

ON METABELIAN p -GROUPS

PAUL M. WEICHSEL

(Received 22 November 1965)

Introduction

In this paper we investigate finite metabelian p -groups from the point of view of varieties and identical relations. In other words we shall be interested in those properties of such groups which are preserved under the operations of forming direct products, taking subgroups and taking factor groups. Ideally one would like to characterize such properties in terms of numerical invariants and with the sole restriction that the p -group in question have class less than p we accomplish this.

We first prove that functions on metabelian p -groups can be put into a given canonical form (1.13). From this theorem we readily deduce a characterization of all critical metabelian p -groups of class c , $p > c$ and show that the exponents of the elements of the descending central series completely characterize the variety generated by a finite metabelian p -group of class c , $p > c$ (1.14, 1.15). In part II we produce a set of groups which act as a basis for the construction of an arbitrary group of this type (2.3).

Notation and preliminaries

A simple commutator of weight m on the group elements a_1, \dots, a_n is defined inductively by $(x_1, x_2) = x_1^{-1}x_2^{-1}x_1x_2$, $(x_1, \dots, x_m) = ((x_1, \dots, x_{m-1}), x_m)$ with $x_i \in \{a_1, \dots, a_n\}$. We denote by G_2 the subgroup of G generated by all commutators of weight 2 and in general G_i is the subgroup generated by all simple commutators of weight i . A group is called nilpotent of class c or simply of class c if $G_{c+1} = 1$ and $G_c \neq 1$. A group G is called *metabelian* if G_2 is abelian.

We will need certain elementary facts about finite metabelian p -groups which we list below without proof. Let G be a finite metabelian p -group.

1. If $u = (g_1, g_2, g_3, \dots, g_m)$ is a simple commutator with $g_i \in G$, then u is unaffected by an arbitrary permutation on $\{g_3, \dots, g_m\}$.
2. If $g_1, \dots, g_m \in G$, then $(g_1, g_2, g_3, \dots, g_m)^{-1} = (g_2, g_1, g_3, \dots, g_m)$.

A reduced word f in the free group generated by a_1, \dots, a_m, \dots is called a function. If we allow a_i to take on values in G , the subgroup generated by the values of f is called the *verbal subgroup* $f(G)$. A function is said to be an identical relation on G if $f(G) = 1$. If V is a set of functions then the class of groups \mathcal{V} for which each element of V is an identical relation is called a *variety*. If g is an identical relation for all the groups in \mathcal{V} then g is said to be a consequence of the functions in V and V is called a *basis* for the set of all identical relations satisfied by all the elements of \mathcal{V} . A classical theorem of G. Birkhoff states that any variety is closed under the operations of forming unrestricted direct products, taking subgroups and factor groups, and conversely any class of groups closed under these operations is in fact the class of all groups for which some set of functions are identical relations. A set of groups \mathcal{G} is said to generate the variety \mathcal{V} if \mathcal{V} is the smallest variety which contains the elements of \mathcal{G} .

A group is called *critical* if it is not contained in the variety generated by its proper subgroups and factor groups. If G is critical, then there is a function f which is an identical relation for all proper subgroups and factor groups of G but not for G . Such a function is called a *G-critical function* and can be chosen to be an element in the free group of rank m where m is the order of a minimal generating set of elements of G . The critical groups form the focus of our investigation. Our main technique will be an examination of the formal properties of G -critical functions and identical relations.

The reader is referred to [1] for a fuller discussion of these matters.

1. Identical relations and critical functions on metabelian p -groups

DEFINITION 1.1. A simple commutator u on a_1, \dots, a_m is said to be in *normal form* and of sign i , $sign\ u = i$, if $u = (a_1, a_i, \dots)$. By the j^{th} degree of u , $d_j(u)$, we shall mean the number of occurrences of a_j in u .

DEFINITION 1.2. Let $f(a_1, \dots, a_m)$ or simply f be a word (function) in the free metabelian group generated by a_1, \dots, a_m . Then f is said to be in *normal form* if

$$f = \prod_{i=1}^n u_i^{\alpha_i}$$

with u_i a simple non-trivial commutator on a_1, \dots, a_m in normal form, α_i a non-zero integer, $d_j(u_i) > 0$ for $i = 1, \dots, n$, $j = 1, \dots, m$, and $u_i \neq u_k$ if $i \neq k$. We then say that $u_i^{\alpha_i}$ is a *factor* of f and write $u_i^{\alpha_i} || f$. We may also write $u_i || f$.

