ISRAEL JOURNAL OF MATHEMATICS, Vol. 38, No. 4, 1981

POWER AUTOMORPHISMS OF FINITE p-GROUPS

BY
THOMAS MEIXNER

ABSTRACT
For a finite group G let $A(G)$ denote the group of power automorphisms, i.e. automorphisms normalizing every subgroup of G. If G is a p-group of class at most p, the structure of $A(G)$ is shown to be rather restricted, generalizing a result of Cooper ([2]). The existence of nontrivial power automorphisms, however, seems to impose restrictions on the p-group G itself. It is proved that the nilpotence class of a metabelian p-group of exponent p^2 possessing a nontrival power automorphism is bounded by a function of p. The "nicer" the automorphism — the lower the bound for the class. Therefore a "type" for power automorphisms is introduced. Several examples of p-groups having large power automorphism groups are given.

In the following, groups will always be finite. We denote by $\{K_i(G)\}_{i\geq 1}$ the descending central series of the group G, by $c(G)$ the nilpotence class of G, and we define

$$\Omega_i(G):=\langle x\in G \mid x^{p^i}=1\rangle,\qquad \mho_i(G):=\langle x\in G \mid x=y^{p^i} \text{ for some } y\in G\rangle.$$

For abbreviation let us put

$$v_{i,j}(x,y):=[y,\underbrace{x,\cdots,x}_{i},\underbrace{y,\cdots,y}_{j}] \quad\text{and}\quad v_i(x,y):=v_{i,0}(x,y).$$

A special part is played by commutators of length p, so define $s_i(x,y):=v_{i,p-i-1}(x,y)$. If G is a metabelian group, we shall always use identities like (1) to (7) of [3], page 364. The rest of the notation is taken from [8]. Of course, p will always denote a prime number.

1. Definition and well-known facts

Let G be a group; an automorphism α of G is called a power automorphism

Received May 8, 1979

of G, if it maps every subgroup of G onto itself. Power automorphisms were studied by Cooper in [2]; we restate those results of his that we use frequently:

(1.1) LEMMA. *The set $A(G)$ of power automorphisms of G is a normal abelian subgroup of* Aut(G) ([2], theorem 2.1.1, p. 337).

(1.2) THEOREM. *Let $\alpha \in A(G)$. Then $[\alpha, \beta] = 1$ for every $\beta \in \mathrm{Inn}(G)$* ([2], theorem 2.2.1, p. 339).

(1.3) COROLLARY. *Let $\alpha \in A(G)$. Then*
(a) *the map $x \to [x, \alpha]$ is a homomorphism from G into $Z(G)$,*
(b) *G' is fixed elementwise by α* ([2], corollary 2.2.2, p. 339).

Let G from now on always denote a p-group. We shall define what we call the type of a power automorphism of G, so let $\alpha \in A(G)$. Then α maps every cyclic subgroup of G onto itself, so for every $x \in G$ there is a positive integer r_x such that $x^\alpha = (x)^{r_x}$. These exponents r_x of α will in general depend on the element $x \in G$. If there is a set Σ_α of n positive integers such that for every $x \in G$ there is an $r \in \Sigma_\alpha$ satisfying $x^\alpha = x^r$, but no set of $n-1$ positive integers has this property, then α is said to be of type n. It is clear that such minimal sets Σ_α do exist, but even if we restrict ourselves to sets $\Sigma_\alpha \subseteq \{1, 2, \cdots, \exp(G)-1\}$, there are more than one minimal Σ_α. Power automorphisms of type 1 are called universal; a power automorphism α of type 2 for which we can choose $\Sigma_\alpha = \{1, r\}$ is called quasi-universal. It was shown in [11] how to assign to every $\alpha \in A(G)$ a unique set Σ_α, having the following properties: (i) $\Sigma_\alpha \subseteq \{1, 2, \cdots, \exp(G)-1\}$, (ii) $|\Sigma_\alpha| =$ type of α, (iii) $\Sigma_\alpha = \{1, r\}$, if α is quasi-universal.

So in the following let Σ_α always have these three properties. Power automorphisms of an abelian group G are universal ([2], theorem 3.4.1, p. 343), and the restriction map gives an isomorphism from $A(G)$ onto Aut($\langle x \rangle$) for every cyclic subgroup $\langle x \rangle$ of G which is of maximal order.

(1.4) LEMMA. *Let G be a non-abelian p-group, $\alpha \in A(G)$. Then $r \equiv 1 \bmod p$ for every $r \in \Sigma_\alpha$, α stabilizes the series $1 \subseteq \Omega_1(G) \subseteq \Omega_2(G) \subseteq \cdots \subseteq G$, and $A(G)$ is a p-group* ([7], Hilfssatz 5, p. 166).

(1.5) THEOREM. *Let G be a regular p-group, then $A(G)$ consists of universal power automorphisms only. Therefore via the restriction homomorphism $A(G)$ is embeddable into* Aut($\langle x \rangle$) *for every cyclic subgroup $\langle x \rangle$ of G, that is of maximal order* ([2], theorem 5.3.1, p. 349).

REMARK. Since every p-group of class less than or equal to $p-1$ is a regular

p-group, the simplest class of p-groups not covered by (1.5) is the one of p-groups of class p.

2. p-groups of class p

(2.1) THEOREM. *Let G be a p-group of class p. Then $A(G)$ is elementary abelian or can be embedded via the restriction homomorphism into* $\mathrm{Aut}(\langle x\rangle)$ *for some cyclic subgroup $\langle x\rangle$ of G, that is of maximal order.*

For $p=2$, the rank of $A(G)$ is always at most 2.

PROOF. Let G be of exponent p^n, and let G' be of exponent p^k, then $1\leqq k\leqq n$, since G is non-abelian. We have $\Omega_k(G)\subseteq C_G(A(G))$; for let $x\in G$ be of order p^k, then $\langle x, G'\rangle$ is a regular p-group, as its class is at most $p-1$. Thus $\exp(\langle x, G'\rangle)=p^k$, and so by (1.5) and (1.3b) x is centralised by every power automorphism of G.

Now if $k=n$, then $G=\Omega_k(G)\subseteq C_G(A(G))$; so $A(G)=1$. If $k=n-1$, then $[G, A(G)]\subseteq\Omega_k(G)\subseteq C_G(A(G))$ by (1.4) and so for $x\in G$, $\alpha\in A(G)$ we have by (1.3a)

$$[x^p,\alpha]=[x,\alpha]^p=[x,\alpha^p]=1$$

whence $A(G)$ is elementary abelian. For $p=2$, we can make use of one of Cooper's results ([2], theorem 6.3.1, p. 351) to conclude that the rank of $A(G)$ is at most two, since by $[G, A(G), A(G)]=1$ we know that $A(G)$ and $D(G)^+$ (see [2], a remark on page 349) are isomorphic.

