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) $G/K_2(G) = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ and $K_i(G)/K_{i+1}(G) = \mathbb{Z}_{p^n}$ 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 $2 \leq i \leq m - 1$, $K_i(G)/K_{i+1}(G) = \mathbb{Z}_{p^n}$. 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 $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ (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 $P \triangleleft G \triangleleft P$, the size of $B/G$ is bounded from below by a number which depends on $Z(G)$ and $G'$ (Theorem 2.3). Under certain conditions this means that $G$ has many outer automorphisms. Here $G'$ 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 $B/G$ has a very similar structure to that of a subgroup of $K_2(G)$. We also give a lower bound for $B/G$ 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.

Received by the editors December 19, 1978 and, in revised form, February 18, 1981.
1980 Mathematics Subject Classification. Primary 20D45; Secondary 20D15.
Key words and phrases. Finite $p$-group, automorphism group, metabelian group, power-structure of $p$-groups, commutator-structure of $p$-groups, $p$-groups of maximal class.

© 1982 American Mathematical Society
0002-9947/81/0000-1062/$04.25

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 $[a, ob] = a$ and for every $0 < n \in \mathbb{Z}$ 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 $\text{cl}(G)$. 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 $n$, $\Omega_p(G) = \langle x \in G | x^p = 1 \rangle$, $\Theta_p(G) = \langle x^p^n | x \in G \rangle$ and abbreviate the exponent of $G$ by $\text{exp}(G)$. $\text{Aut}(G)$ stands for the group of automorphisms of $G$ and if $G$ is abelian then $\text{End}(G)$ stands for the endomorphism ring of $G$. For every $\sigma \in \text{Aut}(G)$ 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 $\text{Aut}(G)$; 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) $x \in (X)$ 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 $a, b, c \in G$:

$$(a) \ [a, b^{-1}] = [a, b]^{-1},$$

$$(b) \ [a, bc] = [a, c][a, b]^c,$$

$$(c) \ [ab, c] = [a, c]b[a, c],$$

$$(4) \ [a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}b]^a = 1 \ (\text{Witt's identity}).$$

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

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

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 $G_1/G_4 = C_{G/G_4}(G_2/G_4)$. 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 $s_i = \langle s_{i-1}, s \rangle$ then $G_i = \langle G_i, s \rangle$.

Every element in $G$ can be expressed uniquely by $s^{\alpha_0}s_1^{\alpha_1} \cdots s_i^{\alpha_i} \cdots s_{m-1}^{\alpha_{m-1}}$, $\alpha_i \in \mathbb{Z}$, $0 \leq \alpha_i < p^n$. 
A CLASS OF FINITE $p$-GROUPS

(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) $Z_j(G) = G_{m-i}$, for $1 < i < m - 1$.

(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 $\mathcal{D}_1(G_i) \leq G_{i+p-1}$ and, for $n = 1$, $\mathcal{D}_1(G_i) = G_{i+p-1}$.

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

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

(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 $[s_1, s_2] = s_{m-1}^{s_{m-2}} \cdots s_{m-1}^{s_{m-1}}$ then $[s_1, s_j] = s_{m-1}^{s_{m-2}} \cdots s_{m-1}^{s_{m-1}}$, for every $i \geq 2$.

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

$$\begin{align*}
&\alpha) s_i^{p^n} \cdots s_i^{(p^n)} \cdots s_{i+p-1} = 1, \text{ for } i \geq 2. \\
&\beta) s_i^{m+1} = 1, \text{ for } \mu \geq 0 \text{ and } [s_i, s_j] = 1 \text{ for } i, j \geq 2. 
\end{align*}$$

(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 $(m + 2, n)$, $m \geq 2$, $\phi$ the natural homomorphism $\phi: \text{Aut}(G) \to \text{Aut}(G_2)$. Let $s \in G \setminus \Phi(G)G_1$ 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 $R/J = F_p$.

(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 $pJ$, $1 + K \cong K$ as abelian groups.

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

(a) $\mathcal{D}_1(1 + H) \leq 1 + pH$ and

(b) $|1 + H/\mathcal{D}_1(1 + H)| = |H/pH|$

then $H \cong 1 + H$.

