PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 92, Number 4, December 1984

THE POWER STRUCTURE OF METABELIAN p-GROUPS

NORMAN BLACKBURN[1] AND ALBERTO ESPUELAS

ABSTRACT. In a metabelian p-group in which the pth powers generate a subgroup of order p, the elements of order p generate a subgroup of index at most p^p. This is best possible.

1. Let p be a prime number and for any p-group G write

$$\Omega_n(G) = \langle x | x \in G,\ x^{p^n} = 1 \rangle, \quad \mho_n(G) = \langle x^{p^n} | x \in G \rangle$$

($n \geq 0$). Although these subgroups are the objects of the study of the power structure of p-groups (see, for example, Mann [**4**]), very little is known about them in general. In the metabelian case, however, there is an explicit formula for a power of a product, so it is to be expected that more can be said. In this note we prove the following:

Let G be a metabelian p-group and suppose that $|\mho_1(G)| = p$. Then $|G : \Omega_1(G)| \leq p^p$. This result is best possible.

Some consequences of this result are discussed in [**1**]. We use standard notation [**2**].

2. To obtain the bound we prove the following.

LEMMA 1. *Suppose that P is a p-group of class at most p, and that $|\mho_1(P)| = p$. Then $K_2(P)$ is of exponent at most p and $|P : \Omega_1(P)| \leq p^p$.*

PROOF. The class of $P' = K_2(P)$ is less than p, so P' is regular. Since $|\mho_1(P')| \leq p$, it follows that $|P' : \Omega_1(P')| \leq p$. Thus $K_3(P) \leq \Omega_1(P')$ and the exponent of $K_3(P)$ is at most p. For elements x, y of P the class of $\langle x, y \rangle$ is at most p. Hence the class of $H = \langle x, [x, y] \rangle$ is less than p and H is regular. Hence

$$(x[x, y])^p = x^p [x, y]^p u,$$

where $u \in \mho_1(H')$. But $H' \leq K_3(P)$, so $u = 1$. Since $\mho_1(P) \leq Z(P)$,

$$x^p = (x^p)^y = (x^y)^p = (x[x, y])^p = x^p [x, y]^p.$$

Thus $[x, y]^p = 1$ and $K_2(P)$ is of exponent at most p.

We prove that $|P : \mho_1(P)| \leq p^p$ by induction on $|P|$. We suppose that the class of P is exactly p; otherwise P is regular and $|P : \Omega_1(P)| = p$. If the centre of P contains an element v of order p for which $v \notin \mho_1(P)$, the inductive hypothesis may be applied in $P/\langle v \rangle$. Thus $|P : R| \leq p^p$, where $R/\langle v \rangle = \Omega_1(P/\langle v \rangle)$. But if $x\langle v \rangle$ is

Received by the editors August 30, 1983.
1980 *Mathematics Subject Classification.* Primary 20D15.

[1]During the preparation of this paper, the first author was a visiting professor at the University of Vienna, and he wishes to thank the Department of Mathematics there for its hospitality.

0002-9939/84 $1.00 + $.25 per page

an element of $P/\langle v\rangle$ of order p, $x^p \in \langle v\rangle \cap \mathfrak{V}_1(P) = 1$, so $R = \Omega_1(P)$. We may, therefore, suppose that $\mathfrak{V}_1(P)$ is the only subgroup of the centre of P of order p; in particular, $\mathfrak{V}_1(P) \leq K_p(P)$ and $K_p(P)$ is cyclic. Since P' is elementary abelian, it follows that $K_p(P) = \mathfrak{V}_1(P)$.

Now $P' \leq \Omega_1(P)$ and $P/\Omega_1(P)$ is a vector space over GF(p). It is to be proved that the dimension is at most p. Suppose not. Then there exist elements $a_1, \ldots, a_{p+1}$ of P which are linearly independent modulo $\Omega_1(P)$; that is,

$$(a_1^{\lambda_1} \cdots a_{p+1}^{\lambda_{p+1}})^p \neq 1$$

except when $\lambda_1 \equiv \cdots \equiv \lambda_{p+1} \equiv 0\ (p)$.