So let finally $k\leqq n-2$, and assume that $A(G)\neq 1$. Then direct application of the Hall–Petrescu Formula ([8], Satz III.9.4, p. 317) gives that G is p^{n-1}-abelian (see [12]), and $\Omega_{n-1}(G)=\{g\in G \mid g^{p^{n-1}}=1\}\subsetneqq G$. Thus G can be generated by elements of order p^n, and we can find an element $x\in G$ of order p^n, such that $[x,\alpha]\neq 1$ for at least one $\alpha\in A(G)$.

Assume, by way of contradiction, that there is a nontrivial element $\beta\in A(G)$ with $[x,\beta]=1$. Then take $y\in G\backslash C_G(\beta)$ of minimal order p^s; obviously $s>k$ holds, and we first assume $k<s<n$. Since $xy\notin C_G(\beta)$, we have $1\neq[xy,\beta]=[y,\beta]\in\langle xy\rangle\cap\langle y\rangle$, and since G is p^{n-1}-abelian, we have $1\neq x^{p^{n-1}}\in\langle xy\rangle$. As G is a p-group, we can conclude that $\langle x\rangle\cap\langle y\rangle\neq 1$, and so there is an integer j, such that $x^{jp^{n-1}}=y^{-p^{s-1}}$. Using the Hall–Petrescu Formula we get

$$(x^{jp^{n-s}}y)^{p^{s-1}}=x^{jp^{n-1}}y^{p^{s-1}}\prod_{i=2}^{p^{s-1}} d_i\binom{p^{s-1}}{i}$$

where $d_i\in K_i(\langle x^{p^{n-s}}, y\rangle)$; I don't care about the order of the product for a moment. Since the class of G is p, since p^{s-1} divides $\binom{p^{s-1}}{i}$ for $1 \leqq i \leqq p-1$ and p^{s-2} divides $\binom{p^{s-1}}{p}$ and since $k \leqq s-1$, we can write this equation

$$(x^{jp^{n-s}}y)^{p^{s-1}} = \tilde{d}_p^{\,p^{s-2}}, \qquad \tilde{d}_p \in K_p(\langle x^{p^{n-s}}, y\rangle).$$

But the element $\tilde{d}_p$ lies in the center of G, and so it can be expanded into a product of p-fold commutators with entries $x^{jp^{n-s}}$ and y, of course always one entry (at least) equal to $x^{jp^{n-s}}$, and since $n > s$ the element $\tilde{d}_p$ is equal to a pth power of an element of the commutator subgroup of G, so

$$(x^{jp^{n-s}}y)^{p^{s-1}} = 1.$$

But $(x^{jp^{n-s}}y) \in G \backslash C_G(\beta)$, contradicting the minimality of s. So assume finally that $n = s$. Then there is an integer j such that $x^{jp^{n-1}} = y^{-p^{n-1}}$ since $\langle xy\rangle \cap \langle y\rangle \neq 1$, and $(x^jy)^{p^{n-1}} = x^{jp^{n-1}}y^{p^{n-1}} = 1$ since G is p^{n-1}-abelian. But again $x^jy \in G\backslash C_G(\beta)$, contradicting the minimality of s.

In the following we shall investigate whether (2.1) can be generalised in one direction or the other. First, we give a family of groups $H_{n,p}$, for which $A(H_{n,p})$ is neither elementary nor can be embedded by restriction into $\mathrm{Aut}(\langle x\rangle)$ for any element $x \in H_{n,p}$.

(2.2) EXAMPLE. Let $A_{n,p}$ be an abelian p-group of rank $p-1$ and type $(n+1, n, n, \cdots, n)$, that is $A_{n,p} = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_{p-1}\rangle$ where a_1 is of order p^{n+1} and a_i is of order p^n, if $2 \leqq i \leqq p-1$. Then an endomorphism T of $A_{n,p}$ is defined by:

$$a_i^T := a_ia_{i+1} \quad \text{for } 1 \leqq i \leqq p-2, \qquad a_1^{1+T+T^2+\cdots+T^{p-1}} = 1.$$

Obviously T is an automorphism of $A_{n,p}$ of order p, which has the property that for any integer $i \not\equiv 0 \bmod p$ the endomorphism $1 + T^i + (T^i)^2 + \cdots + (T^i)^{p-1}$ is identically zero on $A_{n,p}$. The extension $G_{n,p}$ of $A_{n,p}$ by T, where $T^p = a_1^{p^n}$, is a p-group of maximal class, and $A(G_{n,p})$ is elementary abelian of rank 2, two linearly independent elements $\alpha, \beta \in A(G_{n,p})$ given by $a_1^\alpha = a_1$, $T^\alpha = T^{1+p}$; $a_1^\beta = a_1^{1+p^n}$, $T^\beta = T$.

It should be remarked that $G_{n,2}$ is a generalised quaternion group of order 2^{n+2}, and $G_{1,p}$ is Blackburn's example of an irregular p-group of class p, given in ([8], III.10.15).

Let k, n always denote positive integers, $\mathbf{Z}[X]$ the integer polynomial ring, and $n_k(X) := \sum_{i=0}^{p^k-1} X^i \in \mathbf{Z}[X]$. Then for any $1 \leqq r < k$ we have $n_k(X) = n_r(X)n_{k-r}(X^{p^r})$. We often consider the ring $\mathbf{Z}[T]$ of endomorphisms of the abelian group B, $T \in \mathrm{Aut}(B)$, which is commutative, and obviously, if $o(T) = p^k$, $j \not\equiv 0 \bmod p$, then $n_k(T^j) = n_k(T)$.

Proposition. *Let $B_{n,p,k}$ be an abelian p-group of rank $(p-1)p^{k-1}$ and type $(n+1, n, n, \cdots, n)$. Then $B_{n,p,k}$ has an automorphism T_k of order p^k, such that the endomorphism $n_k(T^j)$ is zero on $B_{n,p,k}$ for every $j \not\equiv 0 \bmod p^k$.*

Proof. Let $B_{n,p,k} = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_{(p-1)p^{k-1}} \rangle$, where $o(b_1) = p^{n+1}$ and $o(b_i) = p^n$ for $2 \leqq i \leqq (p-1)p^{k-1}$. We shall prove by induction over k the following, stronger fact: $B_{n,p,k}$ has an automorphism T_k of order p^k, satisfying (i) $B_{n,p,k} = \langle b_1^{\mathbf{Z}[T_k]} \rangle$, (ii) $b_1^{n_k(T_k^j)} = 1$ for $j \not\equiv 0 \bmod p^k$. The case $k = 1$ was described above as $(A_{n,p}, T)$. To prove the induction, we embed $B_{n,p,k}$ into

$$B_{n,p,k+1} = \langle b_{1,0} \rangle \times \langle b_{1,1} \rangle \times \cdots \times \langle b_{1,p-1} \rangle \times \langle b_{2,0} \rangle \times \cdots \times \langle b_{(p-1)p^{k-1},p-1} \rangle$$

by identifying it with the subgroup $\tilde{B}_{n,p,k} = \langle b_{i,0} \mid 1 \leqq i \leqq (p-1)p^{k-1} \rangle$ of $B_{n,p,k+1}$. ($o(b_{1,0}) = p^{n+1}$, and $o(b_{i,j}) = p^n$ for $(i,j) \neq (1,0)$.) Then we can carry the action of T_k on $B_{n,p,k}$ over to $\tilde{B}_{n,p,k}$ and define T_{k+1} on $B_{n,p,k+1}$ by

$$b_{i,j}^{T_{k+1}} := b_{i,j} b_{i,j+1} \qquad \text{if } 1 \leqq i \leqq (p-1)p^{k-1}, \quad 0 \leqq j < p-1,$$

$$b_{i,0}^{T_{k+1}{}^p} := b_{i,0}^{T_k} \qquad \text{if } 1 \leqq i \leqq (p-1)p^{k-1}.$$