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

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

$$s_2^{\sum_{\mu=0}^{p^{n-1}} (p^n)(\alpha - 1)^{p^j} = 1}$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
for every \( j \geq 0 \) and by part (a) the defining relations of \( R \) are

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

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

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

\( I = \left\langle (t - 1)^m, (t^{p^n} - 1)/(t - 1) \right\rangle \) 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) \( |A| \leq p^2(mn - 2)^{l+1} \cdot (p - 1)^2 \).

(b) \( B \triangleleft A \) 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: \( 1 \triangleleft K \triangleleft \text{Aut}(G) \), 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 \( \overline{G} \cong K \). In Theorem 2.3 we show that for \( p \)-groups of type \( (m, n) \), \( K \) is a splitting extension of \( \overline{G} \) by a subgroup of \( \text{Aut}(G) \) which fixes a generator of \( G \). Also, a lower bound for \( |K| \) is given.
(2.1) Proposition. Let \( G \) be a \( p \)-group of type \((m, n)\). Let \( G_1 \leq G \) and let \( u \in G_{m-1} \cap Z(G_1) \), or \( u \in G_2 \) if \( G_2 \) is abelian. Define \( \sigma : G \to G \) by \( \sigma : s \to s, \sigma : s_1 \to s_1u \) and if \( x = s^b \prod_{i=1}^{m-1} s_1^{a_i}, 0 \leq b, a_i < p^n \), then \( \sigma : x \to x \prod_{i=1}^{m-1} u^{a_i} \). 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 \( G \).

We show that \([s_i^p, s^p] = s_i^{p+1} \) and \([s_i^p, s_1] = [s_i, s_1]^p\). Since \( u_i \in Z(G_2) \), \([s_i^p, s^p] = [s_i u, s^p] = s_i u s [u_i, s_i] = s_i^{p+1} \).

Now \([s_i^p, s_1] = [s_i u, s_1] = [s_i u, s_1] = [s_i, u s] = [s_i, s_1] = [s_i, s] \).

On the other hand \([s_i, s_1]^p = [s_i, s_1][s_i, s_1] \).

Hence we have to prove
\[ [s_i, s_1, s] = [s_i, s, s_1] \]

Assume first that \( G_2 \) is not abelian. Then by assumption \([s_i, s_1, s] = [G_1, \sigma] = G_{l+m-1} = G_1 = 1 \).

(1) \[ [s_i, s_1, s] = 1. \]

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

(2) \[ [s_i, s_1, s] = 1. \]

(1) and (2) imply (*).

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 \([s_i, s_1] \in G_2 \), Lemma 1.11(b) implies \([s_i, s_1, s] = [s_i, s, s_1, s_1] = s_i^{f(\alpha)g(\alpha)} \), where \( f(t), g(t) \in Z[t] \), and \([s_i, s_1, s] = [s_i, s_2, s_1] = s_i^{f(\alpha)g(\alpha)} \). Since \( R \) is commutative, (*) holds.

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

(3) \[ (sv)^{p^n} = s^{p^n}v^{p^n} \prod_{i} d_i(s, v), \]

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

(4) \[ ((sv)^{p^n}) = (sv)^{p^n} \prod_{i} d_i(s, v), \]

Since \([v, s] = u \in G_2 \), \((sv)^{p^n} = (svu)^{p^n} = (sv)^{p^n} \) and, as \((sv)^{p^n} \notin Z(G), (sv)^{p^n} = (sv)^{p^n} \). Hence \((sv)^{p^n} = (sv)^{p^n} \). But then by (4) \( (v^{p^n}) = (v^{p^n}) \).
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 (\delta) of \S 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 $u^x = [x, s]$, for some $x \in G_1$. By (1.3) $u = [s, x^{-1}]$ for some $x \in G_1$. So $u^x = [s, x^{-1}] = [s, x]^{-1} x = [x, s]$, by 0(a).

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

(a) $|A_3| \geq |G_{m-l+1} \cap Z(G_1)|$, where $G_i' \leq G_i$ but $G_i' \not< G_i$.

(b) $B$ is a splitting extension of $G$ by $A_3$.

Proof. (a) follows from Proposition 2.1.