Let F be a free group with group-basis $x_1, \ldots, x_{p+1}$. By the Hall-Petresco formula [**2**, III, 9.4],

$$x_1^p \cdots x_{p+1}^p = c_1^p c_2^{\binom{p}{2}} \cdots c_p.$$

where $c_1 = x_1 \cdots x_{p+1}$, $c_2, \ldots, c_{p-1}$ lie in F' and c_p is a product of conjugates of commutators in $x_1, \ldots, x_{p+1}$ of weight p. Substituting $a_i^{\lambda_i}$ for x_i gives

$$a_1^{p\lambda_1} \cdots a_{p+1}^{p\lambda_{p+1}} = (a_1^{\lambda_1} \cdots a_{p+1}^{\lambda_{p+1}})^p c_p',$$

and c_p' is a product of commutators in $a_1^{\lambda_1}, \ldots, a_{p+1}^{\lambda_{p+1}}$ of weight p. Let $K_p(P) = \langle z\rangle$. Then such a commutator is of the form $z^{\varepsilon \lambda_1^{k_1} \cdots \lambda_{p+1}^{k_{p+1}}}$, where ε is independent of $\lambda_1, \ldots, \lambda_{p+1}$ and $k_1 + \cdots + k_{p+1} = p$. Also $a_i^p = z^{\eta_i}$ since $\mathfrak{V}_1(P) = K_p(P)$, and by Fermat's theorem $a_i^{p\lambda_i} = z^{\lambda_i \eta_i^p}$. Thus

$$(a_1^{\lambda_1} \cdots a_{p+1}^{\lambda_{p+1}})^p = z^{f(\lambda_1, \ldots, \lambda_{p+1})},$$

where $f(t_1, \ldots, t_{p+1})$ is a homogeneous polynomial of degree p with coefficients in GF(p). By a well-known theorem of Chevalley, there exist $\lambda_1, \ldots, \lambda_{p+1}$, not all zero modulo p, for which $f(\lambda_1, \ldots, \lambda_{p+1}) \equiv 0\ (p)$, a contradiction.

THEOREM 2. *Suppose that P is a p-group for $p \leq 3$. If $|\mathfrak{V}_1(P)| \leq p$, then $|P : \Omega_1(P)| \leq p^p$.*

PROOF. If the class of P is less than p, the assertion follows from the regularity of P, so we suppose that the class of P is at least p. For $p = 2$, $P/\mathfrak{V}_1(P)$ is elementary abelian, so the class of P is 2 and the assertion follows from Lemma 1.

Suppose that $p = 3$. Then for any elements x, y of P with $H = \langle x, y\rangle$, we have $[x, y, y] \in \mathfrak{V}_1(H)$, by [**2**, III, 6.6]. Thus $K_3(H) \leq \mathfrak{V}_1(H)$, and by Lemma 1, $[x, y]^3 = 1$. The class of $P/\mathfrak{V}_1(P)$ is at most 3 [**2**, III,6.5] and that of P is at most 4. Thus P' is regular and the exponent of P' is 3.

If $\mathfrak{V}_1(P) \not\leq K_3(P)$, then $K_4(P) \leq \mathfrak{V}_1(P) \cap K_3(P) = 1$ and the class of P is 3. Suppose, then, that $\mathfrak{V}_1(P) \leq K_3(P)$. Then P/P' is elementary abelian. Since $P' \leq \Omega_1(P)$, $P/P' = (\Omega_1(P)/P') \times (T/P')$ for some T. Now $\Omega_1(T) \leq \Omega_1(P) \cap T = P'$, so $\Omega_1(T) = P'$. Since

$$|P : \Omega_1(P)| = |T : P'| = |T : \Omega_1(T)|,$$

it is to be proved that $|T : \Omega_1(T)| \leq p^p$, and we do this by applying Lemma 1. Thus it must be shown that the class of T is at most 3, and we do this by applying a result of Heineken [**2**, III, 6.9]. We must therefore show that $[x, y, y, z] = [x, y, z, z] = 1$

