TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 270, Number 2, April 1982

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) $G/K_2(G) \cong \mathbf{Z}_{p^n} \times \mathbf{Z}_{p^n}$ and $K_i(G)/K_{i+1}(G) \cong \mathbf{Z}_{p^n}$ for every i, $2 \leq i \leq n - 1$. In this work we describe the structure of $\mathrm{Aut}(G)$ and certain relations between $\mathrm{Out}(G)$ 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 $G/K_2(G) \cong \mathbf{Z}_{p^n} \times \mathbf{Z}_{p^n}$ and, for $2 \leq i \leq m - 1$, $K_i(G)/K_{i+1}(G) \cong \mathbf{Z}_{p^n}$. We call such groups G of type (m, n). Here $K_i(G)$ denotes the ith 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 $\mathrm{Aut}(G)$ has a normal Sylow p-subgroup P and $\mathrm{Aut}(G)/P$ is isomorphic to a subgroup of $\mathbf{Z}_{p-1} \times \mathbf{Z}_{p-1}$ (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 $\overline{G} \triangle B \triangle P$, the size of $B/\overline{G}$ is bounded from below by a number which depends on $Z(G_1)$ and G_1' (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 $\mathrm{Aut}(G)$ of all automorphisms which fix $G/K_2(G)$ elementwise and P/B is a subgroup of $\mathrm{GL}(2, p^n)$ which is isomorphic to $\mathrm{Aut}(G/K_2(G))$.

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.

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.

0002-9947/81/0000-1062/$04.25

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 $0 < n \in \mathbf{Z}$ 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 $[x, y] = \langle [x, y] \mid x \in X, y \in Y\rangle$. For every $i > 1$ let $K_i(G)$ and $Z_i(G)$ be the ith member of the descending and ascending central series of G, respectively. Abbreviate $Z_1(G)$ by $Z(G)$ and the nilpotency class of G by $\mathrm{cl}(G)$. 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, $\Omega_n(G) = \langle x \in G \mid x^{p^n} = 1\rangle$, $\mho_n(G) = \langle x^{p^n} \mid x \in G\rangle$ and abbreviate the exponent of G by $\exp(G)$. $\mathrm{Aut}(G)$ stands for the group of automorphisms of G and if G is abelian then $\mathrm{End}(G)$ stands for the endomorphism ring of G. For every $\sigma \in \mathrm{Aut}(G)$ and $x \in G$ we denote the action of σ on x by x^σ and write $[x, \sigma]$ for $x^{-1}x^\sigma$. These commutators are defined in the semidirect product of G by $\mathrm{Aut}(G)$; 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 $\bar{x}$ $(\bar{X})$ 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 $a, b, c \in G$:

(α) $[a, b^{-1}] = [a, b]^{-b^{-1}}$,

(β) $[a, bc] = [a, c][a, b]^c$,

(γ) $[ab, c] = [a, c]^b[b, c]$,

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

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

$$(ab)^{p^n} = a^{p^n}b^{p^n}c_2^{\binom{p^n}{2}}\ldots c_t^{\binom{p^n}{t}}\ldots c_{p^n}, \qquad c_t \in K_t(\langle a, b\rangle).$$

1. Basic results. Let G be a p-group of type (m, n), $m \geqslant 4$. For $i \geqslant 2$ 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 $i, j \geqslant 1$, $[G_i, G_j] \leqslant G_{i+j+k}$, 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), $m \geqslant 4$. 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 $i \geqslant 2$ 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 $s^{\alpha_0}s_1^{\alpha_1}\ldots s_t^{\alpha_t}\ldots s_{m-1}^{\alpha_{m-1}}$, $\alpha_t \in \mathbf{Z}$, $0 \leqslant \alpha_t < p^n$.

(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 $1 < i < m - 1$.
(1.5) If $m \leqslant p + 1$, then $\exp(G_2) = \exp(G/G_{m-1}) = p^n$.
(1.6) If $m \geqslant p + 2$, then $\mho_1(G_i) \leqslant G_{i+p-1}$ and, for $n = 1$, $\mho_1(G_i) = G_{i+p-1}$.
(1.7) If $m \geqslant p + 2$, then

$$s_1^{p^n} \equiv s_p^{\binom{p^n}{p}} \operatorname{mod}(G_{p+1}).$$

(1.8) If G is metabelian then G has degree of commutativity $\geqslant 1$.
(1.9) Let G be metabelian and let $s \in G \setminus G_1\Phi(G)$ and for $i \geqslant 1$ let s_i be as defined in (1.1). Then
(a) If $[s_1, s_2] = s_{m-k}^{x_k} \dots s_{m-1}^{x_1}$ then $[s_1, s_i] = s_{m-k+i-2}^{x_k} \dots s_{m-1}^{x_{i-1}}$, for every $i \geqslant 2$.
(b) The following are defining relations for G_2:

(α) $s_i^{p^n} \dots s_{i+t}^{\binom{p^n}{t+1}} \dots s_{i+p^n-1} = 1$, for $i \geqslant 2$.
(β) $s_{m+\mu} = 1$, for $\mu \geqslant 0$ and $[s_i, s_j] = 1$ for $i, j \geqslant 2$.

(1.10) For every $i \geqslant 1$, $H_i = \langle G_i, s \rangle$ 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 $(m + 2, n)$, $m > 2$, ϕ the natural homomorphism ϕ: $\operatorname{Aut}(G) \to \operatorname{Aut}(G_2)$. Let $s \in G \setminus \Phi(G)G_1$ and denote $\alpha = \phi(\bar{s})$. Let R be the subring of $\operatorname{End}(G_2)$ generated by α. Then*
(a) *G_2 is a cyclic R-module, isomorphic to R (as an R-module) by θ: $R \to G_2$, $\theta(r) = s_2^r$.*
(b) $R \cong \mathbf{Z}[t]/\langle (t^{p^n} - 1)/(t - 1), (t - 1)^m \rangle$.
(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, $1 + K \cong K$ as abelian groups.*
(f) *If H is a subring of J such that*
(α) *$\mho_1(1 + H) \leqslant 1 + pH$ and*
(β) *$|1 + H/\mho_1(1 + H)| = |H/pH|$*
then $H \cong 1 + H$.