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

Corollary. Let notation be as in the theorem. If $G$ has degree of commutativity $l$ then $|\text{Aut}(G)/\bar{G}| \geq p^\alpha t$, 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 $A_i = \{ \alpha \in \text{Aut}(G) \mid [s, \alpha] = 1, [sx, \alpha] \in G_1 \}$ and let $B = \bar{G} A_3$ as in Theorem 2.3. Assume that $G$ has an automorphism $\tau$ such that $s^\tau = ss^{-1}$ and $s_1^\tau = s_1 \mod G_3$ 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) $\phi(A_1) = 1 + x^{-1}R$.

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

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

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

Proof. (a) Let $\alpha \in A_i$. Then by Proposition 2.1 there exists a $u \in G_{i+1}$ such that $[s_2, \alpha] = u$. Since $G_1$ 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 $\phi(\alpha) = 1 + f(x)$. Since $1 + f(x)$ and $\phi(\alpha)$ are $R$-endomorphisms of $G_2$, it suffices to show that
A CLASS OF FINITE $p$-GROUPS

475

To every $y \neq 2$ if $y = [s, a, b]$, $a, b \in \mathbb{Z}$. Therefore, if $[s_1, s_2] \equiv s^b \mod G_{r+1}$ and $(s, p) = 1$ then $s^{x+y}b = [s_1, s_2] \equiv s^b \mod G_{r+1}$ and $(s, p) = 1$, by 1.9(b). Hence if $g(x, y) = \sum a_{x+y}b$ and $b(r-2) + j + a$ attains its minimum for a unique pair $(a, b)$ such that $c_{a,b} \equiv o(p)$, then $g(x, y) = s_j$ if $j^a b = s_j$. 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 $s_j^a b = s_j$ iff $[s_{j+i-2}, s_j] = 1$, 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 $j \geq n - k - i + 2$. By the choice of $j, i = m - k - i + 2$. Hence $G_{m-k+i+2} \subseteq C_{G_2}(1 + x^{i-1}, \tau)$ and $G_{m-k+i+2} \subseteq C_{G_2}(1 + x^{i-1}, \tau)$, as required.

(c) If $[1 + x^{i-1}, \tau] \in 1 + x^R \setminus 1 + x^{i+1}R$ then the smallest $j$ such that $s_j^1(1 + x^{i-1}, \tau) = s_j$ 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. $[a, \tau] \in G_2 A_3$. To prove this it suffices to show that $s_j^a \equiv s \mod G_3$ and $s_j^a \equiv s \mod G_3$.

In particular $s_j^a \equiv s \mod G_3$. Clearly $s_j^a \equiv s \mod G_3$. This proves Step I.

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

$$\tau: \sum a_i x^i \to \sum a_i (x + y + xy)^i.$$  

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

$$t + f(t) + if(t) \in I \quad \text{and} \quad \sum_{i=1}^{p^a} (p^a)(t + f(t) + if(t))^{i-1} \in I.$$
Here $I = \langle t^m, (1 + t)^{p^s} - 1 \rangle/t$ and we have written $t$ instead of $t - 1$ in Lemma 1.11(b). As $f(t) \in t^2R$, by the definition of $s_i$, $t + f(t) + tf(t) \in tR$ and $(t + f(t) + tf(t))^m \in t^mR \leq I$. Finally let $\bar{s}_i = [s_i, (i - 1)ss_{i-1}^{-1}]$ for $i \geq 2$. As $ss_{i-1}^{-1} \in G \setminus G_1 \Phi(G)$,

$$\bar{s}_2^p \bar{s}_3^p \cdots \bar{s}_j^{p^{n_j-1}} \cdots \bar{s}_{p^n+1}^p = 1,$$

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

$$\bar{s}_2^p \bar{s}_3^p \cdots \bar{s}_j^{p^{n_j-1}} \cdots \bar{s}_{p^n+1}^p = 1$$

implies that

$$\sum_{i=1}^{n} \binom{p^n}{i} \left(\phi\left(\bar{s}_{s_{i-1}}^{-1}\right) - 1\right)^{i-1} = 0 \quad \text{in } R.$$