for all x, y, z in T. The first of these is clear, since $[x, y, y] \in \mho_1(P)$. For the second, we prove that $[a, z, z] = 1$ for $a \in P'$. This is clear if $z \in P'$. Suppose that $z \notin P' = \Omega_1(T)$, and put $b = [z, a]$. Then $z^a = zb$, $z^{a^2} = zb^2$, since $[b, a] \in K_5(P) = 1$. Now

$$(za)^3 = zz^{a^2}z^a = z^2b^2zb = z^3[z, b],$$

$$(za^2)^3 = zz^az^{a^2} = z^2bzb^2 = z^3[z, b^{-1}] = z^3[z, b]^{-1}.$$

Thus $[z, b] \in \mho_1(P)$, and if $[z, b] \neq 1$, $z^3, (za)^3, (za^2)^3$ are distinct elements of $\mho_1(P)$. Since $|\mho_1(P)| = 3$, it follows that one of them is 1, and this leads to the contradiction $z \in \Omega_1(T)$. Thus $[z, b] = 1$ and $[a, z, z] = 1$. Theorem 2 is therefore proved.

It is not known if the condition $p \leq 3$ in Theorem 2 can be dropped, but this can be done with an additional assumption which is more general than being metabelian.

THEOREM 3. *Suppose that P is a p-group in which*

$$[K_2(P), K_i(P)] \leq K_{i+3}(P)Z_{p-i-1}(P) \quad \textit{for } i = 2, \ldots, p-1.$$

If $|\mho_1(P)| \leq p$, then the class of P is at most p and $|P : \Omega_1(P)| \leq p^p$.

PROOF. In view of Theorem 2 we may suppose that $p > 2$.

Suppose that $2 \leq j \leq p-1$. For $a \in K_j(P)$ and x, y in P, we have

$$[x, y^{-1}, a] \in [K_2(P), K_j(P)] \leq K_{j+3}(P)Z_{p-j-1}(P).$$

Thus by the Witt identity [**2**, III, 1.4],

$$[y, a^{-1}, x]^a[a, x^{-1}, y]^x \in K_{j+3}(P)Z_{p-j-1}(P);$$

hence

$$[a, y, x] \equiv [a, x, y] \quad \text{modulo } K_{j+3}(P)Z_{p-j-1}(P).$$

Thus

$$[x_1, \ldots, x_j, y, x] \equiv [x_1, \ldots, x_j, x, y] \quad \text{modulo } K_{j+3}(P)Z_{p-j-1}(P),$$

and

$$[x_1, \ldots, x_j, y, x, y_1, \ldots, y_{p-j-1}] \equiv [x_1, \ldots, x_j, x, y, y_1, \ldots, y_{p-j-1}] \quad \text{modulo } K_{p+2}(P).$$

for $2 \leq j \leq p-1$. It follows at once that

$$[x, y, x_1, \ldots, x_{p-1}] \equiv [x, y, x_{\sigma(1)}, \ldots, x_{\sigma(p-1)}] \quad \text{modulo } K_{p+2}(P) \tag{1}$$

for any permutation σ of $1, \ldots, p-1$.

We now use a well-known argument (cf. [**3**, p. 387]) to show that the class of P is at most p. By a theorem of Zassenhaus [**2**, III, 9.7],

$$[y, \underbrace{x, \ldots, x}_{p-1}] \in K_{p+1}(P)\mho_1(P),$$

so

$$[y, \underbrace{x, \ldots, x}_{p-1}, z] \in K_{p+2}(P) \quad \text{for all } x, y, z \text{ in } P.$$

By (1)

$$[y, x, z, \underbrace{x, \ldots, x}_{p-2}] \in K_{p+2}(P).$$

By the Witt identity, $[y, x, z][z, y, x][x, z, y] \in K_4(P)$, so it follows that

$$[z, y, \underbrace{x, \ldots, x}_{p-1}][x, z, y, \underbrace{x, \ldots, x}_{p-2}] \in K_{p+2}(P).$$