This defines an endomorphism of $B_{n,p,k+1}$, since the images of the generators $b_{i,j}$ have suitable orders, and obviously using the induction hypothesis, we get $B_{n,p,k+1} = \langle b_{1,0}^{\mathbf{Z}[T_{k+1}]} \rangle$. But then, for $b_{1,0}^{f(T_{k+1})} \in \ker(T_{k+1})$ we have

$$1 = b_{1,0}^{f(T_{k+1})T_{k+1}} = b_{1,0}^{f(T_{k+1})T_{k+1}{}^p} = b_{1,0}^{T_{k+1}{}^p f(T_{k+1})},$$

since $\mathbf{Z}[T_{k+1}]$ is commutative. On the subgroup $\tilde{B}_{n,p,k}$ however, T_{k+1}^p and T_k coincide, and therefore some power T_{k+1}^{ps} inverts T_{k+1}^p on $\tilde{B}_{n,p,k}$. Thus

$$1 = b_{1,0}^{(T_{k+1})^p f(T_{k+1})(T_{k+1})^{ps}} = b_{1,0}^{(T_{k+1})^p (T_{k+1})^{ps} f(T_{k+1})} = b_{1,0}^{f(T_{k+1})};$$

and T_{k+1} is an automorphism of $B_{n,p,k+1}$. Clearly the order of T_{k+1} is p^{k+1}.

Now let j be a positive integer with $j \not\equiv 0 \bmod p^{k+1}$, let $j = tp^r$, where $(t,p) = 1$. Then if $r = 0$, we get $n_{k+1}(T_{k+1}^j) = n_{k+1}(T_{k+1})$, whence

$$1 = b_{1,0}^{n_{k+1}(T_{k+1}{}^j)} = b_{1,0}^{n_{k+1}(T_{k+1})} = b_{1,0}^{n_k(T_{k+1}{}^p) n_1(T_{k+1})}$$

since $n_k(T_{k+1}^p) = n_k(T_k)$ on $\tilde{B}_{n,p,k}$, and we can apply the induction hypothesis.

If $r \neq 0$, then $1 \leqq r \leqq k$, since $j \not\equiv 0 \bmod p^{k+1}$, and we have

$$n_{k+1}(T_{k+1}^j) = n_{k+1}(T_{k+1}^{p^r}) = n_k((T_{k+1}^p)^{p^{r-1}}) n_1(T_{k+1}^{p^{r+k}}),$$

and again the induction hypothesis implies

$$1 = b_{1,0}^{n_k((T_{k+1}{}^p)p^{r-1})n_1(T_{k+1}^{p^{r+k}})} = b_{1,0}^{n_{k+1}(T_{k+1}{}^j)},$$

since $r - 1 \leqq k - 1$.

Now the statement of the proposition follows, as any of the generators of $B_{n,p,k}$ can be written $b_1^{f(T_k)}$ by (i), and $n_k(T_k^j)$ commutes with all the endomorphisms $f(T_k)$.

Let $B := B_{n,p,n}$ and $T := T_n \in \mathrm{Aut}(B_{n,p,n})$ a pair with the properties from the proposition.

Let $B = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_{(p-1)p^{n-1}} \rangle$, and consider the extension of B by T where $T^{p^{2n-1}} = b_1^{p^n}$, call it $H_{n,p}$.

Then any element of $H_{n,p}$ can be written $T^j b_1^i b$ with $b \in \Omega_n(B)$. But if $j \not\equiv 0 \bmod p^n$, then $(T^j b_1^i b)^{p^n} = T^{jp^n}(b_1^i b)^{n_n(T^j)} = T^{jp^n}$ by the properties of T. Therefore for every element $x \in H_{n,p} \backslash \langle T^{p^n}, B \rangle$ we have $1 \neq x^{p^n} \in \langle T^{p^n} \rangle$. If $j \equiv 0 \bmod p^n$, then $T^j b_1^i b \in \langle T^{p^n}, B \rangle$ and if $i \not\equiv 0 \bmod p$, $1 \neq (T^j b_1^i b)^{p^n} = b_1^{ip^n} \in \langle T^{p^n} \rangle$. Therefore by

$$b_1^\alpha := b_1, \quad T^\alpha := T^{1+p^n}; \quad \text{and} \quad b_1^\beta := b_1^{1+p^n}, \quad T^\beta := T$$

two linearly independent power automorphisms of $H_{n,p}$ are given. $A(H_{n,p})$ has rank 2 and type $(n, 1)$.

We see that for $n \geqq 2$, $A(H_{n,p})$ is not elementary abelian, and if p is odd, it cen not be embedded into the automorphism group of a cyclic group, since it is not cyclic itself. For $p = 2$ to be embeddable into $\mathrm{Aut}(\langle x \rangle)$ by restriction, $A(H_{n,p})$ would have to induce the inverting automorphism on $\langle x \rangle$. But since $[x, A(H_{n,p})] \subseteq \langle x^{2^n} \rangle$ this yields $n = 1$.

The following two examples show that there are p-groups, the power automorphism group of which has rank 3. The second one is a 3-group of class 3; thus the bound 2 on the rank of $A(G)$ in (2.1) does not carry over to the case of odd primes.

(2.3) EXAMPLES. (a) Let $A = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$ be an abelian group of order 16, such that $a^4 = b^2 = c^2 = 1$, and define automorphisms s, t of A by

$$a^s := ab, \quad b^s := ba^2, \quad c^s := c;$$

$$a^t := ac, \quad b^t := ba^2, \quad c^t := ca^2.$$

Then both are automorphisms of order 4 of A, and t inverts s in $\mathrm{Aut}(A)$. We can therefore extend A successively by s and t setting $a^2 = s^4 = t^4$ and $s^t = s^{-1}$. The extension G has order 2^8 and class 3, and the automorphisms of G induced by the elements t^2, s^2t^2 and bc generate an elementary abelian power automorphism group of order eight.

(b) Let $A = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \times \langle z \rangle$ be an elementary abelian 3-group of order 3^4. Then A has an elementary abelian group of automorphisms $\langle y, x, t \rangle$ of order 3^3, where

$$\begin{array}{llll} a^y := a, & b^y := bz^2, & c^y := cz^2, & z^y := z; \\ a^x := az^2, & b^x := bz^2, & c^x := cz, & z^x := z; \\ a^t := a, & b^t := b, & c^t := cz^2, & z^t := z. \end{array}$$

If we extend A successively by y, x, and t, putting $y^3 = x^3 = t^3 = z$, and $[y, x] = a$, $[y, t] = c$, $[x, t] = b^2$, we get an extension H of order 3^7 and class 3, and the power automorphism group $A(H)$ is elementary abelian of order 3^3, generated by the automorphisms induced by the elements a, a^2b, and abc^2.