Hence

$$\left(\sum_{i=1}^{p^n} \binom{p^n}{i} x^{i-1}\right)^\tau = \sum_{i=1}^{p^n} \binom{p^n}{i} (x + y + xy)^{i-1} = \sum_{i=1}^{p^n} \binom{p^n}{i} ((x + 1)(y + 1) - 1)^{i-1} = 0$$

and $\sum_{i=1}^{n} \binom{p^n}{i}(x + y + xy)^{i-1} = 0$. Therefore by Lemma 1.11(b) the natural homomorphism $\theta: Z[t] \to Z[t]/I$ sends $\sum_{i=1}^{pus^n} \left(\binom{p^n}{i} t + f(t) + tf(t)\right)^{i-1}$ 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 $\text{End} G_1$ 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 $f(x) = r, f(t) \in Z[t]$.) But by the definition of $\tau$, $\phi([\alpha, \tau]) = \phi([\alpha, \tau])$. Consequently $\phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau])$. Consequently $\phi([\alpha, \tau]) \in \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau])$. Consequently $\phi([\alpha, \tau]) \in \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau])$. Consequently $\phi([\alpha, \tau]) \in \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau]) = \phi([\alpha, \tau])$. Therefore $s^{[{\alpha, \tau}]} = s^{[{\alpha, \tau}]}$, as $s^{[{\alpha, \tau}]} = s^{[{\alpha, \tau}]}$. By (1) $s^{[{\alpha, \tau}]} \equiv s \mod G_i$. Hence $s^{[{\alpha, \tau}]} \equiv s \mod G_i$ and this means that $[s, g] \in G_i$. Consequently $g \in G_{i-1}$.

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 $[x_1, \ldots, x_{\mu - 1}] \in G_{m - k} = Z(G_1)$; consequently $[x_1, \ldots, x_\mu] = 1$. Therefore, $[s_j, \tau] = [u, (j - 1)s]$ for $j \geq m - k + 1$. Consequently, $[v, \tau] = [u, \alpha] = s_1^{f(x)g(x)}$, where $f(t), g(t) \in \mathbb{Z}[t], v = s_2^{f(x)}, u = s_2^{g(x)}$ and $x = \phi(s) - 1$. This implies that $s_1^{\tau\sigma} = (s_1v)^\tau = s_1u \cdot v[v, \tau] = s_1uv[u, \alpha] = (s_1u)^\alpha = s_1^{\tau\sigma}$ 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 $A_i = \{\sigma \in \text{Aut}(G) | [s, \sigma] = 1 \text{ and } [s_1, \sigma] \in G_i\}, A = \{\sigma \in \text{Aut}(G) | [s, \sigma] = 1\}$. Then

(a) $A = A_3 \times \langle \hat{s} \rangle$ is abelian.
(b) $|A_3| = |G_3|$.
(c) Let $H \leq \mathcal{B}(G_3) \mathcal{B}_2(G_2)$ such that $H^i = H$ and let $A_H = \{\sigma \in A | [s_2, \sigma] \in H\}$. Then $A_H / A_H \cap A_{m - 1} \approx H$.
(d) The Sylow $p$-subgroup $P$ of $\text{Aut}(G)$ is generated by $p^n + 4$ elements.
(e) $K_1(B) = G_1$ and $Z(B) = G_{m - i - 1}A_{m - 1}$. Here $B = G \cdot A_i$.
(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 $Z(G_1) = G_{m - k}$ then $A_{i - (i - 1)(k - 1)}^i < K_1(B_0) < A_{i - (i - 1)(k - 1) + 3} \cdot G_{i - 1}$ and $G_{i - 1}(B_0) = A_{m - i - 1}G_{m - i - 1}$.