But

$$[x, z, y, \underbrace{x, \ldots, x}_{p-2}] \equiv [z, x, y, \underbrace{x, \ldots, x}_{p-2}]^{-1} \equiv 1 \quad \text{modulo } K_{p+2}(P),$$

so

$$[z, y, \underbrace{x, \ldots, x}_{p-1}] \in K_{p+2}(P) \quad \text{for all } x, y, z \text{ in } P.$$

Replacing x by $x_1 \cdots x_{p-1}$, it follows that

$$\prod [z, y, x_{i_1}, \ldots, x_{i_{p-1}}] \in K_{p+2}(P) \tag{2}$$

for all $z, y, x_1, \ldots, x_{p-1}$ in P. Putting $x_1 = 1$, we see that the product of those factors in (2), for which no i_k is equal to 1, is 1. Removing all such factors from (2), we see that (2) remains true if the product is taken over those factors for which at least one i_k is equal to 1. We now repeat this argument on the formula thus obtained for the suffix 2, then for 3, and so on. The conclusion is thereby reached that (2) is valid if the product is restricted to those suffixes for which $i_1, \ldots, i_{p-1}$ is a permutation of $1, 2, \ldots, p-1$. By (1), $[z, y, x_1, \ldots, x_{p-1}]^{(p-1)!} \in K_{p+2}(P)$. Since P is a p-group, $[z, y, x_1, \ldots, x_{p-1}] \in K_{p+2}(P)$. Thus $K_{p+1}(P) \leq K_{p+2}(P)$ and $K_{p+1}(P) = 1$. The class of P is thus at most p. By Lemma 1, $|P : \Omega_1(P)| \leq p^p$.

COROLLARY 1 (cf. MEIER-WUNDERLI [5], MEIXNER [6]). *If P is a group of exponent p in which $[K_2(P), K_i(P)] \leq K_{i+3}(P)$ for all $i = 2, \ldots, p-1$, the class of P is at most p.*

COROLLARY 2. *Suppose that P is a p-group and that $|\mho_1(P)| \leq p$. If $P'' \leq Z(P)$ and $K_{p-1}(P) \leq Z(P')$, then $|P : \Omega_1(P)| \leq p^p$. In particular, this is so if P is metabelian.*

3. We shall show that Theorem 3 is best possible by constructing a metabelian p-group G in which $|\mho_1(G)| = p$ and $|G : \Omega_1(G)| = p^p$. Our group is similar to one constructed by G. E. Wall [7], but our method of calculation is different. We shall use the fact that in any metabelian group,

$$x^n y^n = (xy)^n \prod_{i=2}^{n} [x, y, \underbrace{x, \ldots, x}_{i-2}]^{\binom{n}{i}} \prod_{k=1}^{n-1} \prod_{l=1}^{n-1} [x, y, \underbrace{x, \ldots, x}_{k-1}, \underbrace{y, \ldots, y}_{l}]^{a_{kl}}, \tag{3}$$

where

$$a_{kl} = \sum_{i=1}^{n-1} \binom{i}{k} \binom{i}{l}$$

$$= \binom{l}{k} \binom{n}{l+1} + \binom{k}{1} \binom{l+1}{k} \binom{n}{l+2} + \cdots + \binom{l+k}{k} \binom{n}{l+k+1};$$

this is proved by a routine induction on n.

Thus, if the group is nilpotent of class at most the prime p and the derived group is of exponent p,

$$x^p y^p = (xy)^p \prod_{k=1}^{p-1} [x, y, \underbrace{x, \dots, x}_{k-1}, \underbrace{y, \dots, y}_{p-k-1}]^{\binom{p-1}{k}}.$$

It follows that if u is in the derived group, $x^p = (xu)^p$ and

$$x_1^p \cdots x_k^p = (x_1 \cdots x_k u)^p \prod [x_i, x_j, \underbrace{x_i, \dots, x_i}_{r_i}, \dots, \underbrace{x_k, \dots, x_k}_{r_k}]^{a_i(r_i, \dots, r_k)}, \tag{4}$$

the product being taken over $1 \le i < j \le k$, $r_i + \cdots + r_k = p - 2$, $r_l \ge 0$, and

$$a_i(r_i, \dots, r_k) = \binom{p-1}{r_{i+1} + \cdots + r_k} \binom{r_{i+1} + \cdots + r_k}{r_{i+2} + \cdots + r_k} \cdots \binom{r_{k-1} + r_k}{r_k}.$$

Thus $a_i(r_i, \dots r_k)$ is not divisible by p.