REMARK. As indicated in the preceding examples, there is a general method to construct p-groups having non-universal power automorphisms. It is based on extending a group H of exponent p^n, $n > 1$, by a cyclic p-group $\langle y \rangle$ such that the "norm map" (when H is abelian it is an endomorphism of H)

$$x \rightarrow (x)^{y^{i(p-1)}}(x)^{y^{i(p-2)}} \cdots (x)^{y^i}(x) \quad \text{of } y^i \text{ on } H$$

maps every element $x \in H$ onto 1, if p does not divide i. This situation is very similar to the one with p-groups for which the Hughes H_p-subgroup is a proper subgroup (see [6], theorem 2, p. 1099); in fact, if $y^p = 1$, the semidirect product of H by $\langle y \rangle$ will have this property. And indeed, for groups of exponent p^2 there is a correspondence between groups possessing quasi-universal power automorphisms and groups of Hughes type, if we use this expression for the not necessarily splitting extension of the group H of exponent p^n, $n > 1$, by the automorphism y of order p, such that the "norm maps" on H are trivial for all the nontrivial powers y^i of y.

(2.4) (a) *Every group G of exponent p^2 which is of Hughes type has a central extension P possessing a quasi-universal power automorphism.*

(b) *Every group G of exponent p^2 possessing a quasi-universal power automorphism has a subgroup of Hughes type.*

PROOF. (a) Let $y \in G$ and $H \subsetneq G$ of index p, such that $G = \langle y, H \rangle$ is of Hughes type. Then, if the extension is non-split, we have $\langle y \rangle \cap H = \langle y^p \rangle \subsetneq$

$Z(G)$, and by $y^\theta := y^{1+p}$, $h^\theta := h$ for $h \in H$ an automorphism θ of G is defined ([13], lemma 3, p. 42), which satisfies $(y^i h)^\theta = y^i h y^{ip} = y^i h (y^i h)^p$ for every element $y^i h \in G \backslash H$ by the properties of y. Therefore, since H is of exponent p^2, θ is quasi-universal with $\Sigma_\theta = \{1, 1+p\}$.

If $y^p = 1$, define P to be the extension of H by a cyclic group of order p^2, $\langle x \rangle$, such that x acts on H in the same way as y does, and that the extension splits. Then $\langle x^p \rangle \subseteq Z(P)$, and $P/\langle x^p \rangle \cong G$, so P is a central extension of G. And again the setting $x^\alpha := x^{1+p}$, $h^\alpha := h$ for $h \in \langle x^p H \rangle$ defines a quasi-universal power automorphism on P.

(b) Let G be a group of exponent p^2, and let $\alpha \in A(G)$ be quasi-universal. Then for some nontrivial power β of α we can choose $\Sigma_\beta = \{1, 1+p\}$. Let $y \in G \backslash C_G(\beta)$, and put $U := \langle y, C_G(\beta) \rangle$. Then for every element $y^i h \in U \backslash C_G(\beta)$ we have $(y^i h)^p = [y^i h, \beta] = [y^i, \beta] = y^{ip}$, since β is quasi-universal, so $(h)^{y^{i(p-1)}} (h)^{y^{i(p-2)}} \cdots (h)^{y^i} (h) = 1$ and since $y^p \in \Omega_1(Z(G)) \subseteq C_G(\beta)$, we have that $y^i h \in U \backslash C_G(\beta)$ is equivalent to $i \not\equiv 0 \bmod p$, and so U is of Hughes type, as $\exp(C_G(\beta)) = p^2$ (otherwise β would be universal).

3. Metabelian groups of exponent p^2

In this third section we shall consider the question, whether the existence of a nontrivial power automorphism imposes restrictions on the nilpotence class of the p-group G. The procedure is motivated by (1.4), which stated: If G is a group of exponent p, which has a nontrivial power automorphism, then G is abelian.

In the following, we shall answer the question for metabelian groups of exponent p^2. Thereby we make use of a result of Gupta and Newman ([3], theorem, p. 362), but only in the following specialisation:

(3.1) THEOREM. *Let G be a metabelian p-group, and let i, j, k be positive integers strictly smaller than p. Then $c(G) \leqq i + j + k - 1$, provided*

$$v_k(z, v_{j,i-1}(y, x)) = [x, \underbrace{y, \cdots, y}_{j}, \underbrace{x, \cdots, x}_{i-1}, \underbrace{z, \cdots, z}_{k}] = 1 \qquad \textit{for every } x, y, z \in G.$$

PROOF. Since by hypothesis the above word holds in G, [3] tells that the exponent of $K_{i+j+k}(G)/K_{i+j+k+1}(G)$ divides $(i!)(j!)(k!)$. But since i, j and k are strictly smaller than p, none of the factorials $i!$, $j!$, or $k!$ is divisible by p, so the p-group $K_{i+j+k}(G)/K_{i+j+k+1}(G)$ is trivial, and since G is a finite nilpotent group, we get $K_{i+j+k}(G) = K_{i+j+k+1}(G) = 1$.

For later reference we also need the following lemma, which is presumably well-known.

(3.2) LEMMA. *Let $G = \langle x, y \rangle$ be a metabelian p-group, and let $\mho_1(G) \subseteq Z(G)$. If G is p-abelian, then $c(G) \leqq p-1$.*

PROOF. Since G is p-abelian, and since $\mho_1(G) \subseteq Z(G)$, the map $z \to z^p$ is a homomorphism from G into $Z(G)$, so $\exp(G') \leqq p$. Since by ([9], Satz 3, p. 10), $c(G/Z(G)) \leqq p-1$, we have $c(G) \leqq p$, and so ([10], Hilfssatz 3, p. 563) gives $\prod_{i=1}^{p-1} s_i(v, w)^{(-1)^i} = 1$ for every $v, w \in G$, as G is p-abelian. But now ([10], Hilfssatz 2, p. 562) which is a special case of ([1], lemma 1, p. 65) tells that $s_i(x, y) = 1$ for $1 \leqq i \leqq p-1$, and by ([10], Hilfssatz 1, p. 562) we get the result.

(3.3) LEMMA. *Let G be a metabelian group of exponent p^2, and let $1 \neq \alpha \in A(G)$ be universal. Then*

(i) *every two-generated subgroup of G has class at most $p-1$,*

(ii) *G is a regular p-group,*

(iii) *$c(G) \leqq p$.*

PROOF. For some nontrivial power β of α we may assume $\Sigma_\beta = \{1+p\}$, and so by (1.3a) G is p-abelian and $\mho_1(G) \subseteq Z(G)$. Thus by (3.2) every two-generated subgroup of G is of class at most $p-1$, and hence regular. Regularity, however, is a property that is checked on two elements, and so G is a regular p-group (see also [12], lemma 1, p. 736). Finally, since $v_{p-1}(y, x) \in K_p(\langle x, y \rangle) = 1$ for every two elements $x, y \in G$, we also have $v_1(z, v_{p-1}(y, x)) = [v_{p-1}(y, x), z] = 1$ for every $x, y, z \in G$. Now (3.1) tells $c(G) \leqq p$.