**Proof.** (a) $A = A_3 \times \langle \hat{s} \rangle$ by the definitions of $A$, $A_3$, and by Theorem 2.3. Hence we show that $A_3$ is abelian. Let $\alpha, \beta \in A_3, [s, \alpha] = u, [s, \beta] = v$. Then $s_1^{\alpha\beta} = (s_1u)^\beta = s_1uv[u, \beta]$ and $s_1^{\beta\alpha} = (s_1v)^\alpha = s_1uv[v, \alpha]$. Hence $s_1^{\alpha\beta} = s_1^{\beta\alpha}$ 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 $a = s_2^{f_0(x)}$. In particular $v = s_2^{f_0(x)}, u = s_2^{g(x)}$ for suitable $f(t), g(t) \in \mathbb{Z}[t]$. Now $[u, \beta] = [u, \phi(\beta)] = s_2^{f_0(x)\phi(\beta) - 1} = s_2^{g(x)}f_0(x) g(x) = \phi(s) - 1 = [v, \alpha]$, 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 $\theta(pJ) = \mathcal{B}_1(G_3) \cdot \mathcal{B}_2(G_2)$. Hence if $H \leq \mathcal{B}_1(G_3) \cdot \mathcal{B}_2(G_2)$ then $\theta^{-1}(H) \subseteq 1 + pJ$ and, as $H$ is $s$-invariant, $\theta^{-1}(H) \approx 1 + \theta^{-1}(H)$ by Lemma 1.11(c). But $1 + \theta^{-1}(H) = \phi(A_H)$. Hence $A_{m - 1} / \ker \phi \cap A_{m - 1} \approx 1 + \theta^{-1}(H) \approx \theta^{-1}(H) \approx H$ and $H \approx A_{m - 1} / A_H \cap A_{m - 1}$ as $\ker \phi = G_2A_{m - 1}$ and $A_H \leq A$.

(d) It is not difficult to see that $A_3$ is generated by $\{\sigma | \sigma; s_1 \rightarrow s_i, 3 \leq i \leq p^n + 2\}$. Hence $A_3$ is generated by $p^n - 1$ elements and $B = G_1A_3$ is generated by $p^n + 1$ elements. Every $p$-subgroup of $\text{GL}(2, \mathbb{Z}_p)$ can be generated by 3 elements. Hence $P$ is generated by $p^n + 4$ elements.

(e) By Theorem 2.3(b) $B / G_1 \approx A$ and by part (a) of Theorem 3.2 $A$ is abelian. Hence $K_2(B) \approx G_1$. On the other hand $[\phi(s_1), \phi(A)] = 1$, i.e. $[s_1, A] \approx G_2A_{m - 1}$. Therefore as $A$ is abelian, $K_2(B) = [B, B] = G_1A_3 \leq G_2A_{m - 1} = G_2$. But obviously $G_2 \leq K_2(B)$. Consequently $K_2(B) = G_2$. Since $[G_2, s] = G_{i - 1}$ for $i \geq 2$, we get by induction on $i$ that $K_i(B) = G_i$ for $2 \leq i \leq m - 2$. To determine the upper central series of $B$ determine first $Z(B)$. Let $\sigma \in Z(B), \sigma = \bar{g}_p,$
\[ \overline{g} \in \overline{G}, \rho \in A_3. \text{ Since } [s, \sigma] = [\overline{s}, \overline{g}], [s, \overline{g}] = 1 \text{ and } g \in G_{m-2}. \text{ Also, as } G \text{ has degree of commutativity } \geq 1 \text{ by (1.8) and } \overline{g} \in \overline{G}_{m-2}, [s_1, \sigma] = [s_1, \rho] \text{ and } [s_1, \rho] = 1. \text{ This implies that } [s, \rho] \in \overline{G}_{m-1}. \text{ Consequently } \sigma \in \overline{G}_{m-2}A_{m-1} \text{ and } Z(B) \leq \overline{G}_{m-2}A_{m-1}. \text{ But obviously } \overline{G}_{m-2}A_{m-1} \leq Z(B). \text{ Thus } Z(B) = \overline{G}_{m-2}A_{m-1}. \text{ Since } Z(B) \text{ is the kernel of the natural homomorphism } \psi: \text{Aut}(G) \to \text{Aut}(G/G_{m-1}), \text{ we get the results by induction on } cl(G). \]

(f) Since \( G \) may be embedded in \( G_0 \) there exists a \( \tau \in \text{Aut}(G) \) such that \( s^\tau = ss_1^{-1} \) (\( \tau \) plays here the role of \( s_1 \) in \( G \)). Since \( \tau \notin B \) and \( B \triangleleft \text{Aut}(G) \) by Theorem 2.3(b), \( \tau \) acts by conjugation on \( B \) and

\[ B_0 = B\langle \tau \rangle, \quad [\overline{s}, \tau] = \overline{s_1} \quad \text{and} \quad [\overline{s}, \tau] = \overline{s_1} \in G_3. \]