We will use the notation $f(a_i \rightarrow g)$ to represent the function f with the word g substituted for a_i .

It is easy to show that any function on a fixed nilpotent group G is equivalent on G to a set of functions, each in normal form on a separate set of variables. (See, for example, [1], Lemma 1.1). If G is nilpotent of class c , then only those commutators of weight less than $c+1$ need be considered. Hence when we discuss functions in normal form on a group which is nilpotent of class c we will assume that only powers of commutators of weight c or less appear as factors.

We now define an ordering on the set of all simple commutators in normal form which will be useful in constructing induction proofs.

DEFINITION 1.3. Let u and v be two simple commutators on a_1, \dots, a_m in normal form. Associate with u and v the $m+1$ -tuples of integers

$$U = (d_1(u), d_2(u), \dots, d_m(u), \text{sign } u)$$

and

$$V = (d_1(v), d_2(v), \dots, d_m(v), \text{sign } v) \text{ respectively.}$$

Then we say $u \geq v$ if $U \geq V$ in the lexicographic ordering.

Now if a_1, \dots, a_m are taken to be elements of a metabelian group, then it follows from 1 above that the simple commutator u in normal form is uniquely determined by the $m+1$ -tuple U . Thus the order defined above is a total order.

DEFINITION 1.4. A function $f(a_1, \dots, a_m)$ is called G -subcritical if f is an identical relation on the proper subgroups and factor groups of G .

The reader should note that if G is a critical group and f is G -subcritical, then f is either an identical relation on G or f is G -critical. If, on the other hand, G is not critical, then f is an identical relation on G .

The following lemma is then a trivial consequence of the definition.

LEMMA 1.5. Let f be a G -subcritical function. Then $f(a_i \rightarrow a_i^n) = f^n R_n(a_1, \dots, a_m)$ and R_n is a G -subcritical function for each integer n . Furthermore if f is an identical relation on G , then so is R_n .

DEFINITION 1.6. Let u^α be a power of the simple commutator u in a_1, \dots, a_m of weight r . We say that u^α is G -multilinear if $(G_{r+1})^\alpha = 1$.

The next lemma provides the justification of the use of this term.

LEMMA 1.7. Let G be a metabelian group and let u^α be G -multilinear. Then $u^\alpha(a_i \rightarrow a_i^n) = (u^\alpha)^{n^{d_i(u)}}$ on G .

PROOF. If u is of weight r , then $u(a_i \rightarrow a_i^n) \in u^{n^{d_i(u)}} G_{r+1}$. Thus $u^\alpha(a_i \rightarrow a_i^n) = (u^{n^{d_i(u)}} g)^\alpha$ with $g \in G_{r+1}$, and since G is metabelian and $(G_{r+1})^\alpha = 1$, $(u^{n^{d_i(u)}} g)^\alpha = (u^\alpha)^{n^{d_i(u)}}$.

LEMMA 1.8. Let G be a metabelian p -group of class c , $p > c$, and let f be a G -subcritical function on a_1, \dots, a_m in normal form, each of whose

factors is G -multilinear. Let e be an integer, $1 \leq e \leq p-1$, satisfying $e^x \equiv 1(p)$ if and only if $x \equiv 0 \pmod{p-1}$.

Then $f(a_j \rightarrow a_j^e) = (f)^{e^v} R'$ where $v = \min \{d_j(w) \mid 1 \neq w^v \in f\}$ and R' is a G -subcritical function. Further if $u^{\alpha'}$ is a factor of R' , then u^{α} is a factor of f , $d_j(u) > v$, and $\alpha' = \alpha\beta$, $(\beta, p) = 1$.

PROOF. It follows from Lemma 1.7 that if u^{α} is a factor of f , then $u^{\alpha}(a_j \rightarrow a_j^e) = u^{\alpha e^{d_j(u)}}$. Hence, if $v = \min \{d_j(w) \mid 1 \neq w^v \in f\}$, $f(a_j \rightarrow a_j^e) = (f)^{e^v} R'$ where each factor of R' is of the form $u^{(\alpha e^{d_j(u)} - \alpha e^v)}$. Thus those factors of f with $d_j(w) = v$ don't appear in R' and if u^{α} is a factor of f with $d_j(u) > v$, then $u^{\alpha(e^{d_j(u)} - e^v)}$ is a factor of R' . Now $e^{d_j(u)} - e^v = e^v(e^{d_j(u)-v} - 1)$ and since $p \mid e^v - 1$ if and only if $u \equiv 0(p-1)$, then $(\beta, (e^{d_j(u)} - e^v)) = 1$.