PROOF. (a) By (1.9) G_2 is a cyclic R-module generated by s_2. Since $R \leqslant \operatorname{End}(G_2)$, G_2 is a faithful R-module. Hence $G_2 \cong R$ as R-modules.
(b) Since the defining relations of G_2 are $\prod_{\mu=0}^{p^n-1} s_{i+\mu}^{\binom{p^n}{\mu+1}} = 1$ for $i \geqslant 2$ and $s_{m+2} = 1$ by (1.9),

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

for every $j \geqslant 0$ and by part (a) the defining relations of R are

$$\sum_{\mu=0}^{p^n-1} \binom{p^n}{\mu+1} (\alpha-1)^{\mu+j} = 0, \qquad j \geqslant 0 \text{ and } (\alpha-1)^m = 0.$$

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

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

But as

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

$I = \langle (t-1)^m, (t^{p^n}-1)/(t-1) \rangle$ 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 $|1+H| = |H|$, (β) implies that $|1+pH| = |pH| = |\mho_1(1+H)|$. By ($\alpha$) this means that $\mho_1(1+H) = 1+pH$. 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 Aut(G) is its Sylow p-subgroup.

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

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

(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 $\mathbf{Z}_{p-1} \times \mathbf{Z}_{p-1}$.*

(c) $A' \leqslant B$.

(d) *A is solvable.*

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

(f) $m - 2 \leqslant \mathrm{cl}(B) \leqslant mn - 1$.

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

2. The structure of the Sylow p-subgroup of Aut(G). It is well known (e.g. [7, Corollary 1]) that if G is a finite p-group then Aut(G) has the following normal series: $1 \triangle K \triangle \mathrm{Aut}(G)$, where K is the set of all the elements of Aut(G) which fixes $G/K_2(G)$ elementwise and Aut$(G)/K$ is isomorphic to the subgroup of all elements Aut$(G)/K_2(G)$ which can be extended to an automorphism of G. Obviously $\overline{G} \triangle K$. 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 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 $G_1' \leqslant G_l$ and let $u \in G_{m-l+1} \cap Z(G_1)$, or $u \in G_2$ if G_2 is abelian. Define σ: $G \to G$ by σ: $s \to s$, σ: $s_1 \to s_1 u$ and if $x = s^b \prod_{i=1}^{m-1} s_i^{a_i}$, $0 \leqslant b$, $a_i < p^n$, then σ: $x \to x \prod_{i=1}^{m-1} u_i^{a_i}$. Then σ is an automorphism of G iff $u_i = [u, (i-1)s]$, for $i \geqslant 2$.*

PROOF. σ is a well-defined map of G on itself. We prove, by induction on $|G|$, that σ 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 σ_w, the restriction of σ to H_w, is an automorphism of H_w. Let $H_2 = \langle G_2, s \rangle$ and assume, by induction, that σ_2 is an automorphism of H_2. We prove that σ is an automorphism of G. By induction $[s_i^\sigma, s_j^\sigma] = [s_i, s_j]^\sigma$ for $i, j \geqslant 2$.

We show that $[s_i^\sigma, s^\sigma] = s_{i+1}^\sigma$ and $[s_i^\sigma, s_1^\sigma] = [s_i, s_1]^\sigma$. Since $u_i \in Z(G_2)$, $[s_i^\sigma, s^\sigma] = [s_i u_i, s] = s_{i+1}[u_i, s] = s_{i+1} u_{i+1} = s_{i+1}^\sigma$. Now

$$\begin{aligned}[s_i^\sigma, s_1^\sigma] &= [s_i u_i, s_1 u] = [s_i, s_1 u]^{u_i}[u_i, s_1 u_1] = [s_i, u_1][s_i, s_1][u_i, u_1][u_i, s_1] \\ &= [s_i, s_1][u_i, s_1] = [s_i, s_1][s_i, \sigma, s_1].\end{aligned}$$

On the other hand $[s_i, s_1]^\sigma = [s_i, s_1][s_i, s_1, \sigma]$. Hence we have to prove

$$(*) \qquad [s_i, s_1, \sigma] = [s_i, \sigma, s_1].$$

Assume first that G_2 is not abelian. Then by assumption $[s_i, s_1, \sigma] \leqslant [G_1', \sigma] \leqslant G_{l+m-l} = G_m = 1$. So

$$(1) \qquad [s_i, s_1, \sigma] = 1.$$

On the other hand, if $x \in Z(G_1)$, then $[x, s] \in Z(G_1)$. Consequently $[u_i, s_1] = 1$ for $i > 1$ and

$$(2) \qquad [s_i, \sigma, s_1] = 1.$$

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

Assume now that G_2 is abelian. Let notation be as in Lemma 1.11 and denote by σ_2 the restriction of σ to G_2. Then $\sigma_2 \in R$, by the definition of σ. Since s_i, $[s_i, s_1] \in G_2$, Lemma 1.11(b) implies $[s_i, s_1, \sigma] = [s_i, \phi(s_1), \sigma_2] = s_i^{f(\alpha)g(\alpha)}$, where $f(t), g(t) \in \mathbf{Z}[t]$, and $[s_i, \sigma, s_1] = [s_i, \sigma_2, \phi(s_1)] = s_i^{g(\alpha)f(\alpha)}$. Since R is commutative, $(*)$ holds.