We compute \( K_2(B_0) \) and then \( K_i(B_0) \) for \( i > 3 \) by induction on \( i \). Since \( B_0/B \) is cyclic by (2), \( K_2(B_0) = [B_0, B] = [B, A_3][B, \overline{G}]^\tau[A_3, A_3] \cdot [\tau, \overline{G}]^A_1 \leq \overline{G}_1[A_1, A_3] \). By Lemma 3.1(d) \( \tau, A_3] \leq \overline{G}_2A_{k+2}. \text{ Hence } K_2(B_0) \leq \overline{G}_1A_{k+2}. \text{ Since } [\overline{s}, \tau] = \overline{s_1}^{-1}, \overline{G}_1 \leq K_2(B_0). \text{ Now}

\[ \overline{G}_i A_j, B_0 = \overline{G}_i[A_j, B_0] = [A_j, B_0]\overline{G}_{i+1} = G_{i+1}[A_j, \langle \tau \rangle B] \]

\[ = \overline{G}_{i+1}[A_j, B][A_j, \tau][A_j, \tau, B] \leq G_{i+1}\overline{G}_j A_{j+k-1} \overline{G}_{i+1}\overline{G}_j A_{j+k} \]

by Lemma 3.1(d). Therefore,

\[ K_{i+1}(B_0) = [K_i(B_0), B_0] = \overline{G}_{i+1-1}A_{j+i(k-1)} \leq \overline{G}_{i+1}A_{j+i(k-1)} \]

Also, \( \overline{G}_i \leq K_{i+1}(B_0) \), as \( \tau, \overline{s} \in K_{i+1}(B_0) \).

(h) First we compute \( Z(B_0) \). Obviously \( Z(B_0) \leq Z(B) \) as \( Z(B_0) \leq B_0 \). Hence \( Z(B_0) \leq A_{m-1}\overline{G}_{m-2}. \text{ We show that } Z(B_0) = \overline{G}_{m-2}. \text{ Let } \sigma \in A_{m-1} \cap Z(B_0). \text{ Then}

\[ [s, \sigma] \in G_{m-1} \text{ and if } [s, \sigma] = z \text{ then } s = s^{\sigma^s \sigma^{s_1} \cdots \sigma^{s_{i-1}}} = (s^{s_1^{-1}})^{s^{-1}} = (s^{-1})^{s_1^{-1}} = [s_1^{-1}, \sigma^{-1}] = s \sigma_1^{-1}. \text{ Hence } z = 1 \text{ and } [s, \sigma] = 1, \text{ i.e. } \sigma = 1. \]

On the other hand \( s_{m-2} = Z(B) \) as \( s_{m-2}^{s_{m-2}^{-1} s^{-1}} = s \) and \( s_{m-2}^{s_{m-2}^{-1} s^{-1}} = s_1 \). Consequently \( Z(B_0) = \overline{G}_{m-2}. \text{ Next we compute } Z_2(B_0). \text{ Let } \psi: \text{Aut}(G) \to \text{Aut}(G/G_{m-1}) \) be the natural homomorphism and let \( B_1 = \psi(B_0) \). Then \( \text{Ker } \psi = \overline{G}_{m-2}A_{m-1} \) and \( \text{Ker } \psi = Z(B_0) \leq \psi^{-1}(Z(B_1)). \text{ For, by Lemma 3.1(d) if } \sigma \in A_{m-1} \text{ then } \sigma, \tau \in \overline{G}_{m-2} = Z(B_0); \text{ hence } \overline{G}_{m-2}A_{m-1} \leq Z_2(B_0). \text{ Also } Z_2(B_0) = \{ \sigma \in B_0 \mid [\sigma, \rho] \in \overline{G}_{m-2} \} \leq \{ \sigma \in B_0 \mid [\sigma, \rho] \in \overline{G}_{m-2}A_{m-1} \} = \psi^{-1}(Z(B_1)). \text{ By direct calculation } [s_{m-2}, \tau] \in \overline{G}_{m-2} = Z(B_0). \text{ Hence as } s_{m-3} \in Z(B), \overline{Z}_2(B_0) = \overline{G}_{m-3}A_{m-1} \leq \psi^{-1}(Z(B_1)) \text{ and } Z_2(B_0) \leq \psi^{-1}(Z(B_1)). \text{ Thus } B_0/Z_2(B_0) \cong B_1/Z(B_1) \text{ and } Z_i(B_0/Z_2(B_0)) \cong Z_i(B_1/Z(B_1)). \text{ Consequently } Z_i(B_0) = \overline{G}_{m-i+1}A_{m-i-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 \( G_i/A_i \) is of order \( p \) for \( 1 \leq i < m - 1 \) 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 \mapsto ss_1^\alpha, s_1 \mapsto s_1 u, \text{ where } \alpha \in Z, 1 \leq \alpha \leq p - 1, \alpha, p = 1 \text{ and } u \in G_3. \]

