POLYNOMIAL FUNCTIONS AND WREATH PRODUCTS[1]

BY

JOSEPH T. BUCKLEY

Introduction

We introduce the concept of a polynomial function from a group B to an abelian group A (see Definition 1). Let B be written multiplicatively and A additively and let $Z[B]$ denote the integral group ring of B. A function $f : B \to A$ can be extended to an additive homomorphism $f^* : Z[B] \to A$. In Section 1 we characterize polynomial functions by various properties of f and f^* (see Theorem 1.1). Also we show that polynomial functions $f : B \to A$ with $f(1) = 0$ must take p-elements to p-elements[2] (see Theorem 1.2).

Section 2 deals with some general results on extensions. We give necessary and sufficient conditions for an extension E of an abelian group M by a nilpotent group B to be nilpotent. This condition is formulated in terms of the action of B on M. In the split case we describe the lower central series $\{E_k\}$ of E and the series $\{Z_k(E) \cap M\}$ in terms of the action of B on M and compute the class of E in the nilpotent case. These results are well known.

We then turn our attention to wreath products in Section 3. Let A, B be groups and $F = A^{(B)}$. Then W, the standard restricted wreath product of A with B, is a split extension of F by B. We first make use of our results on polynomial functions to give a new proof of a theorem of Baumslag [1]; this theorem states that W is nilpotent if and only if B is a finite p-group and A is a nilpotent p-group of finite exponent[3]. In the case where A is abelian we are also able to describe the lower central series $\{W_k\}$ of W in terms of the action of B on F and the so-called α-central series $\{Z_k(W) \cap F\}$ of W in terms of polynomial functions. This latter result overlaps to an extent with a result of Meldrum [4]. He described the α-central series of W when both A and B are abelian in terms of a polynomial condition.

Finally we discuss the class of these nilpotent wreath products. This has been computed by Liebeck [3] and Meldrum [4] in the case where both A and B are abelian. We show that when A is abelian, it depends only on B and the exponent of A. In fact, it can be described as the class of a nilpotent ideal (the augmentation ideal) in the group ring of B over the integers modulo the exponent of A. Then by making use of work of Jennings [2] we are able to determine the class of W when A is abelian of exponent p and B is any finite p-group.

Received April 10, 1968.

[1] Presented to the American Mathematical Society at San Francisco, January 24, 1968.

[2] A p-element is an element whose order is a power of p.

[3] A p-group is a group in which every element is a p-element.

1. Polynomial functions

In this section A denotes an abelian group written additively and B an arbitrary group written multiplicatively.

DEFINITION 1. *A function $f : B \to A$ is a polynomial function of degree $\leq r$ if for each $b_1, \cdots, b_k$ in B there exist numerical polynomials $p_1, \cdots, p_t$ all of degree $\leq r$ and $a_1, \cdots, a_t$ in A such that*

$$f(b_1^{m_1} \cdots b_k^{m_k}) = \sum_1^t p_i(m_1, \cdots, m_k)a_i$$

for all integers $m_1, \cdots, m_k$.

Note. By a numerical polynomial $p(x_1, \cdots, x_k)$ we mean a polynomial with rational coefficients which is integral valued when integers are substituted for the variables. If $i = 0$, denote

$$\binom{x+i-1}{i} = 1.$$

If $i > 0$,

$$\binom{x+i-1}{i} = \frac{x\cdot(x+1)\cdots(x+i-1)}{i!}.$$

Then the product

$$\binom{x_1+i_1-1}{i_1} \cdots \binom{x_k+i_k-1}{i_k}$$

is a numerical polynomial of degree $i_1 + \cdots + i_k$. Also, it is well known that every numerical polynomial is an integral linear combination of such polynomials.

It is not difficult to show that the constant functions are precisely the polynomial functions of degree 0 and that the polynomial functions of degree 1 are those functions which are the sum of a non-zero group homomorphism and a constant function.

As before, f denotes a function $B \to A$ and f^* denotes the extension of f to an additive homomorphism $Z[B] \to A$. Here $Z[B]$ denotes the integral group ring of B and I the augmentation ideal in $Z[B]$. I is generated as an additive group by the set of all $b - 1$, b in B. Hence the ideal I^k is generated as an additive group by the set of all products $(b_1 - 1) \cdots (b_k - 1)$ where the b_i are in B. The functions from B to A form a right module, denoted A^B over the ring $Z[B]$ in the usual way. Namely, for f in A^B and b in B, f^b is the function given by $f^b(x) = f(xb^{-1})$ for x in B.