The next lemma is a simple consequence of a result of N. Gupta and M. Newman [3, Theorem] which we present without proof.

LEMMA 1.9. Let G be a metabelian p -group of class c with $p > c$. Let u be a simple non-trivial commutator of weight r and suppose that for some integer α , u^{α} is an identical relation for G , that is $(u(G))^{\alpha} = 1$. Then, if $(G_{r+1})^{\alpha} = 1$, $(G_r)^{\alpha} = 1$, that is, $(x_1, \dots, x_r)^{\alpha} = 1$ for all $x_i \in G$.

The following two theorems (1.10 and 1.12) are the principal tools from which we derive all of the results that follow.

THEOREM 1.10. Let G be a metabelian p -group of class c with $p > c$, and let f be a G -subcritical function on $\{a_1, \dots, a_m\}$ in normal form each of whose factors is G -multilinear.

(If u^{α} is a factor of f and u has weight r , then $(G_{r+1})^{\alpha} = 1$).

(i) If G is an m -generator group with $m > 2$, and u^{α} is a factor of f of weight r , then $(G_r)^{\alpha} = 1$. Thus, in particular $f(G) = u^{\alpha}(G) = 1$.

ii) If G is a 2-generator group and f is an identical relation on G , then the same conclusion follows.

PROOF. The proof is by induction on the factors of f ordered as in Definition 1.3. Let u^{α} be a factor of f and suppose that $v^{\beta}(G) = 1$ for all factors v^{β} of f with $v > u$. We thus assume that all such v^{β} have been deleted from f . If v is of weight r , then it follows from Lemma 1.9 that $G_r^{\beta} = 1$. Now let A_i be the set of all factors $w^{\gamma} \neq 1$ of f with $d_i(w) < d_i(u)$. Let A_j be the first such set that is nonempty and let e be an integer satisfying the hypothesis of Lemma 1.8. Then it follows from Lemma 1.8 that $f(a_j \rightarrow a_j^e) = f^{e^v} R'$ where $v = \min \{d_j(w) \mid 1 \neq w^v \mid f\}$ and R' is a G -subcritical function whose factors, $w^{\alpha'}$, satisfy $d_j(w) > v$ and $w^{\alpha} \mid f$, $\alpha' = \alpha\beta$, $(\beta, p) = 1$.

Hence by induction there is a G -subcritical function R_j whose factors are powers of factors of f (relatively prime to p) and such that $d_j(v) = d_j(u)$ for all $v \mid R_j$. We now repeat this procedure for $j+1$ and so on until we

obtain a G -subcritical function R whose factors are powers of factors of f and satisfy: $d_i(v) = d_i(u)$ for all $i = 1, \dots, m$ and all $v \mid R$. Now either R consists of a single factor or else $\text{sign } v < \text{sign } u$ for all $v \mid R, v \neq u$. If $m > 2$ and $\text{sign } u = k$, then by setting $a_1 = \dots = a_{k-1}$, we get $(u_0^\alpha)^\theta = 1$ where $u_0 = (a_1, a_k, \dots)$ and u_0 is of the same weight as u and $(\theta, \rho) = 1$. Thus it follows from Lemma 1.9 that $u^\alpha(G) = 1$. Hence by induction i) follows and $(G_r)^\alpha = 1$.

If $m = 2$, then since $d_i(v) = d_i(u)$ for all $v \mid R$, it follows that R consists of $(u^\alpha)^\theta$ alone. But in this case we are assuming that $f(G) = 1$ and hence $R(G) = 1$ and hence $(G_r)^\alpha = 1$.