2. \( \tau^p \in \overline{G}, \tau^p \notin \overline{G}. \)
(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 \( s_t \) with \([s, s_t] = s_t^{-1}\). So the automorphism induced on \( G \) by \( s \) satisfies (1) and (2) of part (a) of the proposition. Assume that \( G \) has an automorphism \( \tau \) which satisfies (1) and (2). Then by (2) and the definition of \( \tau \), \( H/G \) is cyclic of order \( p^n \). We prove by induction on \(|H|\) that \( H_{m-i} = G_{m-i-1} \), for \( i \geq 0 \). Hence \( H_m = \langle \{\tau, (m - 1)s\} \rangle = G_{m-1} \). Hence by the induction hypothesis for \( G/G_{m-1} \) we get \( H_{m-1}/H_m = K_{m-i-1}(G/G_{m-1}) = G_{m-i-1}/G_{m-1} = G_{m-i-1}/H_m \) 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 \( s\tau^{p^{m-1}} = s[s, \tau]^{p^{m-1}} \) mod \( G_2 \) by the collection formula, \( s\tau^{p^{m-1}} = s[s, \tau]^{p^{m-1}} \) mod \( G_2 \) for every \( \tau \) which satisfies (1) of part (a). Since \([s, \tau] \in G_2\) by (1.3) this implies that \([s, \tau] \in G_2\); hence \( \tau^{p^{m-1}} \notin G \). Thus we prove \( \tau^{p^{m}} \notin G \).

By the collection formula \( s_{i}^{\tau^{p^{i}}} = s_{1}^{[s_{1}, \tau]^{p^{i}}} = s_{1}[s_{1}, \tau]^{p^{i}} = c_{2}^{(i)} \ldots c_{p^{n}} \), where \( c_{i} \in K_{i}([s_{1}, \tau], \tau) \) for \( i \geq 2 \). Since \( u = [s_{1}, \tau] \in G_{3}, [s_{1}, \tau, \tau] \leq [G_{3}, \tau] \). Now, \( s_{2}^{\tau^{p}} = [s_{1}, s]^{\tau^{p}} = [s_{1}u, ss_{a}] = s_{2} \) where \( p \in G_{4} \) and by induction on \( i \) we see that \( [s_{1}, \tau] \in G_{i+2} \). Hence \( K_{i}([s_{1}, \tau], \tau) \leq G_{i+2} \). In particular, \( c_{p} \in G_{p+2} = 1 \) and \( s_{1}^{\tau^{p}} = s_{1}u^{p} = s_{1} \), as \( \exp(G_{3}) = p^{n} \) by (1.5). By a similar application of the collection formula we get \( s^{\tau^{p}} = s(s_{1})^{\tau^{p}} \) mod \( G_{p} \), by (1.5). We claim that \( \tau^{p^{n}} = s_{p}^{-\beta} \). Indeed, \([s_{1}, s_{p}^{-\beta}] \in G_{p+1} = 1 \) as \( G \) has degree of commutativity \( \geq 1 \) and \([s, s_{p}^{-\beta}] = [s, s_{p-1}]^{-\beta} = [s_{p-1}, s]^{-\beta} = s_{p}^{-\beta} \). Hence with \( \tilde{g} = s_{p}^{-\beta} \) we get \( s\tilde{g} = s^{\tau^{p}}, s\tilde{g} = s^{p} \) and \( \tau^{p^{n}} \in G \), 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 \( B = \{ \sigma \in P \mid [s, \sigma], [s_{1}, \sigma] \in G_{2} \} \).