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

$$(3) \qquad (sv)^{p^n} = s^{p^n} v^{p^n} \prod_i d_i(s, v),$$

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

$$(4) \qquad \begin{cases} \left((sv)^\sigma\right)^{p^n} = (sv_1)^{p^n} = s^{p^n} v_1^{p^n} \prod_i d_i(s, v_1) = s^{p^n} v_1^{p^n} \prod_i d_i(s, v^\sigma), \\ \left((sv)^{p^n}\right)^\sigma = \left(s^{p^n} v^{p^n} \prod_i d_i(s, v)\right)^\sigma = (s^{p^n})^\sigma (v^{p^n})^\sigma \prod_i d_i(s, v^\sigma). \end{cases}$$

Since $[v, \sigma] = \tilde{u} \in G_2$, $((sv)\sigma)^{p^n} = (sv\tilde{u})^{p^n} = (sv)^{p^n}$ and, as $(sv)^{p^n} \notin Z(G)$, $((sv)^{p^n})^\sigma = (sv)^{p^n}$. Hence $((sv)^\sigma)^{p^n} = ((sv)^{p^n})^\sigma$. But then by (4) $(v^{p^n})^\sigma = (v^\sigma)^{p^n}$

and since G_1/G_2 is cyclic, this proves that $\sigma \in \mathrm{Aut}(G)$. The other direction follows from Witt's identity with $a = s_1$, $b = s^{-1}$ and $c = \sigma$ in formula (δ) of §0.

(2.2) PROPOSITION. *Let G be a finite p-group of type (m, n), $m \geqslant 4$. 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 $u^x = [s, x^{-1}]^x = [s, x]^{-x^{-1} \cdot x} = [x, s]$, 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), $m \geqslant 4$, and let P be the Sylow p-subgroup of* $\mathrm{Aut}(G)$.

Let $A_3 = \{\sigma \in \mathrm{Aut}(G) \mid [s, \sigma] = 1,\ [s_1, \sigma] \in G_3\}$ and let B be the subgroup of $\mathrm{Aut}(G)$ *which fixes G/G_2 elementwise. Then*

(a) $|A_3| \geqslant |G_{m-l+1} \cap Z(G_1)|$, *where $G_1' \leqslant G_l$ but $G_1' \nleqslant G_{l-1}$.*

(b) *B is a splitting extension of $\bar{G}$ 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 $A_3\bar{G} \leqslant B$. Let $\sigma \in B$, $[s, \sigma] = u$, $[s_1, \sigma] = v$, $u, v \in G_2$. By Proposition 2.2 there is an element $x \in G_1$ such that $[s, x]u[u, x] = 1$. Hence $s^{\sigma x} = (su)^x = s[s, x]u[u, x] = s$ and $s_1^{\sigma x} = s_1 v_1$, where $v_1 = [s_1, x]v[v, x] \in G_2$. Assume that $v_1 \equiv s_2^{\alpha} \bmod G_3$, $0 \leqslant \alpha < p^n$. Then $\sigma\bar{x}\bar{s}^{-\alpha}$: $s \to s$ and $\sigma\bar{x}\bar{s}^{-\alpha}$: $s_1 \to [s_1, v_1]^{s(-\alpha)} \equiv s_1 s_2^{-\alpha} v_1 [v_1, s^{-\alpha}] \equiv s_1 s_2^{-\alpha} s_2 \equiv \bmod G_3$, i.e. $\sigma\bar{x}\bar{s}^{-\alpha} \in A_3$. 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* $|\mathrm{Aut}(G)/\bar{G}| \geqslant p^{nt}$, *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 ϕ be as defined in Lemma* 1.11. *For every $i \geqslant 3$ let $A_i = \{\alpha \in \mathrm{Aut}(G) \mid [s, \alpha] = 1,\ [s_1, \alpha] \in G_i\}$ and let $B = \bar{G}A_3$ as in Theorem* 2.3. *Assume that G has an automorphism τ such that $s^{\tau} = ss_1^{-1}$ and $s_1^{\tau} \equiv s_1 \bmod G_3$ and which induces an automorphism on R such that $x^{\tau} = x + y + xy$, where $x = \phi(s) - 1$ and $y = \phi(\bar{s}_1^{-1}) - 1$. Then for every $i \geqslant 3$*

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

(b) *If $Z(G_1) = G_{m-k}$ then $C_{G_2}([1 + x^{i-1}, \tau]) \geqslant G_{m-k-i+2}$, $C_{G_2}([1 + x^{i-1}, \tau]) \ngeqslant G_{m-k-i+1}$ and*

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

(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 $i \leqslant m - k$ 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_2 is a cyclic R-module by Lemma 1.11(a), there exists a polynomial $f(t) \in \mathbf{Z}[t]t^{i-1}$ 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

$s_2^{\phi(\alpha)} = s_2^{1+f(x)}$. But $s_2^{\phi(\alpha)} = s_2^{\alpha} = s_2 u = s_2 \cdot s_2^{f(x)} = s_2^{1+f(x)}$. Hence $\phi(\alpha) = 1 + f(x)$ and $\phi(A_i) \subseteq 1 + x^{i-1}R$. Conversely, let $f(t) \in \mathbf{Z}[t]t^{i-1}$ 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 $s_j^{[1+x^{i-1},\tau]} = s_j$. Denote $\sigma = 1 + x^{i-1}$ for brevity. Then since $\sigma^{\tau} \in R$, by definition, $[\sigma, \tau] = \sigma^{-1}\sigma^{\tau} = \sigma^{\tau}\sigma^{-1}$, as R is commutative. Hence $s_j^{[\sigma,\tau]} = s_j \Leftrightarrow s_j^{[\sigma,\tau]-1} = 1 \Leftrightarrow s_j^{\sigma^{-1}\sigma^{\tau}-1} = 1 \Leftrightarrow s_j^{(\sigma^{\tau}\sigma^{-1}-1)\sigma} = 1 \Leftrightarrow s_j^{\sigma^{\tau}-\sigma} = 1$, i.e. $s_j^{[\sigma,\tau]} = s_j \Leftrightarrow s_j^{\sigma^{\tau}-\sigma} = 1$. Now