THEOREM 1.1.[4] *The following conditions are equivalent.*

(i) *$f : B \to A$ is a polynomial function of degree $\leq r$.*

(ii) *I^{r+1} is contained in the kernel of $f^* : Z[B] \to A$.*

(iii) *I^{r+1} annihilates f (considering f in the right $Z[B]$-module A^B).*

(iv) *For $b_1, \cdots, b_k$ in B*

$$f(b_1^{m_1} \cdots b_k^{m_k}) = \sum \binom{m_1+i_1-1}{i_1} \cdots \binom{m_k+i_k-1}{i_k} a_{i_1,\cdots,i_k}$$

[4] This theorem is contained in the author's Ph.D. thesis, Indiana University, 1964.

for all integers $m_1, \cdots, m_k$ *where*

$$a_{i_1,\cdots,i_k} = f^*[(1 - b_1^{-1})^{i_1} \cdots (1 - b_k^{-1})^{i_k}]$$

and the summation is over all $i_1, \cdots, i_k$ *such that* $0 \leq i_1, \cdots, i_k$ *and* $i_1 + \cdots + i_k \leq r$.

Proof. We shall prove (i) $\Rightarrow$ (ii) $\Rightarrow$ (iv) $\Rightarrow$ (i) and then (ii) $\Leftrightarrow$ (iii).

(i) $\Rightarrow$ (ii). Here we proceed by induction on r. If $r = 0$, f is a constant function. Hence $f^*(b - 1) = f(b) - f(1) = 0$ for all b in B and consequently I is contained in the kernel of f^*. Suppose the statement is true for polynomial functions of degree $\leq r - 1$ and let f have degree $\leq r$. It is sufficient to show $f^*(P(b - 1)) = 0$ for all P in I^r and b in B. Now

$$f^*(P(b - 1)) = f^*(Pb) - f^*(P) = g^*(P)$$

where $g = f^{(b^{-1}-1)}$. By our induction hypothesis we will be done after proving the following

LEMMA. *If* $f : B \to A$ *is a polynomial function of degree* $\leq r$ *and* b *in* B, *then* $g = f^{(b^{-1}-1)}$ *is a polynomial function of degree* $\leq r - 1$.

Proof.

$$\begin{aligned} g(b_1^{m_1} \cdots b_k^{m_k}) &= f(b_1^{m_1} \cdots b_k^{m_k} \cdot b) - f(b_1^{m_1} \cdots b_k^{m_k}) \\ &= \sum p_i(m_1, \cdots, m_k, 1)a_i - \sum p_i(m_1, \cdots, m_k, 0)a_i \\ &= \sum [p_i(x_1, \cdots, x_k, 1) - p_i(x_1, \cdots, x_k, 0)]a_i . \end{aligned}$$

Since degree $p_i(x_1, \cdots, x_k, x_{k+1}) \leq r$ we have

$$\text{degree } [p_i(x_1, \cdots, x_k, 1) - p_i(x_1, \cdots, x_k, 0)] \leq r - 1.$$

Hence $f^{(b^{-1}-1)}$ has degree $\leq r - 1$.

(ii) $\Rightarrow$ (iv). Here we make use of a congruence in the group ring, the proof of which we omit. Let b in B, m be an integer positive or negative or 0 and r a non-negative integer.[5] Then

$$b^m \equiv \textstyle\sum_{i=0}^{r} \binom{m+i-1}{i} (1 - b^{-1})^i \mod I^{r+1}.$$

Let $b_1, \cdots, b_k$ in B and $r \geq 0$. Using this congruence we obtain

$$b_1^{m_1} \cdots b_k^{m_k} \equiv \sum \binom{m_1+i_1-1}{i_1} \cdots \binom{m_k+i_k-1}{i_k} (1 - b_1^{-1})^{i_1} \cdots (1 - b_k^{-1})^{i_k} \mod I^{r-1}$$

for all integers $m_1, \cdots, m_k$. The summation can be restricted to those

[5] Whether m is positive, negative, or zero we denote

$$\binom{m+i-1}{i} = 1 \quad \text{if } i = 0$$

and

$$\binom{m + i - 1}{i} = \frac{m(m + 1) \cdots (m + i - 1)}{i!} \quad \text{if } i > 0.$$

$i_1, \cdots, i_k$ such that $0 \leq i_1, \cdots, i_k$ and $i_1 + \cdots + i_k \leq r$. The result (iv) now follows immediately.

(iv) $\Rightarrow$ (i). This is clear from the note following Definition 1.

