (a), then $\tau$ satisfies (2) as well.

**Proof.** (a) If $G$ is embedded in a $p$-group $H$ of type $(m + 1, n)$ then $H$ is generated by two elements $s$ and $\sigma_1$ with $[s, \sigma_1] = s^{-1}$. So the automorphism induced on $G$ by $\sigma_1$ satisfies (1) and (2) of part (a) of the proposition. Assume that $G$ has an automorphism $\sigma$ which satisfies (1) and (2). Then by (2) and the definition of $\sigma$, $H/G$ is cyclic of order $p^n$. We prove by induction on $|H|$ that $H_{m-i} = G_{m-i-1}$, for $i \geq 0$. $H_m$ is generated by $\{[\sigma, s, x_1, \ldots, x_{m-2}]\}$ where $x_i \in \{\sigma, s\}$. Since $[\sigma, s] \equiv s^a \mod G_2$ and $[s, \tau] \in G_3$, it follows that if one of the $x_i$'s is $\tau$ then $[\sigma, s, x_1, \ldots, x_{m-2}] \equiv \tau G_m = 1$. Hence $H_m = \langle [\sigma, (m-1)s] \rangle = G_{m-1}$. Hence by the induction hypothesis for $G/G_{m-1}$ we get $H_{m-1}/H_m = K_{m-1}(G/G_{m-1}) = G_{m-1}/G_{m-1} = G_{m-1}/H_m$ for every $i \geq 1$. Consequently $H_{m-i} = G_{m-i-1}$ for $i \geq 1$ and $H$ is of type $(m + 1, n)$, by definition.

(b) Since $s^{\nu^{m-1}} = s[s, \nu^{m-1}] = s[s, \nu]^m \mod G_2$ by the collection formula, $s^{\nu^{m-1}} \equiv s^{a_{m-1}} \mod G_2$ for every $\nu$ which satisfies (1) of part (a). Since $[s, g] \in G_2$ by (1.3) this implies that $[s, \bar{g}] \in G_2$; hence $\nu^{m-1} \in G$. Thus we prove $\nu^{m-1} \in G$.

By the collection formula $s^{\nu^m} = s^{[s_1, \nu]} = s^{[s_1, \nu]^{p^m}} \in G$ for every $\nu$. Since $u = [s, \tau] \in G_3$, $[s_1, \tau, \nu] \in [G_3, \tau]$. Now, $s^{c} = [s_1, s]^\tau = [s_1, s^a] = s^{\nu}$ where $\nu \in G_4$ and by induction on $i$ we see that $[s_i, \tau] \in G_{i+2}$. Hence $K_{i+2}([s_1, \tau], \nu) \subseteq G_{i+2}$. In particular, $c_p \in G_{p+2} = 1$ and $s^{c_p} = s^{[s, a]} = s^{[s_1, s^a]} = s^{a_1}$, as $\exp(G_3) = p$. By a similar application of the collection formula we get $s^{\nu^m} = s^{[s_1, \nu]} = s^{a_n}$, and $\nu^{m-1} \in G$, as required.

(4.2) **Theorem.** Let $G$ be a $p$-group of maximal class of order $p^m$, $P$ the Sylow $p$-subgroup of $\text{Aut}(G)$ and $B = \{s \in P | [s, \sigma], [s_1, \sigma] \in G_2\}$.

(a) If $G$ can be embedded in a $p$-group of maximal class $G_0$ of class $m$ then $P = G_0B$, $|P/B| = p$.

(b) If $G/G_{p+1}$ cannot be embedded in a $p$-group of maximal class of order $p^{p+1}$ and $G$ has degree of commutativity $> 1$ then $P = B$.

(c) If $m > 3p + 6$ then $|A_3| \geq p^{(m-3p+8)/2}$ for $p > 3$ and $|A_3| \geq 3^{(m+1)/2}$ for $p = 3$. Here $A_3 = \{s \in B | [s, \sigma] = 1, [s_1, \sigma] \in G_3\}$ and $[a]$ is the integral part of $a$, for every $a \in \mathbb{Q}$.

**Proof.** (a) By (1.1) $P/B$ is isomorphic to a subgroup of

$$\left\{ \left( \begin{array}{c} 1 \\cdot \\cdot \cdot \cdot \\ 0, 1 \end{array} \right) \mid c \in \mathbb{Z}_p \right\}.$$

If $G$ can be embedded in $G_0$ then $B \neq P$ by Proposition 4.1; hence $P = G_0B$ and $|P/B| = p$.

(b) If $G/G_p$ cannot be embedded in a $p$-group of maximal class of order $p^{p+1}$ then $G$ has no automorphism $\sigma$ such that $[s, \sigma] \in G_1/G_2$ and $[s_1, \sigma] \in G_3$, by Proposition 4.1. As every $\sigma \in P/B$ would move $s$ to $ss^a \mod G_2$, this means that $P = B$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(c) Assume that $G$ has degree of commutativity $k$. If $i$ is the smallest $j$ such that 
$[s_2, s_j] = 1$ then $i + k + 1 = m$, i.e. $i = m - k - 1$. For $m \geq 3p - 6, 2k \geq m - 3p + 6$ by [3] or [9]. Hence for $m \geq 3p - 6, i \leq m - 1 - (m - 3p + 6)/2 \leq [(m - 8 + 3p)/2]$. Hence if $i_0 = [(m - 8 + 3p)/2]$ then $G_{i_0} \leq Z(G_1)$ and the result follows by Proposition 2.1.