If the power automorphism α of G is not universal, we have to consider subgroups $\langle x, y \rangle$ of G, where y is fixed by α, while x is not. The easiest case is the following one.

(3.4) LEMMA. *Let G be a metabelian group of exponent p^2, and let $1 \neq \alpha \in A(G)$. Let $x \in G \setminus C_G(\alpha)$, and $v \in G'$ of order p. Then $c(\langle x, v \rangle) \leqq p-1$.*

PROOF. Let $U := \langle x, v \rangle$, then since G is metabelian and $v^p = 1$, we have $\exp(U') \leqq p$, and $K_i(U) = \langle v_{i-1}(x, v), K_{i+1}(U) \rangle$. Thus $[xv, \alpha] = [x, \alpha] \in \langle x^p \rangle \subseteq Z(G)$ gives

$$1 = [v, x^p] = \prod_{i=1}^{p} v_i(x, v)^{\binom{p}{i}} = v_p(x, v),$$

so $c(U) \leqq p$, and we can use ([10], Hilfssatz 3) to get

$$(x^j v)^p = x^{jp} s_{p-1}(x^j, v)^{(-1)^{p-1}} = x^{jp} s_{p-1}(x, v)^{(-j)^{p-1}} = x^{jp} \cdot s_{p-1}(x, v) \quad \text{for every integer } 1 \leqq j \leqq p-1.$$

Therefore $\langle [xv, \alpha] \rangle = \langle (xv)^p \rangle$ gives $s_{p-1}(x, v) \in \langle x^p \rangle$, and since for $1 \leqq j \leqq p-1$ we have $x^j v \in G \backslash C_G(\alpha)$ and so $(x^j v)^p \neq 1$, we conclude $s_{p-1}(x, v) = 1$.

Now we treat the general case. Again, we make use of the fact that for $x, y \in G$, where G is a metabelian group of exponent p^2, $1 \neq \alpha \in A(G)$ and $x \in G \backslash C_G(\alpha)$, $y \in C_G(\alpha)$, we have

$$(*) \qquad \langle (x^j y)^p \rangle = \langle [x^j y, \alpha] \rangle = \langle [x^j, \alpha] \rangle = \langle x^p \rangle \subseteq Z(G) \quad \text{for } 1 \leqq j \leqq p-1.$$

(3.5) Lemma. *Let G be a metabelian group of exponent p^2 and $1 \neq \alpha \in A(G)$. Let $U := \langle x, y \rangle \subseteq G$, where $x \in G \backslash C_G(\alpha)$ and $y \in C_G(\alpha)$. Then*

(i) $\mho_1(K_m(U)) \subseteq K_{m+p-1}(U)\langle x^p \rangle$ *for every* $m \geqq 2$,

(ii) $s_i(x, y) \in K_{p+1}(U)\langle x^p \rangle$ *for* $1 \leqq i \leqq p-2$, $y^p s_{p-1}(x, y) \in K_{p+1}(U)\langle x^p \rangle$,

(iii) $c(U) \leqq 2(p-1)$.

Proof. Since U is a nilpotent group, $\mho_1(K_m(U)) \subseteq K_{m+p-1}(U)\langle x^p \rangle$ for sufficiently large m. So let k be the minimal integer for which this relation holds, and assume by way of contradiction that $k > 2$. Let $v \in K_{k-1}(U)$ be an element of order p^2, then we can easily show by induction that $K_j(\langle x, v \rangle) \subseteq K_{j+(k-1)-1}(U)$ for $j \geqq 2$, so $K_p(\langle x, v \rangle) \subseteq K_{(k-1)+p-1}(U)$. By hypothesis we have $\mho_1(\langle x, v \rangle') \subseteq \mho_1(K_k(U)) \subseteq K_{k+p-1}(U)\langle x^p \rangle$, so the Hall–Petrescu Formula tells $x^p v^p \equiv (xv)^p$ mod $K_{k-1+p-1}(U)\langle x^p \rangle$ and by (*), since by hypothesis $v \in K_2(U) \subseteq C_G(\alpha)$, we get $v^p \in K_{k-1+p-1}(U)\langle x^p \rangle$, contradicting the minimality of k. By (i) and (*) we get from ([10], Hilfssatz 3)

$$y^p \prod_{i=1}^{p-1} s_i(x^j, y)^{(-1)^i} \equiv 1 \bmod K_{p+1}(U)\langle x^p \rangle \qquad \text{for } 1 \leqq j \leqq p-1.$$

But instead of using ([10], Hilfssatz 2) like in (3.2) we must go back to Brisley's theorem now.

Put $\tilde{s}_i(x^j, y) := s_i(x^j, y)^{(-1)^i}$ for $1 \leqq i \leqq p-2$, and $\tilde{s}_{p-1}(x^j, y) := y^p s_{p-1}(x^j, y)$. Then we have for $1 \leqq j \leqq p-1$

$$\prod_{i=1}^{p-1} \tilde{s}_i(x^j, y) \equiv 1 \bmod K_{p+1}(U)\langle x^p \rangle.$$

Since the elements $s_i(x^j, y)$ are central mod $K_{p+1}(U)\langle x^p \rangle$, the elements $\tilde{s}_i(x^j, y)$ do commute mod $K_{p+1}(U)\langle x^p \rangle$ and we have

$$\tilde{s}_i(x^j, y) \equiv \tilde{s}_i(x, y)^{j^i} \bmod K_{p+1}(U)\langle x^p \rangle, \qquad 1 \leqq i, j \leqq p-1.$$

Therefore we can apply ([1], lemma 1, p. 65) to get (ii). $K_p(U)$ is spanned mod $K_{p+1}(U)$ by the .elements $s_i(x, y)$, since U is metabelian, and so $K_p(U) \subseteq \langle y^p, x^p, K_{p+1}(U) \rangle$. Thus

$$[K_p(U), y] \subseteq [\langle y^p, x^p, K_{p+1}(U)\rangle, y] \subseteq K_{p+2}(U),$$

and since U is metabelian, we get $y \in C_U(K_i(U)/K_{i+2}(U))$ for every $i \geqq p$. So $K_i(U) = \langle v_{i-p}(x, y^p), K_{i+1}(U)\rangle$ for $i > p$. Since $y^p \in \langle x^p, U'\rangle$ and is an element of order at most p, the elements x and y^p lie in a subgroup of G that is generated by x and an element of order p in G', and so (3.4) yields $v_{p-1}(x, y^p) = 1$. Therefore $K_{2p-1}(U) = K_{2p}(U) = 1$, and (iii) holds.

For the proof of the main result in this section we need one more definition. If $a \in G$, we denote by M_a the set $\{v_{p-1}(a, w) \mid w \in G'\}$.