$$(*)\qquad \sigma^{\tau} - \sigma = (x + y + xy)^{i-1} - x^{i-1} = g(x, y)$$

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

To every $j \geqslant 2$ $s_j^{x^a y^b} = [s_{j+a}, bs_1]$, $a, b \in \mathbf{Z}$. Therefore, if $[s_1, s_2] \equiv s_r^{\delta} \bmod G_{r+1}$ and $(\delta, p) = 1$ then $s_j^{x^a y^b} \equiv s_{b(r-2)+j+a}^{\varepsilon} \bmod G_{b(r-2)+j+a+1}$, $(\varepsilon, p) = 1$, by 1.9(b). Hence if $g(x, y) = \sum c_{a,b} x^a y^b$ and $b(r-2) + j + a$ attains its minimum for a unique pair (a, b) such that $c_{a,b} \not\equiv o(p)$, then $s_j^{g(x,y)} = s_j$ iff $s_j^{x^a y^b} = s_j$. But in $g(x, y)$ of $(*)$, $b(r-2) + j + a$ obtains its minimal value for $a = i - 2$ and $b = 1$, as $r \geqslant 4$ by the definition of G_1, and for this (a, b), $c_{a,b} = -1$. Therefore $s_j^{[\sigma,\tau]} = s_j$ iff $[s_{j+i-2}, s_1] = 1$, i.e. $s_{j+i-2} \in Z(G_1)$. Thus $s_{j+i-2} \in G_{m-k}$, $j + i - 2 \geqslant m - k$ and $j \geqslant m - k - i + 2$. By the choice of j, $j = m - k - i + 2$. Hence $G_{m-k-i+2} \subseteq C_{G_2}([1 + x^{i-1}, \tau])$ and $G_{m-k-i+1} \nsubseteq C_{G_2}([1 + x^{i-1}, \tau])$, as required.

(c) If $[1 + x^{i-1}, \tau] \in 1 + x^{l}R \setminus 1 + x^{l+1}R$ then the smallest j such that $s_j^{[1+x^{i-1},\tau]} = s_j$ 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. $[\alpha, \tau] \in \bar{G}_2 A_3$.

To prove this it suffices to show that $s^{[\alpha,\tau]} \equiv s \bmod G_3$ and $s_1^{[\alpha,\tau]} \equiv s_1 \bmod G_3$.

$$s^{\alpha\tau\alpha^{-1}\tau^{-1}} = s^{\tau\alpha^{-1}\tau^{-1}} = \left(ss_1^{-1}\right)^{\alpha^{-1}\tau^{-1}} = \left(ss_1^{-1}\left[s_1^{-1}, \alpha^{-1}\right]\right)^{\tau^{-1}}$$
$$= s\left[s, \tau^{-1}\right]s_1^{-\tau^{-1}}\left[s_1^{-1}\alpha^{-1}\right]^{\tau^{-1}}.$$

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

$$(1)\qquad s^{\alpha\tau\alpha^{-1}\tau^{-1}} = s\left[s_1^{-1}, \alpha^{-1}\right]^{-1} \equiv s \bmod G_i, \qquad i \text{ defined by assumption.}$$

In particular $s^{\alpha\tau\alpha^{-1}\tau^{-1}} \equiv s \bmod G_3$. Clearly $s_1^{\alpha\tau\alpha^{-1}\tau^{-1}} \equiv s_1 \bmod G_3$. This proves Step I.

Step II. $[\alpha, \tau] \in \bar{G}_2 A_{i+k-1} A_{m-1} \setminus \bar{G}_2 A_{i+k} A_{m-1}$ for $i + k \leqslant m - 1$ and $[\alpha, \tau] \in \bar{G}_2 A_{i+k-1} A_{m-1}$ for $i + k > m - 1$. Let $\tau \in \operatorname{Aut}(G)$ satisfying $[s, \tau] = s_1^{-1}$, $[s_1, \tau] \in G_3$. We show that τ induces an automorphism on R by

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

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

$$t + f(t) + tf(t) \in I \quad \text{and} \quad \sum_{i=1}^{p^n} \binom{p^n}{i}(t + f(t) + tf(t))^{i-1} \in I.$$

Here $I = \langle t^m, ((1+t)^{p^n} - 1)/t \rangle$ 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_1, $t + f(t) + tf(t) \in tR$ and $(t + f(t) + tf(t))^m \in t^m R \leqslant I$. Finally let $\tilde{s}_i = [s_1, (i-1)ss_1^{-1}]$ for $i \geqslant 2$. As $ss_1^{-1} \in G \setminus G_1\Phi(G)$,

$$\tilde{s}_2^{p^n}\tilde{s}_3^{\binom{p^n}{2}}\ldots\tilde{s}_j^{\binom{p^n}{j-1}}\ldots\tilde{s}_{p^n+1} = 1,$$

by 1.9(α). Thus, if R_1 is the subring of End G_2 generated by $\phi(\overline{ss_1^{-1}})$, then G_2 is a faithful cyclic R_1- module generated by $\tilde{s}_2$ and

$$\tilde{s}_2^{p^n}\tilde{s}_3^{\binom{p^n}{2}}\tilde{s}_j^{\binom{p^n}{j-1}}\ldots\tilde{s}_{p^n+1} = 1$$

implies that

$$\sum_{i=1}^{n} \binom{p^n}{i}\left(\phi\left(\overline{ss_1^{-1}}\right) - 1\right)^{i-1} = 0 \quad \text{in } R.$$

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 $\sum_{i=1}^{p^n} \binom{p^n}{i}(x + y + xy)^{i-1} = 0$. Therefore by Lemma 1.11(b) the natural homomorphism θ: $Z[t] \to Z[t]/I$ sends $\sum_{i=1}^{p^n}\binom{p^n}{i}(t + f(t) + tf(t))^{i-1}$ to the zero element of $Z[t]/I$ and $I^\tau = I$. Thus, since τ 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 τ 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 τ, $\phi([\alpha, \tau]) = [\phi(\alpha), \tau]$. Consequently $\phi([\alpha, \tau]) = [1 + x^{i-1}r, \tau] \in 1 + x^{i+k-2}R \setminus 1 + x^{i+k-1}R$ by parts (a) and (c) and $[\alpha, \tau] \in \phi^{-1}(1 + x^{i+k-2}R) \setminus \phi^{-1}(1 + x^{i+k-1}R) = \overline{G}_2A_{i+k-1}A_{m-1} \setminus \overline{G}_2A_{i+k}A_{m-1}$ for $i + k \leqslant m - 1$ and $[\alpha, \tau] \in \overline{G}_2A_{i+k-1}A_{m-1} \setminus \overline{G}_2A_{i+k}A_{m-1}$.