LEMMA 1.11. *Let G be a metabelian p -group of class c and f a function on $\{a_1, \dots, a_m\}$ in normal form. Then for a fixed integer $i > 1$ $f(a_i \rightarrow a_1^n a_i) = f(a_i \rightarrow a_1^n)ABC$ with A, B , and C defined as follows:*

For each weight r , and each set of $m-2$ positive integers $\{t_l \mid l \neq 1, i\}$ let $u_1^\alpha, \dots, u_s^\alpha$ be those factors of f of weight r satisfying:

$$\text{sign } u_j = i, \quad d_i(u_j) = j, \quad d_l(u_j) = t_l$$

for $j = 1, \dots, s$ $l \neq 1, i$.

Then let u_0 be a simple commutator of weight r satisfying $\text{sign } u_0 = i, d_i(u_0) = 1, d_l(u_0) = t_l$ for $l \neq 1, i$. Then for each r , and each set $\{t_l\}$ $u_0^{\alpha_1 + n\alpha_2 + \dots + n^{s-1}\alpha_s}$ is a factor of A and A is the product of such factors.

B is a product of powers of simple commutators in normal form each containing at least one a_i in other than the second position.

Each factor of C will be of the form $(u')^{\alpha r}$, where $u^\alpha \mid f$ and the weight of u' is greater than the weight of u .

PROOF. The proof follows from the fact that if u is simple commutator in normal form with $\text{sign } u = i$ and $d_i(u) = j$, then $u(a_i \rightarrow a_1^n a_i) = u_0 u(a_i \rightarrow a_1^n) u' D = u_0 u' D$ where u_0 is as defined above and u' is either 1 (if $d_i(u) = 1$) or contains a_i in other than the first or second position and D is a product of factors each having greater weight than u .

THEOREM 1.12. *Let G be a metabelian p -group of class $c, p > c$ and let f be a G -subcritical function on $\{a_1, \dots, a_m\}$ in normal form. Then every factor of f is G -multilinear.*

PROOF. We will prove that if u^α is a factor of f of weight r , then $(G_{c-m+r-j+1})^\alpha = 1$ for $j = 1, \dots, c-m$ and $r = m, \dots, c$ by induction on j . It will then follow that $(G_{r+1})^\alpha = 1$.

If $j = 1$, then we need only consider the case $r = m$, since $j = 1$ and $r > m$ implies that $c-m+r-j+1 > c$. Let u^α be the (unique) factor of f of weight m and $\text{sign } i$. Now let v be a commutator of weight $c-m+1, \text{sign } 1, d_1(v) = c-m$ and $d_i(v) = 1$. Thus $v = (a_i, a_1, \dots, a_1)$. Then

$1 = f(a_i \rightarrow v) = (u')^\alpha$ where u' is of weight c , sign $u' = i$, $d_1(u') = c - m + 1$ and $d_j(u') = 1$ for $j \neq 1$. Hence $f(a_i \rightarrow v)$ is G -multilinear and by Lemma 1.9, $(G_c)^\alpha = (G_{c-m+m-1+1})^\alpha = 1$. But this result holds for all $i = 1, \dots, m$ and hence for every factor of f of weight m . Thus the theorem follows for $j = 1$.

Now assume the theorem is proved for all r and all $j < k$ and consider the substitution $a_i \rightarrow a_1^n a_i$ for a fixed $i > 1$ and fixed n . Then by Lemma 1.11 $f(a_i \rightarrow a_1^n a_i) = f(a_i \rightarrow a_1^n)ABC = ABC$ since f is G -subcritical. Now perform the substitution $a_i \rightarrow v$ with v of weight $c - m - k + 2$, $d_i(v) = 1$, $d_1(v) = c - m - k + 1$ and $v = (a_i, a_1, \dots, a_1)$. Then $(ABC)(a_i \rightarrow v) = A(a_i \rightarrow v) = A'$ since each commutator in B contains a_i in other than the first or second position and by the induction assumption $C = 1$. Further if $\alpha_1 + n\alpha_2 + \dots + n^{s-1}\alpha_s = \beta_n$ and $u_0^{\beta_n}$ is the factor of A described in Lemma 1.11 and u'_0 is defined by: sign $u'_0 = i$, $d_j(u'_0) = d_j(u_0)$ for $j > 1$ and $d_1(u'_0) = c - m - k + 1 + d_1(u_0)$, then $(u'_0)^{\beta_n}$ is a factor of A' . Thus if the weight of u_0 is t , then u'_0 has weight $t + c - m - k + 1 = t'$. By the induction hypothesis $(G_{c-m+t-(k-1)+1})^{\alpha_i} = 1$ for $i = 1, \dots, s$ and thus $(G_{t'+1})^{\beta_n} = 1$ for all factors $(u'_0)^{\beta_n}$ of A' . Thus by Theorem 1.10 $(G_{t'})^{\beta_n} = 1$ and hence $(G_{c-m+t-k+1})^{\beta_n} = 1$. Therefore if p^γ is the exponent of $G_{c-m+t-k+1}$, then allowing n to take on the values $1, 2, \dots, s$, we have