(a) If \( G \) can be embedded in a \( p \)-group of maximal class \( G_{0} \) of class \( m \) then \( P = G_{0}B, |P/B| = p \).

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

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

**Proof.** (a) By (1.1) \( P/B \) is isomorphic to a subgroup of \( \left\{ \begin{array}{c} 1, c \vspace{1em} \end{array} \right\} c \in \mathbb{Z}_{p} \right\} \).

If \( G \) can be embedded in \( G_{0} \) then \( B \neq P \) by Proposition 4.1; hence \( P = G_{0}B \) 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 \( \tau \) such that \([s, \tau] \in G_{1}/G_{2} \) and \([s_{1}, \tau] \in G_{3} \), by Proposition 4.1. As every \( \tau \in P/B \) would move \( s \) to \( ss_{a} \) mod \( G_{2} \), this means that \( P = B \).
(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 $A_i = \{s \in P | [s, \sigma] = 1, [s_1, \sigma] \in G_i\}$. 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 $G/G_{p+1}$ 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 $x = \phi(s) - 1$ 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 $u = f(x)$, $f(t) = \sum_{i=2}^n a_i t^i$, $f(i) \in i^2Z[i]$, then $u^p = \sum_{i=2}^n a_i x^i p \mod px^2R$; hence $u^p \equiv 0 \mod px^2R$, i.e. $u^p \in pH$. Thus $(1 + u)^p \in 1 + pH$ and $\theta(1 + H) = 1 + pH$. Since $\theta$ sends $H$ on $G_4$, $H$ is generated as an abelian group, by $x^2, x^3, \ldots, x^p$ by (1.6) 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 $A_3/A_{m-1} = H \cong G_4$. Since $G_4 = G_3/G_{m-1}$ by 1.9(b) and (1.10), $G_3/G_{m-1} = A_3/A_{m-1}$. We claim that if $s \in A_{i-1}/A_{i-1}$ then $|s| = |s|$, $m - 1 \leq i \leq 3$. Indeed, by the collection formula $[s_1, \sigma]^p = [s_1, \sigma]^p c_1 \ldots c_p$ where $c_j \in K_j(P), |s_j| = G_{i-1}$. Hence $[s_1, \sigma]^p = [s_1, \sigma]^p \mod G_{i-1}G_{i-1}$. Since $\mathcal{O}_i(G_{i-1}) = G_{2i-1} \cong G_{i-1}$ by (1.5) and $2i + p - 1$, $pi \equiv i + p$ for $i \equiv 2$, we have $[s_1, \sigma]^p \equiv [s_1, \sigma]^p \mod G_{i-1}G_{i-1}$, i.e. $[s_1, \sigma]^p \equiv u^p \mod G_{i-1}G_{i-1}$, where $u = [s_1, \sigma] \in G_{i-1}/G_{i-1}$. But as $u \in G_{i-1}G_{i-1}$ by (1.5), this means that $[s_1, \sigma]^p \in G_{i-1}/G_{i-1}$ and our claim follows. In particular, $G_3$ and $A_3$ have the same exponent $p^e$, say, and to every $1 \leq i \leq e$, $\mathcal{O}_i(A_3) = A_{m-i-1}$ and $G_{m-i-1}$ for $1 \leq i \leq e - 2$. Thus, $G_{m-i-1} \cong G_3$. 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 $P = \overline{G}_3$ or $P = \overline{G}_3$, where $[\tau, \sigma] = s_1$ 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) $Z_i(P) = A_{i-1}\overline{G}_{i-1}$ and $\overline{G}_{i-1}$ is $K_i(P)$ 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 $K_i(P) \equiv A_{i+k-1} \mod \overline{G}_{i-1}$, and the result follows.

(d) By Theorem 4.2(b) $P = A_{3}\overline{G}_3$. Hence the result follows from Theorem 3.2(e).
REFERENCES


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

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use