Step III. $[\alpha, \tau] \in \overline{G}_{i-1}A_{i+k-1}A_{m-1}$. Let $[\alpha, \tau] = \beta\bar{g}$, $\bar{g} \in \overline{G}_2$, $\beta \in A_{i+k-1}A_{m-1}$. Then $s^{[\alpha,\tau]} = s^{\beta\bar{g}} = s^{\bar{g}}$, as $s^\beta = s$. By (1) $s^{[\alpha,\tau]} \equiv s \bmod G_i$. Hence $s^{\bar{g}} \equiv s \bmod G_i$ and this means that $[s, g] \in G_i$. Consequently $g \in G_{i-1}$.

Step IV. $[\alpha, \tau] \in \overline{G}_{i-1}A_{i+k-1} \setminus \overline{G}_{i-1}A_{i+k}$ for $i \leqslant m - k$ and $[\alpha, \tau] \in \overline{G}_{i-1}$ for $i \geqslant m - k + 1$. If $i + k - 1 \leqslant m - 1$ then $A_{i+k-1} \geqslant A_{m-1}$ and nothing has to be proved, by Step III. Hence assume $i + k \geqslant m + 1$, i.e. $i \geqslant m - k + 1$. We show that $[A_{m-k+1}, \tau] \leqslant \overline{G}_2$. For this it suffices to show that if $\alpha \in A_{m-k+1}$ then $s_1^{[\alpha,\tau]} = s_1$; for $[\alpha, \tau] = \bar{g}^\beta$, $\bar{g} \in \overline{G}_{m-k}$, and $\beta \in A_{m-1}$ by Step III. Hence $\beta = 1 \Leftrightarrow s_1^\beta = s_1 \Leftrightarrow s_1^{[\alpha,\tau]} = s_1$, as $g \in G_{m-k} = Z(G_1)$. Let $[s_1, \alpha] = v$ and $[s_1, \tau] = u$. It follows by induction on j that $[s_j, \tau] = [u, (j-1)s] \cdot \Pi[x_1, \ldots, x_\mu]$ where $x_h \in \{s, u, s_r, 1 \leqslant r \leqslant j\}$, $\mu \geqslant j$, 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 $\mu \geqslant m - k + 1$ 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 $j \geqslant m - k + 1$. Consequently, $[v, \tau] = [u, \alpha] = s_2^{f(x)g(x)}$, where $f(t), g(t) \in \mathbf{Z}[t]$, $v = s_2^{f(x)}$, $u = s_2^{g(x)}$ and $x = \phi(\bar{s}) - 1$. This implies that $s_1^{\alpha\tau} = (s_1 v)^\tau = s_1 u \cdot v[v, \tau] = s_1 vu[u, \alpha] = (s_1 u)^\alpha = s_1^{\tau\alpha}$ and $s_1^{[\alpha, \tau]} = s_1$, as required.

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

(a) *$A = A_3 \times \langle \bar{s} \rangle$ is abelian.*

(b) $|A_3| = |G_3|$.

(c) *Let $H \leqslant \mho(G_3)\mho_2(G_2)$ such that $H^s = H$ 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* Aut(G) *is generated by $p^n + 4$ elements.*

(e) *$K_i(B) = \bar{G}_i$ and $Z_i(B) = \bar{G}_{m-i-1} A_{m-1}$. Here $B = \bar{G} \cdot A_3$.*

(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* Aut(G_0) *which fix $G_0/K_2(G_0)$ elementwise. If $Z(G_1) = G_{m-k}$ then $A_{(i-1)\cdot(k-1)+2}\bar{G}_{i-1} < K_i(B_0) \leqslant A_{(i-1)(k-1)+3} \cdot \bar{G}_{i-1}$ and*

(g) $Z_i(B_0) = A_{m-i-1}\bar{G}_{m-i+1}$.

PROOF. (a) $A = A_3 \times \langle \bar{s} \rangle$ by the definitions of A, A_3 and by Theorem 2.3. Hence we show that A_3 is abelian. Let $\alpha, \beta \in A_3$, $[s_1 \alpha] = u$, $[s_1, \beta] = v$. Then $s_1^{\alpha\beta} = (s_1 u)^\beta = s_1 vu[u, \beta]$ and $s_1^{\beta\alpha} = (s_1 v)^\alpha = s_1 uv[v, \alpha]$. 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 $x = \phi(\bar{s}) - 1$, where ϕ is the canonical homomorphism from Aut(G) to Aut(G_2). Then for every element $a \in G_2$ there exists a polynomial $f_0(t) \in \mathbf{Z}[t]$ such that $a = s_2^{f_0(x)}$. In particular $v = s_2^{f(x)}$, $u = s_2^{g(x)}$ for suitable $f(t), g(t) \in \mathbf{Z}[t]$. Now $[u, \beta] = [u, \phi(\beta)] = s_2^{g(x)(\phi(\beta)-1)} = s_2^{g(x)f(x)} = s_2^{f(x)g(x)} = v^{g(x)} = v^{(\phi(\alpha)-1)} = [v, \alpha]$, 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 $\theta(pJ) = \mho_1(G_3) \cdot \mho_2(G_2)$. Hence if $H \leqslant \mho_1(G_3) \cdot \mho_2(G_2)$ then $\theta^{-1}(H) \subseteq 1 + pJ$ and, as H is s-invariant, $\theta^{-1}(H) \cong 1 + \theta^{-1}(H)$ by Lemma 1.11(c). But $1 + \theta^{-1}(H) = \phi(A_H)$. Hence $A_H/\mathrm{Ker}\, \phi \cap A_H \cong 1 + \theta^{-1}(H) \cong \theta^{-1}(H) \cong H$ and $H \cong A_H/A_H \cap A_{m-1}$ as $\mathrm{Ker}\, \phi = \bar{G}_2 A_{m-1}$ and $A_H \leqslant A$.