$$\begin{aligned} \alpha_1 + \alpha_2 + \dots + \alpha_s &\equiv 0(p^\gamma) \\ \alpha_1 + 2\alpha_2 + \dots + 2^{s-1}\alpha_s &\equiv 0(p^\gamma) \\ &\vdots \\ \alpha_1 + s\alpha_2 + \dots + s^{s-1}\alpha_s &\equiv 0(p^\gamma). \end{aligned}$$

But the determinant of this system of linear congruences is a product of powers of positive integers all $< s$. Thus since $p > c > s$, $\alpha_i \equiv 0(p^\gamma)$ for $i = 1, \dots, s$. Therefore $(G_{c-m+t-k+1})^{\alpha_i} = 1$ for all factors $u_i^{\alpha_i}$ of f of weight t . The same argument may be repeated for each weight and each i and thus the theorem follows by induction.

We sum up these two theorems in the following.

COROLLARY 1.13. *Let G be a metabelian p -group of class c , $p > c$ and let f be a G -subcritical function on $\{a_1, \dots, a_m\}$ in normal form.*

i) *If f is an identical relation on G , then f is equivalent to a set of relations of the form:*

$$\begin{aligned} &x^{p^{\alpha_1}} \\ &(x_1, x_2)^{p^{\alpha_2}} \\ &(y_1, y_2, y_3)^{p^{\alpha_3}} \\ &\dots \\ &(z_1, z_2, z_3, \dots, z_c)^{p^{\alpha_c}} \end{aligned}$$

where p^{α_i} is the smallest power of p which divides all exponents of factors of f of weight i .

ii) If f is a G -critical function, then $m = 2$.

The following theorems are direct consequences of the Corollary above.

THEOREM 1.14. *Let G be a finite metabelian p -group of class c , with $p > c$. Then G is critical if and only if G is a 2-generator group with cyclic center.*

PROOF. If G is critical and f is a G -critical function, then f is a function on 2 variables. Hence by Lemma 1.2 of [1,86], G is a 2-generator group and since G is a p -group G has a cyclic center.

Conversely, if G is a 2-generator group with cyclic center, then by Theorem 4.1 of [1, 93], G is critical.

THEOREM 1.15. *Let G be a metabelian p -group of class c with $p > c$ and $e(G_i) = p^{\alpha_i}$ $i = 1, \dots, c$. Then the variety generated by G is characterized by the identical relations:*

$$\begin{aligned} &x^{p^{\alpha_1}} \\ &(x_1, x_2)^{p^{\alpha_2}} \\ &\vdots \\ &(y_1, \dots, y_c)^{p^{\alpha_c}} \\ &(z_1, \dots, z_{c+1}) \\ &((u, v), (w, t)). \end{aligned}$$

PROOF. This follows directly from Corollary 1.13.

The next theorem gives the answer, in terms of numerical invariants, to the question: When do two metabelian p -groups generate the same variety?

THEOREM 1.16. *Let G and H be two metabelian p -groups of class $\leq c$ with $p > c$. Then the variety generated by G is the same as that generated by H if and only if*

$$e(G_i) = e(H_i) \text{ for } i = 1, \dots, c.$$

PROOF. The two varieties mentioned are completely determined by the integers $c, \{e(G_i)\}$.

2. A basis for the construction of all finite metabelian p -groups of class $c, p > c$

In this section we construct a class of metabelian p -groups, one for each class and exponent and show that these groups are *basic* in the sense of Definition 6.1 of [1,96]. That is, each of these is a critical group and generates a join-irreducible variety. We then show that any metabelian p -group of class $c, p > c$, is contained in the variety generated by at most c of these.