(3.6) LEMMA. *Let G be a metabelian group of exponent p^2, $1 \neq \alpha \in A(G)$ and $a \in G \backslash C_G(\alpha)$. Then*

(i) *M_a is an elementary abelian normal subgroup of G,*

(ii) *if $y \in C_G(\alpha)$, and $U := \langle y, a\rangle$, then $K_{p+1}(U) \subseteq M_a$.*

PROOF. The set M_a is a subgroup of G; for, since G is metabelian, $v_{p-1}(a, w_1)v_{p-1}(a, w_2) = v_{p-1}(a, w_1w_2)$ if $w_1, w_2 \in G'$. Of course, $M_a \subseteq G'$ is abelian, and since

$$(v_{p-1}(a, w))^g = v_{p-1}(a, w^g) \qquad \text{for } w \in G', \quad g \in G,$$

M_a is a normal subgroup of G.

Let $v_{p-1}(a, w) \in M_a$. Then, since by (3.5) the class of $\langle a, w\rangle$ is at most $2p-2$, we know that $c(\langle a, v_{p-1}(a, w)\rangle) \leqq p-1$, and $\langle a, v_{p-1}(a, w)\rangle$ is a regular subgroup of G. Therefore the (nontrivial!) restriction of α on $\langle a, v_{p-1}(a, w)\rangle$ is universal, and $v_{p-1}(a, w)^p = 1$.

To prove (ii), let $y \in C_G(\alpha)$, and put $U := \langle a, y\rangle$. Then by (3.5ii), $K_p(U)\langle a^p\rangle = \langle s_{p-1}(a, y), a^p, K_{p+1}(U)\rangle$, and $y \in C_U(K_i(U)/K_{i+2}(U))$ for $i \geqq p$, and so for $i > p$ $K_i(U) = \langle v_{i-1}(a, y), K_{i+1}(U)\rangle$, and $K_{p+1}(U) = \langle v_{i-1}(a, y) \mid i > p\rangle = \langle v_{p-1}(a, v_{i-p}(a, y)) \mid i > p\rangle$, which is a subgroup of M_a.

(3.7) LEMMA. *Let G be a metabelian group of exponent p^2, $1 \neq \alpha \in A(G)$ and $s, t \in G$. Then there is an element $a \in G \backslash C_G(\alpha)$ such that $v_{p-1,1}(s, t) \in M_a$.*

PROOF. If $s \in C_G(\alpha)$ and $t \in G \backslash C_G(\alpha)$, then $v_{p-1,1}(s, t)$ is in M_t by (3.6ii); and if $t \in C_G(\alpha)$ and $s \in G \backslash C_G(\alpha)$ then $v_{p-1,1}(s, t) \in M_s$ by (3.6ii).

If $s, t \in G \backslash C_G(\alpha)$, then consider the group $G/[G, \alpha]$. If $\exp(G/[G, \alpha]) = p$, then $\langle s, t, [G, \alpha]\rangle/[G, \alpha]$ is a two-generated metabelian group of exponent p, and has therefore at most nilpotence class $p-1$ by ([9], Satz 3, p. 10). But since $[G, \alpha] \subseteq Z(G)$, we get $v_{p-1}(s, t) \in Z(G)$ and $v_{p-1,1}(s, t) = 1$. If $\exp(G/[G, \alpha]) = p^2$, then the Hughes subgroup $H_p(G/[G, \alpha])$ of $G/[G, \alpha]$ is nontrivial and can by ([4], theorem, p. 451) only be of index 1 or p in $G/[G, \alpha]$. We prove that

$$(**)\quad \begin{array}{c}\text{for any nontrivial subgroup } X \text{ of } A(G) \text{ the Hughes}\\ \text{subgroup } H_p(G/[G,X]) \text{ of } G/[G,X] \text{ is covered by } C_G(X).\end{array}$$

$H_p(G/[G,X])$ is generated by the cosets $b[G,X]$ of order p^2 in $G/[G,X]$, that is, cosets $b[G,X]$ for which $b^p \not\in [G,X]$. But if there was an element β of X not centralising b, we would have $\langle b^p\rangle = \langle [b,\beta]\rangle \subseteq [b,X] \subseteq [G,X]$, so $b \in C_G(X)$.

Since $[G,\alpha] \subseteq C_G(\alpha)$, and since $\alpha \neq 1$, we must have $H_p(G/[G,\alpha]) = C_G(\alpha)/[G,\alpha]$ and $|G/C_G(\alpha)| = p$. Thus $t = sc$ for an element $c \in C_G(\alpha)$ and $v_{p-1,1}(s,t) = v_{p-1,1}(s,sc) \in K_{p+1}(\langle s,c\rangle) \subseteq M_s$.

Let finally $s,t \in C_G(\alpha)$. Then put $U := \langle s,t\rangle \subseteq G$, choose an arbitrary element $a \in G\backslash C_G(\alpha)$ and put $V := UM_a\langle a^p\rangle$, $C := C_V(V/M_a)$. By (3.5ii) we have $u^p v_{p-1}(a,u) \in M_a\langle a^p\rangle$ for every $u \in U$, and since $[v_{p-1}(a,s),t] \equiv [v_{p-1}(a,t),s]$ mod M_a, we have

$$[v_{p-1}(a,s),t,s] = [v_{p-1}(a,s),s,t] \in M_a,$$

$$[v_{p-1}(a,s),t,t] \equiv [v_{p-1}(a,t),s,t] \equiv [v_{p-1,1}(a,t),s] \equiv 1 \bmod M_a,$$

and so $[v_{p-1}(a,s),t]$, $[v_{p-1}(a,t),s] \in C$. Therefore for any $u_1,u_2 \in U$ we have $[v_{p-1}(a,u_1),u_2] \in C$, which is easily shown by induction over the length of u_1 as a product in s and t. But then also $[u_1^p,u_2] \in C$, and therefore $\mho_1(U/U\cap C) \subseteq Z(U/U\cap C)$. $U/U\cap C$ is also p-abelian, for let $u_1,u_2 \in U$, then

$$(u_1u_2)^p v_{p-1}(a,u_1u_2) = (u_1u_2)^p v_{p-1}(a,u_1)[v_{p-1}(a,u_1),u_2]v_{p-1}(a,u_2)$$

$$= (u_1u_2)^p (u_1)^{-p}(u_2)^{-p}[v_{p-1}(a,u_1),u_2] \equiv 1 \bmod M_a\langle a^p\rangle,$$

and hence $(u_1u_2)^p \equiv u_1^p u_2^p$ mod C.

Now (3.2) yields $c(U/U\cap C) \leqq p-1$, and therefore $v_{p-1}(s,t) \in C$. Thus $v_{p-1,1}(s,t) \in M_a$, as required.