(d) It is not difficult to see that A_3 is generated by $\{\sigma_i \mid \sigma_i\colon s_1 \to s_1 s_i, 3 \leqslant i \leqslant p^n + 2\}$. Hence A_3 is generated by $p^n - 1$ elements and $B = \bar{G}A_3$ is generated by $p^n + 1$ elements. Every p-subgroup of $\mathrm{GL}(2, \mathbf{Z}_{p^n})$ can be generated by 3 elements. Hence P is generated by $p^n + 4$ elements.

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

$\bar{g} \in \bar{G}$, $\rho \in A_3$. Since $[\bar{s}, \sigma] = [\bar{s}, \bar{g}]^\rho$, $[\bar{s}, \bar{g}] = 1$ and $g \in G_{m-2}$. Also, as G has degree of commutativity $\geqslant 1$ by (1.8) and $\bar{g} \in \bar{G}_{m-2}$, $[\bar{s}_1, \sigma] = [\bar{s}_1, \rho]$ and $[\bar{s}_1, \rho] = 1$. This implies that $[s_1, \rho] \in G_{m-1}$. Consequently $\sigma \in \bar{G}_{m-2}A_{m-1}$ and $Z(B) \leqslant \bar{G}_{m-2}A_{m-1}$. But obviously $\bar{G}_{m-2}A_{m-1} \leqslant Z(B)$. Thus $Z(B) = \bar{G}_{m-2}A_{m-1}$. Since $Z(B)$ is the kernel of the natural homomorphism ψ: $\mathrm{Aut}(G) \to \mathrm{Aut}(G/G_{m-1})$, we get the results by induction on $\mathrm{cl}(G)$.

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

(2) $$B_0 = B\langle\tau\rangle, \quad [\bar{s}, \tau] = \bar{s}_1 \quad \text{and} \quad [\bar{s}_1, \tau] \in G_3.$$

We compute $K_2(B_0)$ and then $K_i(B_0)$ for $i \geqslant 3$ by induction on i. Since B_0/B is cyclic by (2), $K_2(B_0) = [B_0, B] = [B, A_3]^\tau[B, \bar{G}]^\tau[\tau, A_3] \cdot [\tau, \bar{G}]^{A_3} \leqslant \bar{G}_1[\tau, A_3]$. By Lemma 3.1(d) $[\tau, A_3] \leqslant \bar{G}_2 A_{k+2}$. Hence $K_2(B_0) \leqslant \bar{G}_1 A_{k+2}$. Since $[\bar{s}, \tau] = \bar{s}_1^{-1}$, $\bar{G}_1 \leqslant K_2(B_0)$. Now

$$\begin{aligned}\left[\bar{G}_i A_j, B_0\right] &= \left[\bar{G}_i, B_0\right]\left[A_j, B_0\right] = \left[A_j, B_0\right]\bar{G}_{i+1} = G_{i+1}\left[A_j, \langle\tau\rangle B\right] \\ &= \bar{G}_{i+1}\left[A_j, B\right]\left[A_j, \tau\right]\left[A_j, \tau, B\right] \leqslant \bar{G}_{i+1}\bar{G}_j A_{j+k-1} \setminus \bar{G}_{i+1}\bar{G}_j A_{j+k}\end{aligned}$$

by Lemma 3.1(d). Therefore,

$$K_{i+1}(B_0) = \left[K_i(B_0), B_0\right] = \left[\bar{G}_{i-1}A_{3+(i-1)(k-1)}, B_0\right] \leqslant \bar{G}_i A_{3+i(k-1)} \setminus \bar{G}_i A_{2+i(k-1)}.$$