DEFINITION 2.1. Let A be the direct product of c copies of the cyclic group of order p^α , $p > c$, and let $a = a_1, a_2, \dots, a_c$ be a set of independent generators of A . We denote by $B_p(c, \alpha)$ the split extension of A by an automorphism b of order p^α , defined as follows:

$$b^{-1}a_i b = a_i a_{i+1}, \quad i = 1, \dots, c-1$$

$$b^{-1}a_c b = a_c.$$

It is easy to verify that if $p > c$, the group $B_p(c, \alpha)$ does in fact exist.

THEOREM 2.2 For each prime p and each pair of positive integers α, c , with $p > c$, the group $B_p(c, \alpha)$ is a metabelian basic p -group which generates a variety characterized by the following identical relations:

$$x^{p^\alpha}, \quad (x_1, \dots, x_{c+1}), \quad ((u, v), (r, s)).$$

PROOF. We leave to the reader the verification that $B_p(c, \alpha)$ is a 2-generator metabelian p -group of class c satisfying $e(G_i) = p^\alpha$, $i = 1, \dots, c$. It then follows from Theorem 1.15 that the identical relations above characterize its variety.

To show that $B_p(c, \alpha)$ is basic we merely note that every subvariety of the variety generated by $B_p(c, \alpha)$ must satisfy $(y_1, \dots, y_c)^{p^{\alpha-1}}$. But the identical relations which characterize the join of a collection of varieties is simply the intersection of all identical relations satisfied by each of them. Thus since $B_p(c, \alpha)$ does not satisfy $(y_1, \dots, y_c)^{p^{\alpha-1}}$ $B_p(c, \alpha)$ is basic.

The following theorem provides a ‘‘decomposition theorem’’ in the sense discussed in [2].

THEOREM 2.3. Let G be a metabelian p -group of class c , $p > c$ and let $e(G_i) = p^{\alpha_i}$, $i = 1, \dots, c$. Suppose that $\alpha_1 = \alpha_2 = \dots = \alpha_{n_1} = \beta_1$, $\alpha_{n_1+1} = \dots = \alpha_{n_2} = \beta_2, \dots, \alpha_{n_s+1} = \dots = \alpha_{n_{s+1}} = \alpha_c = \beta_{s+1}$ and $\beta_1, \dots, \beta_{s+1}$ are all different:

Then G is contained in the variety generated by $\{B_p(n_i, \beta_i) \mid i = 1, \dots, s+1\}$, and no proper subset of B_p ’s.

PROOF. We need only verify that the intersection of all identical relations of $\{B_p(n_i, \beta_i) \mid i = 1, \dots, s+1\}$ is in fact the set:

$$x^{p^{\alpha_1}}, \quad (x_1, x_2)^{p^{\alpha_1}}, \dots, (y_1, \dots, y_c)^{p^{\alpha_c}}, \quad (z_1, \dots, z_{c+1}), \quad ((u, v), (w, t)).$$

This is immediate. Hence the join of the varieties generated by the $B_p(n_i, \beta_i)$ is in fact the variety generated by G , by Theorem 1.15. If one of the B_p ’s is omitted, then for at least one j , $e(G_j) < p^{\alpha_j}$, a contradiction.

COROLLARY 2.4. Let G be a metabelian p -group of class c , $p > c$. Then G is basic if and only if G is critical and $e(G_i) = p^\alpha$ for $i = 1, \dots, c$ and fixed p^α .

PROOF. If G is critical and $e(G_i) = p^\alpha$, $i = 1, \dots, c$, then by the same argument which shows that $B_p(c, \alpha)$ is basic it follows that G is basic.

Now suppose that G is basic and that for some $i > 1$, $e(G_i) < e(G)$. Then by Theorem 2.3 the variety generated by G is the join of the varieties generated by the B_p 's which generate proper subvarieties.

References

- [1] P. M. Weichsel, 'On critical p -groups', *Proc. London Math. Soc.* (3) 14 (1964), 83–100.
- [2] P. M. Weichsel, 'On critical and basic p -groups', *Proc. Internat. Conf. Theory of Groups, Australian National Univ.*, Canberra, August 1965.
- [3] N. D. Gupta and M. F. Newman, 'On metabelian groups', *J. Australian Math. Soc.* 6 (1966), 362–368.

Institute of Advanced Studies
Australian National University
Canberra, A.C.T.

University of Illinois
Urbana, Illinois