(4.3) THEOREM. Let $G$ be a metabelian p-group of maximal class of order $p^m$, $m \geq 4$. 
Let $P$ be the Sylow p-subgroup of $\text{Aut}(G)$ and for $i \geq 3$ let $A_i = \{\sigma \in P | [s, \sigma] = 1, [s_1, \sigma] \in G_i\}$. Then

(a) $A_i \cong G_i$ for $i \geq 3$.

(b) $P$ is generated by $p + 1$ elements.

(c) If $G$ can be embedded in a p-group of maximal class of order $p^{m+1}$ then $K_i(P) = \overline{G}_{i-1} A_{(i-1)(k-1)+3}$ and $Z_i(P) = A_{m-i+1}\overline{G}_{m-i-1}$, for $2 \leq i \leq m - 2$.

(d) If $G/P_{p+1}$ cannot be embedded in a p-group of maximal class then $K_i(P) = \overline{G}_i$ and $Z_i(P) = A_{m-i}\overline{G}_{m-i-1}$.

Proof. (a) Let $R, J = J(R)$, $\phi$ and $\theta$ be as in Lemma 1.11, let $x = \phi(\tilde{s}) - 1$ and $H = x^2R$. Then for every $u \in H, u^p \in pH$; for $(x + 1)^p = 1$ implies that $x^p = pxr$, $r \in R$. Therefore if $u = f(x), f(t) = \sum_{i=2}^w a_i t^i, f(t) \in t^2Z[t]$, then $u^p = \sum_{i=2}^w a_i x^i p^i \mod px^2R$; hence $u^p \equiv 0 \mod px^2R$, i.e. $u^p \in pH$. Thus $(1 + u)^p \in 1 + pH$ and $\mathfrak{U}_1(1 + H) \leq 1 + pH$. Since $\theta$ sends $H$ on $G_4$, $H$ is generated as an abelian group, by $x^2, x^3, \ldots , x^p$ by (1.5) and (1.6) and it follows by induction on $|G|$ that $1 + x^2, \ldots , 1 + x^p$ generate $1 + H$. Hence $H \cong 1 + H$ by Lemma 1.11(f). This means that $A_3/A_{m-1} \cong H \cong G_4$. Since $G_4 \cong G_3/G_{m-1}$ by 1.9(b) and (1.10), $G_3/G_{m-1} \cong A_3/A_{m-1}$. We claim that if $\sigma \in A_i/A_{i+1}$ then $|\sigma| = |s_j|, m - 1 \leq i \leq 3$. Indeed, by the collection formula $[s_i, \sigma^p] = [s_i, \sigma]PC^x_1 \cdots c_p$, where $c_j \in K_j(P(s_i, \sigma_1, \sigma)) \leq G_j$. Hence $[s_i, \sigma^p] \equiv [s_i, \sigma] \mod G_{p}G_2(p)$ Since $\mathfrak{U}_i(s_2), G_{2i+1} = G_{2i+1} \mod p - 1, p^i \geq i + p$ for $i \geq 2$, we have $[s_i, \sigma^p] = \mathfrak{U}_i(s_2)^p$. But as $u^p \in G_{i+p-1}/G_{i+p}$ by (1.5), this means that $[s_i, \sigma^p] \in G_{i+p-1}/G_{i+p}$ and our claim follows. In particular, $G_3$ and $A_3$ have the same exponent $p^e$, say, and to every $1 \leq i \leq e, \mathfrak{U}_i(A_3) = A_{m-i(p-1)}$. If $e = 1$ then $A_3$ and $G_3$ are elementary abelian of the same order, hence isomorphic. If $e > 2$, then $G_{m-1}\mathfrak{U}(G_3)$ and by our claim $A_{m-1} \leq \mathfrak{U}_i(A_3)$ for $1 \leq i \leq e - 2$. Thus, $A_3/\mathfrak{U}_i(A_3) \cong G_3/\mathfrak{U}_i(G_3)$ for $1 \leq i \leq e - 1$. But then $\mathfrak{U}_i(A_3) \cong G_3$ for $1 \leq i \leq e - 1$ and as $\exp(A_3) = \exp(G_3) = p^e$ and $|A_3| = |G_3|$ we obtain $A_3 \cong G_3$. By (1.10) this implies $A_i \cong G_i$ for $i \geq 3$.

(b) $A_3$ is generated by $p - 1$ elements. By Theorem 4.2 either $P = \overline{G}A_3$ or $P = \overline{G}A_3(\tau), where [\tau, \tilde{s}] \equiv \tilde{s}_1 \mod \overline{G}_2A_3$. Hence in any case $P$ can be generated by $p - 1 + 2 = p + 1$ elements.

(c) By Theorem 3.2(f) and (d) $Z_i(P) = A_{m+1}\overline{G}_{m-i-1}$ and $\overline{G}_{i-1} \leq K_i(P) \leq A_{i-1}\overline{G}_{i-1}$+$. Since $|G_{i}/G_{i+1}| = p$ for $2 \leq i \leq m - 1$, it follows from Lemma 3.1(d) that $[\tau, A_i] \equiv A_{i+k-1} \mod \overline{G}_{i-1}$, hence $K_i(P) \equiv A_{i-1}\overline{G}_{i-1} \mod \overline{G}_{i-1}$, and the result follows.

(d) By Theorem 4.2(b) $P = A_3\overline{G}$. Hence the result follows from Theorem 3.2(e).
A CLASS OF FINITE $p$-GROUPS

REFERENCES


MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK, COVENTRY CV4 7AL, ENGLAND

Current address: Department of Mathematics, Hebrew University of Jerusalem, Jerusalem, Israel