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

(h) First we compute $Z(B_0)$. Obviously $Z(B_0) \leqslant Z(B)$ as $Z(B_0) \leqslant B_0$. Hence $Z(B_0) \leqslant A_{m-1}\bar{G}_{m-2}$. We show that $Z(B_0) = \bar{G}_{m-2}$. Let $\sigma \in A_{m-1} \cap Z(B_0)$. Then $[s_1, \sigma] \in G_{m-1}$ and if $[s, \sigma] = z$ then $s = s^{\sigma\tau\sigma^{-1}\tau^{-1}} = s^{\tau\sigma^{-1}\tau^{-1}} = (ss_1^{-1})^{\sigma^{-1}\tau^{-1}} = (ss_1^{-1}[s_1^{-1}, \sigma^{-1}])^{\tau^{-1}} = s[s_1^{-1}, \sigma^{-1}]^{\tau^{-1}} = sz$. Hence $z = 1$ and $[s_1, \sigma] = 1$, i.e. $\sigma = 1$. On the other hand $\bar{s}_{m-2} \in Z(B_0)$ as $s^{\bar{s}_{m-2}\tau\bar{s}_{m-2}^{-1}\tau^{-1}} = s$ and $s_1^{\bar{s}_{m-2}\tau\bar{s}_{m-2}^{-1}\tau^{-1}} = s_1$. Consequently $Z(B_0) = \bar{G}_{m-2}$. Next we compute $Z_2(B_0)$. Let ψ: $\mathrm{Aut}(G) \to \mathrm{Aut}(G/G_{m-1})$ be the natural homomorphism and let $B_1 = \psi(B_0)$. Then $\mathrm{Ker}\,\psi = \bar{G}_{m-2}A_{m-1}$ and $\mathrm{Ker}\,\psi \leqslant Z_2(B_0) \leqslant \psi^{-1}(Z(B_1))$. For, by Lemma 3.1(d) if $\sigma \in A_{m-1}$ then $[\sigma, \tau] \in \bar{G}_{m-2} = Z(B_0)$; hence $\mathrm{Ker}\,\psi = \bar{G}_{m-2}A_{m-1} \leqslant Z_2(B_0)$. Also $Z_2(B_0) = \{\sigma \in B_0 \mid [\sigma, \rho] \in \bar{G}_{m-2}$ for every $\rho \in B_0\} \leqslant \{\sigma \in B_0 \mid [\sigma, \rho] \in \bar{G}_{m-2}A_{m-1}\} = \psi^{-1}(Z(B_1))$. By direct calculation $[\bar{s}_{m-3}, \tau] \in \bar{G}_{m-2} = Z(B_0)$. Hence as $\bar{s}_{m-3} \in Z(B)$, $Z_2(B_0) = \bar{G}_{m-3}A_{m-1} = \psi^{-1}(Z(B_1))$ and $Z_2(B_0) = \psi^{-1}(Z(B_1))$. Thus $B_0/Z_2(B_0) \cong B_1/Z(B_1)$ and $Z_i(B_0/Z_2(B_0)) \cong Z_i(B_1/Z(B_1))$. Consequently $Z_i(B_0) = \bar{G}_{m-i+1}A_{m-i-1}$.

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/G_{i+1} is of order p for $1 \leqslant i \leqslant m-1$ 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), $m \geqslant 4$.*

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

(1) τ: $s \to ss_1^\alpha$, τ: $s_1 \to s_1 u$, *where* $\alpha \in \mathbf{Z}$, $1 \leqslant \alpha \leqslant p-1$, $(\alpha, p) = 1$ *and* $u \in G_3$.

(2) $\tau^{p^n} \in \bar{G}$, $\tau^{p^{n-1}} \notin \bar{G}$.

(b) *Assume that G has degree of commutativity* $k = 1$. *If* $m \leqslant p + 1$ *and* $\tau \in \mathrm{Aut}(G)$ *satisfies* (1) *of part* (a), *then* τ *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 σ_1 with $[s, \sigma_1] = s_1^{-1}$. So the automorphism induced on G by σ_1 satisfies (1) and (2) of part (a) of the proposition. Assume that G has an automorphism τ which satisfies (1) and (2). Then by (2) and the definition of τ, H/G is cyclic of order p^n. We prove by induction on $|H|$ that $H_{m-i} = G_{m-i-1}$, for $i \geqslant 0$. H_m is generated by $\{[\tau, s, x_1, \ldots, x_{m-2}]\}$ where $x_t \in \{\tau, s\}$. Since $[\tau, s] \equiv s_1^{\alpha} \bmod G_2$ and $[s_1, \tau] \in G_3$, it follows that if one of the x_i's is τ then $[\tau, s, x_1, \ldots, x_{m-2}] \in G_m = 1$. 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 $i \geqslant 1$. Consequently $H_{m-i} = G_{m-i-1}$ for $i \geqslant 1$ and H is of type $(m + 1, n)$, by definition.

(b) Since $s^{\tau^{p^{n-1}}} = s[s, \tau^{p^{n-1}}] = s[s, \tau]^{p^{n-1}} \bmod G_2$ by the collection formula, $s^{\tau^{p^{n-1}}} \equiv ss_1^{\alpha p^{n-1}} \bmod G_2$ for every τ 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 $\tau^{p^{n-1}} \notin \bar{G}$. Thus we prove $\tau^{p^n} \in \bar{G}$.

By the collection formula $s_1^{\tau^{p^n}} = s_1[s_1, \tau^{p^n}] = s_1[s_1\tau]^{p^n} c_2^{\binom{p^n}{2}} \ldots c_{p^n}$, where $c_i \in K_i(\langle[s_1, \tau], \tau\rangle)$ for $i \geqslant 2$. Since $u = [s_1, \tau] \in G_3$, $[s_1, \tau, \tau] \leqslant [G_3, \tau]$. Now, $s_2^{\tau} = [s_1, s]^{\tau} = [s_1 u, ss_1^{\alpha}] = s_2 v$ where $v \in G_4$ and by induction on i we see that $[s_i, \tau] \in G_{i+2}$. Hence $K_i(\langle[s_1, \tau], \tau\rangle) \leqslant G_{i+2}$. In particular, $c_p \in G_{p+2} = 1$ and $s_1^{\tau^{p^n}} = s_1 u^{p^n} = s_1$, as $\exp(G_3) = p^n$ by (1.5). By a similar application of the collection formula we get $s^{\tau^{p^n}} = s(s_1^{\alpha})^{p^n} = ss_p^{\beta}$, by (1.5). We claim that $\tau^{p^n} = \bar{s}_{p-1}^{-\beta}$. Indeed, $[s_1, \bar{s}_{p-1}^{-\beta}] \in G_{p+1} = 1$ as G has degree of commutativity $\geqslant 1$ and $[s, \bar{s}_{p-1}^{-\beta}] = [s, \bar{s}_{p-1}]^{-\beta} = [s_{p-1}, s]^{\beta} = s_p^{\beta}$. Hence with $\bar{g} = \bar{s}_{p-1}^{-\beta}$ we get $s^{\bar{g}} = s^{\tau^{p^n}}$, $s_1^{\bar{g}} = s_1^{\tau^{p^n}}$ and $\tau^{p^n} \in \bar{G}$, as required.

(4.2) THEOREM. *Let G be a p-group of maximal class of order* p^m, *P the Sylow p-subgroup of* $\mathrm{Aut}(G)$ *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* $P = \bar{G}_0 B$, $|P/B| = p$.