(3.8) THEOREM. *Let G be a metabelian group of exponent p^2, and let $1 \neq \alpha \in A(G)$. Then $c(G) \leqq 2(p-1)+1$.*

PROOF. Let first p be an odd prime. Then (3.1) will prove the statement, provided we can show that for arbitrary elements $x,y,z \in G$ the element $v_{p-1}(z,v_{p-1,1}(y,x))$ is equal to 1. In (3.7) we showed that $v_{p-1,1}(y,x) = v_{p-1}(a,w)$ for some $w \in G'$, $a \in G\backslash C_G(\alpha)$, and $v_{p-1}(a,w)$ is an element of G' of order 1 or p by (3.6i) for every $x,y \in G$. Therefore we are through, if $z \in G\backslash C_G(\alpha)$, since we can apply (3.4). If $z \in C_G(\alpha)$, put $U := \langle w,z\rangle$. Then $U/\mho_1(U)$ is a metabelian group of exponent p that is generated by two elements, and hence by ([9], Satz 3, p. 10) $K_p(U) \subseteq \mho_1(U)$. But $\mho_1(G) \subseteq \mho_1(Z(G)G')$ by (3.5ii), and so $v_{p-1}(z,w)$ is an element of G' of order 1 or p; therefore $v_{p-1}(z, v_{p-1}(a, w)) = v_{p-1}(a, v_{p-1}(z, w)) = 1$ by (3.4), completing the proof.

For $p = 2$, we can even show $c(G) \leqq 2$, and don't even need the hypothesis that G is metabelian. Let $y \in C_G(\alpha)$, $x \in G \backslash C_G(\alpha)$ be arbitrary elements, then $xy \in G \backslash C_G(\alpha)$, and therefore $o(xy) = 4$, and $(xy)^\alpha = (xy)^3$. Thus $[y, x] = y^2$, since $x^2 = [x, \alpha] = [xy, \alpha] = (xy)^2 = x^2 y [y, x] y$. Hence x induces the inverting automorphism on $C_G(\alpha)$, and $C_G(\alpha)$ is abelian. Furthermore the order of $[y, x]$ is 1 or 2.

If $\exp(G/[G, \alpha]) = 2$, then $G' \subseteq [G, \alpha] \subseteq Z(G)$ and $c(G) \leqq 2$. If $\exp(G/[G, \alpha]) = 4$, then the Hughes H_2-subgroup of $G/[G, \alpha]$ is nontrivial, and hence has index at most 2 in $G/[G, \alpha]$ by ([5], lemma 4, p. 664). Again $H_2(G/[G, \alpha])$ is covered by $C_G(\alpha)$, see (**), and so $C_G(\alpha)$ has index 2 in G. Therefore let $x \in G \backslash C_G(\alpha)$, then any nontrivial commutator in G has the form $[y, x]$ for some $y \in C_G(\alpha)$, and lies in $\Omega_1(C_G(\alpha))$. Since x inverts the whole of $C_G(\alpha)$, it centralises the elementary abelian group $G' \subseteq C_G(\alpha)$, and therefore $G' \subseteq Z(G)$, and $c(G) \leqq 2$.

If the group G is generated by two elements, then the bound on the nilpotence class is a little better.

(3.9) THEOREM. *Let G be a two-generated metabelian group of exponent p^2 and $1 \neq \alpha \in A(G)$. Then $c(G) \leqq 2(p-1)$.*

PROOF. Since G is two-generated, and $\phi(G) \subseteq C_G(\alpha)$ by (1.3b) and (1.4), two cases must be considered.

(i) $C_G(\alpha)$ has index p in G. Then we can apply (3.5iii) immediately.

(ii) $\phi(G) = C_G(\alpha)$. Then, since the Hughes H_p-subgroup of $G/[G, \alpha]$ is covered by $C_G(\alpha)$, see (**), it has to be trivial by ([4], theorem, p. 451). Therefore $G/[G, \alpha]$ is a two-generated metabelian group of exponent p, and hence $K_p(G) \subseteq [G, \alpha] \subseteq Z(G)$, and $c(G) \leqq p \leqq 2(p-1)$.

The following case is noted separately.

(3.10) LEMMA. *Let G be a metabelian group of exponent p^2, $1 \neq \alpha \in A(G)$. If α is of type 2, but not quasi-universal, then $c(G) = p$.*

PROOF. Since 1 does not occur in Σ_α, we must have $\exp(C_G(\alpha)) = p$, as $\exp(G) = p^2$. Therefore $\exp(G/[G, \alpha]) = p$, by (**), and for $x, y \in G$ we get $c(\langle x, y[G, \alpha] \rangle / [G, \alpha]) \leqq p - 1$ by ([9], Satz 3, p. 10). Thus $v_{p-1}(x, y) \in [G, \alpha] \subseteq Z(G)$ and

$$[v_{p-1}(x, y), z] = v_1(z, v_{p-1}(x, y)) = 1 \qquad \text{for every } x, y, z \in G.$$

Now (3.1) yields $c(G) \leqq p$, and since α is not universal, we get $c(G) = p$ by (1.5).

(3.11) THEOREM. *Let G be a metabelian group of exponent p^2, and let $|A(G)| \geqq p^2$. Then $c(G) = p$.*

PROOF. Since the automorphism group of a cyclic subgroup of G is cyclic, $A(G)$ cannot be embeddable into $\mathrm{Aut}(\langle x \rangle)$ for any $x \in G$. Therefore G can not be a regular p-group by (1.5), and hence $c(G) \geqq p$. Also, $C_G(A(G))$ is of index greater than p in G, because otherwise G would be generated by $C_G(A(G))$ and one further element $x \in G$, whence $A(G)$ would be embeddable into $\mathrm{Aut}(\langle x \rangle)$ by restriction. But the Hughes H_p-subgroup $H_p(G/[G, A(G)])$ is covered by $C_G(A(G))$, see (**), and so by ([4], theorem) the group $G/[G, A(G)]$ must be of exponent p. Thus again $v_{p-1}(x, y)$ lies in $[G, A(G)] \subseteq Z(G)$ for any $x, y \in G$, and (3.1) gives $c(G) \leqq p$.

(3.12) LEMMA. *Let G be a metabelian group of exponent p^2, $|A(G)| \geqq p^2$, and let $\alpha \in A(G)$ be of type 2. Then α is quasi-universal, there are $p-1$ quasi-universal power automorphisms in $A(G)$, and the rest of the nontrivial power automorphisms in $A(G)$ has type p.*

PROOF. Again $A(G)$ is elementary abelian and can not be embedded into $\mathrm{Aut}(\langle x \rangle)$ for any $x \in G$. Let $x \in G \backslash C_G(\alpha)$, and let $\beta \in A(G) \backslash \langle \alpha \rangle$. Then for some integer j, the element x is centralised by $\alpha^j \beta$. Let $y \in G \backslash C_G(\alpha^j \beta)$, then $A := \langle \alpha, \alpha^j \beta \rangle$ induces a group of power automorphisms on $U := \langle x, y \rangle$ that is of rank two. By (*) $\langle (xy)^p \rangle = \langle y^p \rangle$, and since $[xy, \alpha] = x^{ip} y^{mp} \in \langle (xy)^p \rangle = \langle y^p \rangle$ for some integers i, m, where $i \not\equiv 0 \bmod p$, we get $\langle x^p \rangle = \langle y^p \rangle$. Therefore by (1.3) α induces a homomorphism from U into $\langle x^p \rangle$, the kernel of which is $C_U(\alpha)$. Thus $C_U(\alpha)$ has index p in U, contains $\phi(U)$ properly and so α centralises some element $x^k y^l \in U \backslash \phi(U)$. But $l \not\equiv 0 \bmod p$, since $x \in U \backslash C_U(\alpha)$, and therefore $x^k y^l \in U \backslash C_U(\alpha^j \beta)$ has order p^2. So α centralises some element of order $p^2 = \exp(G)$ and $1 \in \Sigma_\alpha$. Since α has type 2, it must be quasi-universal, and all the nontrivial powers of α are quasi-universal, too.