To construct the example, we start with the free group with p generators in the variety of groups of class at most p in which the derived group is elementary abelian. This may be constructed as follows. Let E be an elementary abelian p-group with $\mathbf{Z}_p$-basis

$$\Omega = \{(i, j, r_i, \dots, r_p) | 1 \le i < j \le p,\ 0 \le r_k,\ r_i + \cdots + r_p \le p - 2\}.$$

The group E has automorphisms $\xi_1, \dots, \xi_p$ given by

$$(i, j, r_i, \dots, r_p)\xi_a = (i, j, r_i, \dots, r_p)\alpha,$$

where

$$\alpha = \begin{cases} (i, j, r_i, \dots, r_a + 1, \dots, r_p) & (a \ge i), \\ (a, j, \underbrace{0, \dots, 0}_{i-a}, r_i + 1, \dots, r_p)(a, i, \underbrace{0, \dots, 0}_{i-a}, r_i, \dots, r_j + 1, \dots, r_p)^{-1} & (a < i) \end{cases}$$

for $r_i + \cdots + r_p < p - 2$, and $\alpha = 1$ for $r_i + \cdots + r_p = p - 2$. By the theory of cyclic extensions, there exists a group $G = E\langle x_1, \dots, x_p \rangle$ in which $E \lhd G$, G/E is free Abelian of rank p and x_a induces the automorphism ξ_a on E; further, for $i < j$,

$$[x_i, x_j] = (i, j, \underbrace{0, \dots, 0}_{p-i-1}).$$

Thus, for $i < j$ and $r_i + \cdots + r_p \le p - 2$,

$$[x_i, x_j, \underbrace{x_i, \dots, x_i}_{r_i}, \dots, \underbrace{x_p, \dots, x_p}_{r_p}] = (i, j, r_i, \dots, r_p).$$

Thus $G = \langle x_1, \dots, x_p \rangle$, $K_2(G) = E$ and

$$K_k(G) = \langle (i, j, r_i, \dots, r_p) | k - 2 \le r_i + \cdots + r_p \le p - 2 \rangle$$

for $k = 2, \dots, p$. Also $K_{p+1}(G) = 1$. Thus G satisfies all the conditions under which (4) holds. Hence for any x, y in G,

$$[x^p, y] = x^{-p}(x[x, y])^p = 1.$$

Thus all pth powers of elements of G lie in the centre of G, and for $u \in G'$,

$$(x_1^{\lambda_1} \cdots x_p^{\lambda_p} u)^p = x_1^{p\lambda_1} \cdots x_p^{p\lambda_p} \prod (i, j, r_i, \ldots, r_p)^{-\pi},$$

where

$$\pi = a_i(r_i, \ldots, r_p)\lambda_j \lambda_i^{r_i+1} \lambda_{i+1}^{r_{i+1}} \cdots \lambda_p^{r_p},$$

the product being taken over $1 \leq i < j \leq p$, $r_i + \cdots + r_p = p - 2$, $r_k \geq 0$.

With each monomial $t_1^{n_1} \cdots t_p^{n_p}$ of degree p other than the t_i^p, we associate an element $\omega = \omega(n_1, \ldots, n_p) \in \Omega$ as follows: If $n_1 = \cdots = n_{i-1} = 0 \neq n_i$, $n_{i+1} = \cdots = n_{j-1} = 0 \neq n_j$, put $\omega = (i, j, n_i - 1, n_{i+1}, \ldots, n_j - 1, \ldots, n_p)$. In G we now add the relations $(i, j, r_i, \ldots, r_p) = 1$ for each element $(i, j, r_i, \ldots, r_p)$ in Ω for which $r_i + \cdots + r_p = p - 2$ and which does *not* arise in this way. Since no two distinct monomials give rise to the same element of Ω, we now have

$$(x_1^{\lambda_1} \cdots x^{\lambda_p} u)^p = x_1^{p\lambda_1} \cdots x_p^{p\lambda_p} \prod \omega(n_1, \ldots n_p)^{b(n_1, \ldots n_p)\lambda_1^{n_1} \cdots \lambda_p^{n_p}},$$

where the product is taken over all monomials of degree p other than the t_i^p, and the $b(n_1, \ldots, n_p)$ are not divisible by p.