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

(c) *If* $m \geqslant 3p + 6$ *then* $|A_3| \geqslant p^{[(m-3p+8)/2]}$ *for* $p > 3$ *and* $|A_3| \geqslant 3^{[(m+1)/2]}$ *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* $a \in \mathbf{Q}$.

PROOF. (a) By (1.1) P/B is isomorphic to a subgroup of

$$\left\{\begin{pmatrix} 1, c \\ 0, 1 \end{pmatrix} \mid c \in \mathbf{Z}_p\right\}.$$

If G can be embedded in G_0 then $B \neq P$ by Proposition 4.1; hence $P = \bar{G}_0 B$ 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 τ 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 $ss_1^{\alpha} \bmod G_2$, 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 $m \geqslant 3p - 6$, $2k \geqslant m - 3p + 6$ by [3] or [9]. Hence for $m \geqslant 3p - 6$, $i \leqslant m - 1 - (m - 3p + 6)/2 \leqslant [(m - 8 + 3p)/2]$. Hence if $i_0 = [(m - 8 + 3p)/2]$ then $G_{i_0} \leqslant Z(G_1)$ 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, $m \geqslant 4$. Let P be the Sylow p-subgroup of* $\mathrm{Aut}(G)$ *and for $i \geqslant 3$ let $A_i = \{\sigma \in P \mid [s, \sigma] = 1, [s_1, \sigma] \in G_i\}$. Then*

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

(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 $K_i(P) = \bar{G}_{i-1}A_{(i-1)(k-1)+3}$ and $Z_i(P) = A_{m-i+1}\bar{G}_{m-i-1}$, for $2 \leqslant i \leqslant m - 2$.*

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

PROOF. (a) Let R, $J = J(R)$, ϕ and θ be as in Lemma 1.11, let $x = \phi(\bar{s}) - 1$ 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 $u^p \equiv \sum_{i=2}^{w} a_i^p x^{ip} \bmod px^2R$; hence $u^p \equiv 0 \bmod px^2R$, i.e. $u^p \in pH$. Thus $(1 + u)^p \in 1 + pH$ and $\mho_1(1 + H) \leqslant 1 + pH$. Since θ 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 $|\sigma| = |s_i|$, $m - 1 \leqslant i \leqslant 3$. Indeed, by the collection formula $[s_1, \sigma^p] = [s_1, \sigma]^p c_2^{\binom{p}{2}} \ldots c_p$ where $c_j \in K_j(\langle [s_1, \sigma], \sigma \rangle) \leqslant G_{ij}$. Hence $[s_1, \sigma^p] \equiv [s_1, \sigma]^p \bmod G_{ip}\mho(G_{2i})$. Since $\mho_1(G_{2i}) = G_{2i+p-1}$ by (1.5) and $2i + p - 1$, $pi \geqslant i + p$ for $i \geqslant 2$, we have $[s_1, \sigma^p] \equiv [s_1, \sigma]^p \bmod G_{i+p}$, i.e. $[s_1, \sigma^p] \equiv u^p \bmod G_{i+p}$, where $u = [s_1, \sigma] \in G_i/G_{i+1}$. But as $u^p \in G_{i+p-1}/G_{i+p}$ by (1.5), this means that $[s_1, \sigma^p] \in G_{i+p-1}/G_{i+p}$ and our claim follows. In particular, G_3 and A_3 have the same exponent p^e, say, and to every $1 \leqslant i \leqslant e$, $\mho_i(A_3) = A_{m-i(p-1)}$. If $e = 1$ then A_3 and G_3 are elementary abelian of the same order, hence isomorphic. If $e \geqslant 2$, then $G_{m-1}\mho_i(G_3)$ and by our claim $A_{m-1} \leqslant \mho_i(A_3)$ for $1 \leqslant i \leqslant e - 2$. Thus, $A_3/\mho_i(A_3) \cong G_3/\mho_i(G_3)$ for $1 \leqslant i \leqslant e - 1$. But then $\mho_i(A_3) \cong \mho_i(G_3)$ for $1 \leqslant i \leqslant e - 1$ 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 $i \geqslant 3$.

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

(c) By Theorem 3.2(f) and (d) $Z_i(P) = A_{m-i+1}\bar{G}_{m-i-1}$ and $\bar{G}_{i-1} \leqslant K_i(P) \leqslant A_{(i-1)(k-1)+3}\bar{G}_{i-1}$. Since $|G_i/G_{i+1}| = p$ for $2 \leqslant i \leqslant m - 1$, it follows from Lemma 3.1(d) that $[\tau, A_i] \equiv A_{i+k-1} \bmod \bar{G}_{i-1}$; hence $K_i(P) \equiv A_{(i-1)(k-1)+3} \bmod \bar{G}_{i-1}$, and the result follows.

(d) By Theorem 4.2(b) $P = A_3\bar{G}$. Hence the result follows from Theorem 3.2(e).

REFERENCES

1. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92.

2. J. A. Gallian, *Finite p-groups with homocyclic central factors*, Canad. J. Math. **26** (1974), 636–643.

3. C. R. Leedham-Green and Susan McKay, *On p-groups of maximal class*. I, Quart. J. Math. Oxford Ser. (2) **27** (1976), 297–311.

4. B. Huppert, *Endlich Gruppen*. I, Springer-Verlag, Berlin, 1967.

5. A. Juhász, *On finite groups with a Sylow p-subgroup of type* (m, n), Israel J. Math. **36** (1980), 133–168.

6. ______, *On metabelian p-groups* (unpublished).

7. H. Liebeck, *The automorphism group of finite p-groups*, J. Algebra **4** (1966), 426–432.

8. M. Lazard, *Quelques calculs concernant la formule de Hausdorff*, Bull. Soc. Math. France **91** (1963), 435–451.

9. R. Shepherd, *p-groups of maximal class*, Ph.D. Dissertation, Univ. of Chicago, 1970.

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

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