Let $z \in \langle x^k y^l \rangle$ such that $z^p = x^p$. Since $x^\alpha = x^{1+ip}$, $i \not\equiv 0 \bmod p$, $z^\alpha = z$ and α is quasi-universal, we get, for $1 \leqq r \leqq p$, $(xz^r)^{1+ip} = (xz^r)^\alpha = (xz^r)x^{ip}$, and $(xz^r)^p = x^p$. Because A induces a noncyclic group of power automorphisms on U, the element $z \in U$ is not fixed by β, so if $z^\beta = z^{1+sp}$, $x^\beta = x^{1+tp}$, then $s \not\equiv 0 \bmod p$. For $1 \leqq r \leqq p$,

$$(xz^r)^\beta = x^{1+tp} z^{r(1+sp)} = (xz^r) x^{p(t+rs)} = (xz^r)^{1+(t+rs)p},$$

and since $(t + rs)$ takes p different values mod p, if r does, the type of β is at least p. But the type of β can not be greater than p by (1.4), since $\exp(G) = p^2$.

REMARK. For groups of exponent 4, a power automorphism of type 2 is always quasi-universal. For odd p however, there are metabelian groups of exponent p^2 that have a power automorphism of type 2 which is not quasi-universal, as the following example will show. The smallest 2-group having a power automorphism of type 2 that is not quasi-universal is the generalised quaternion group of order 16 described in (2.2).

(3.13) EXAMPLE. Let p be an odd prime, and let $A = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_{p-1}\rangle$ be an abelian group with $o(a_1) = p^2$, and $o(a_i) = p$ for $2 \leqq i \leqq p-1$. Then the endomorphism T of A given by $a_i^T := a_i a_{i+1}$ for $1 \leqq i \leqq p-2$, and $a_{p-1}^T := a_{p-1} a_1^p$, defines an automorphism of A of order p for which the "norm endomorphism" $1 + T + T^2 + \cdots + T^{p-1}$ maps every element of A onto its $(2p)$th power (see [8], III.10.15, Beweis, p. 334). We consider the extension G of A by T, where $T^p = a_1^{-2p}$.

Since the endomorphisms $1 + T^j + T^{j2} + \cdots + T^{j(p-1)}$ coincide on A for all the nontrivial powers T^j of T, we get for an arbitrary element $T^j a_1^i w \in G$, $w \in G'$:

$$(T^j a_1^i w)^p = T^{jp}(a_1^i w)^{1+T^j+T^{j2}+\cdots+T^{j(p-1)}} = a_1^{p(2i-2j)} \quad \text{if } 1 \leqq j \leqq p-1,$$

and $(a_1^i w)^p = a_1^{pi}$ for $T^j \in G'$. Put $H := \langle Ta_1, G'\rangle$, then H is a maximal subgroup of G, and by ([13], lemma 3, p. 42) G has an automorphism θ, defined by $T^\theta := T^{1+p}$, $h^\theta := h$ for $h \in H$. θ is a power automorphism of G, and since $H = C_G(\theta)$ is of exponent p (H is a regular p-group generated by elements of order p), 1 does not occur in Σ_θ. Now

$$(T^j a_1^i w)^\theta = (T^{j-i} T^i a_1^i w)^\theta = T^{(j-i)p} T^{j-i} T^i a_1^i w = (T^j a_1^i w) a_1^{p(2i-2j)},$$

and so for $z \in A$ we have $z^\theta = z^{1+2p}$ and for $z \in G \backslash A$ we have $z^\theta = z^{1+p}$.

REMARK. The bounds given in (3.8) and (3.9) should be compared with the nilpotency class of the free n-generated metabelian group of exponent p^2. This class was calculated by several authors according to $n = 2$, $3 \leqq n \leqq p+1$, and $n \geqq p+2$ (see review of N. D. Gupta, *The free metabelian group of exponent* p^2, MR 39 6984) and is $2p(p-1)$ for $n = 2$, and $n(p-1) + (p-1)^2$ for large n. So the existence of a nontrivial power automorsm is fairly restrictive for metabelian groups of exponent p^2.

ADDITIONAL REMARK. It should be pointed out that the family of groups in (2.2) has already been constructed in section 6 of [A1], and that [A2] assures the existence of more examples like those in (2.3).

References

1. W. Brisley, *On varieties of metabelian p-groups and their laws*, J. Austral. Math. Soc. **7** (1967), 64–80.

2. C. D. H. Cooper, *Power automorphisms of a group*, Math. Z. **107** (1968), 335–356.

3. N. D. Gupta and M. F. Newman, *On metabelian groups*, J. Austral. Math. Soc. **6** (1966), 362–368.

4. G. T. Hogan and W. Kappe, *On the H_p-problem for finite p-groups*, Proc. Amer. Math. Soc. **20** (1969), 450–454.

5. D. R. Hughes, *Partial differences sets*, Amer. J. Math. **78** (1956), 650–674.

6. D. R. Hughes and J. G. Thompson, *The H_p-problem and the structure of H_p-groups*, Pacific J. Math. **9** (1959), 1097–1101.

7. B. Huppert, *Zur Sylowstruktur auflösbarer Gruppen*, Arch. Math. **12** (1961), 161–169.

8. B. Huppert, *Endliche Gruppen I*, Springer, Berlin–Heidelberg–New York, 1967.

9. H. Meier-Wunderli, *Metabelsche Gruppen*, Comment. Math. Helv. **25** (1951), 1–10.

10. Th. Meixner, *Eine Bemerkung zu p-Gruppen vom Exponenten p*, Arch. Math. **29** (1977), 562–565.

11. Th. Meixner, *Verallgemeinerte Exponenten von Potenzautomorphismen*, Manuskript, Erlangen, 1978.

12. P. M. Weichsel, *On p-abelian groups*, Proc. Amer. Math. Soc. **18** (1967), 736–737.

13. J. H. Ying, *On finite groups whose automorphism groups are nilpotent*, Arch. Math. **29** (1977), 41–44.

A1. L. G. Kovacs, J. Neubüser and B. H. Neumann, *On finite groups with "hidden" primes*, J. Austral. Math. Soc. **12** (1971), 287–300.

A2. G. E. Wall, *Secretive prime-power groups of large rank*, Bull. Austral. Math. Soc. **12** (1975), 363–369.

Friedrich-Alexander-Universität
Bismarckstrasse $1\frac{1}{2}$
D 8520 Erlangen, W. Germany