As Wall has pointed out in [**7**], there exists a homogeneous polynomial $f(t_1, \ldots t_p)$ of degree p with coefficients in $\mathbf{Z}$ such that $f(\mu_1, \ldots, \mu_p) \equiv 0\ (p)$ only if $\mu_1 \equiv \cdots \equiv \mu_p \equiv 0\ (p)$; for example such a polynomial arises from the norm mapping of $\mathrm{GF}(p^p)$ over $\mathrm{GF}(p)$. Write

$$f(t_1, \ldots, t_p) = \sum c(n_1, \ldots, n_p) t_1^{n_1} \ldots t_p^{n_p}.$$

There is certainly some coefficient $c(n_1, \ldots, n_p) \not\equiv 0\ (p)$ with more than one n_i different from 0, since

$$\sum c_i t_i^p \equiv \sum c_i t_i\ (p).$$

We choose a fixed such $c(m_1, \ldots, m_p) \not\equiv 0\ (p)$ and define $y \in E$ by

$$y^{c(m_1, \ldots, m_p)} = \omega(m_1, \ldots, m_p)^{b(m_1, \ldots, m_p)}.$$

In G we add the relations

$$\omega(n_1, \ldots, n_p)^{b(n_1, \ldots n_p)} = y^{c(n_1, \ldots, n_p)},$$

for all $n_1, \ldots, n_p$ with $n_1 + \cdots + n_p = p$. Thus $K_p(G)$ becomes of order p, being generated by y. We also add the relations

$$x_i^p = y^{c(0, \ldots, 1, \ldots, 0)} \quad (1 \text{ in the } i\text{th place }).$$

as we may since x_i^p lies in the centre. Thus G is now a p-group and $G' = E$, $|G : G'| = p^p$. And

$$(x_1^{\lambda_1} \cdots x_p^{\lambda_p} u)^p = y^{f(\lambda_1, \ldots \lambda_p)}.$$

Hence $(x_1^{\lambda_1} \cdots x_p^{\lambda_p} u)^p \neq 1$ unless $\lambda_1 \equiv \cdots \equiv \lambda_p \equiv 0\ (p)$. Hence $\Omega_1(G) = E$ and $\mho_1(G) = \langle y \rangle$, so G has all the required properties.

REFERENCES

1. A. Espuelas, Thesis, University of Zaragoza.
2. B. Huppert, *Endliche Gruppen.* I, Springer-Verlag, Berlin, 1967.
3. B. Huppert and N. Blackburn, *Finite groups.* II, Springer-Verlag, Berlin, 1982.
4. A. Mann, *The power structure of p-groups.* I, J. Algebra **42** (1976), 121–135.
5. H. Meier-Wunderli, *Über endliche p-Gruppen, deren Elemente der Gleichung* $x^p = 1$ *genügen,* Comment. Math. Helv. **24** (1950), 18–45; *Metabelsche Gruppen,* ibid. **25** (1951), 1–10.
6. T. Meixner, *Eine Bemerkung zu p-Gruppen vom Exponenten p,* Arch. Math. (Basel) **29** (1977), 561–565.
7. G. E. Wall, *Secretive prime-power groups of large rank,* Bull. Austral. Math. Soc. **12** (1975), 363–369.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY, MANCHESTER M13 9PL, ENGLAND

DEPARTAMENTO DE ALGEBRA, FACULTAD DE CIENCIAS, UNIVERSIDAD DE ZARAGOZA, ZARAGOZA, SPAIN