(ii) $\Leftrightarrow$ (iii). Let $P = (b_1 - 1) \cdots (b_{r+1} - 1)$ where the b_i are in B and let $x \in B$. Then

$$f^P(x) = f^*[x(b_{r+1}^{-1} - 1)(b_r^{-1} - 1) \cdots (b_1^{-1} - 1)].$$

Since the ideal I^{r+1} is generated by all such P it is now clear that I^{r+1} annihilates f if and only if I^{r+1} is contained in the kernel of f^*. This completes the proof of Theorem 1.1.

LEMMA. *Let G be a group, $[G, G]$ its commutator subgroup and I the augmentation ideal in $Z[G]$. If $G/[G, G]$ has finite exponent n, then the additive group I/I^{r+1} has exponent dividing n^r.*

Proof. It is well known that the map $G \to I$ sending x to $x - 1$ induces an isomorphism $G/[G, G] \to I/I^2$. Hence $nP \in I^2$ for all P in I. The result now follows easily by induction on r.

THEOREM 1.2. *If $f : B \to A$ is a polynomial function of degree $\leq r$ with $f(1) = 0$ and $O(b) = n$, then $O(f(b))$ divides n^r.*

Proof. Let G be the cyclic subgroup of B generated by b. The restriction of f to G is also a polynomial function of degree $\leq r$. Since $f(1) = 0$, $f(b) = f^*(b - 1)$. By the above lemma, $n^r(b - 1) \in I^{r+1}$. Combining these facts with Theorem 1.1, we obtain $n^r f(b) = n^r f^*(b - 1) = f^*(n^r(b - 1)) = 0$, completing the proof. Note that in particular f takes p-elements to p-elements where p is a prime.

2. Nilpotent extensions

First we collect some notation for commutators. If $x, y \in G$, then $[x, y] = x^{-1}y^{-1}xy$. If $x_1, \cdots, x_{n+1} \in G$, then

$$[x_1, \cdots, x_{n+1}] = [[x_1, \cdots, x_n], x_{n+1}].$$

If S, T are subgroups of G, $[S, T]$ is the subgroup generated by all $[s, t]$ where $s \in S$ and $t \in T$. Also, if n is a positive integer, $[S, (n + 1)T] = [[S, nT], T]$. Finally we have the upper and lower central series of G denoted respectively by $\{Z_n(G)\}$ and $\{G_n\}$ where $Z_1(G) =$ center of G and $Z_{n+1}(G)/Z_n(G) =$ center $G/Z_n(G)$ and $G_1 = G$, $G_{n+1} = [G_n, G]$. We recall that G is nilpotent either when $G_{c+1} = 1$ for some c or $Z_c(G) = G$ for some c. In this case both series have the same length and this is called the class of G. That is, the class of G denoted nil G is the smallest positive integer such that $G_{c+1} = 1$ or $Z_c(G) = G$.

Let E be an extension of an abelian group M by a group B. Hence we can regard M as a normal subgroup of E with quotient isomorphic to B. We then have an exact sequence of groups

$$1 \rightarrow M \xrightarrow{i} E \xrightarrow{\rho} B \rightarrow 1.$$

Now M can be considered as a right B-module where the action of B on M is given by the following. If $a \in M$, $b \in B$ and $\rho(g) = b$, then $a^b = g^{-1}ag$. Again I^k denotes the k^{th} power of I the augmentation ideal in $Z[B]$. Also MI^k denotes the subgroup of M generated by the elements a^P where $a \in M$ and $P \in I^k$. If $\rho(g_i) = b_i$, then

$$a^{(b_1-1)\cdots(b_k-1)} = [a, g_1, \cdots, g_k]$$

and hence $MI^k = [M, kE]$.

In general an extension of a nilpotent group by a nilpotent group is not nilpotent. We now formulate necessary and sufficient conditions for E to be nilpotent in terms of the action of B on M. We also determine the class of E in the split case after first describing the lower central series of E. The proofs of these well-known facts are omitted.

THEOREM 2.1. *Let E be an extension of an abelian group M by a nilpotent group B. Then E is nilpotent if and only if for some integer k, I^k annihilates M. In this case* nil $E \leqq k +$ nil B *where k is the smallest such integer.*

Now let E be a *split* extension of an abelian group M by a group B. So $M \lhd E$, $B \subset E$, $M \cap B = 1$ and $E = MB$. We shall denote all this by $E = [M]B$. Again we have the induced action of B on M making M a right B-module.

THEOREM 2.2. *Let $k \geqq 1$. Using the above notation,*

(i) $E_{k+1} = [MI^k]B_{k+1}$.

(ii) $Z_k(E) \cap M = \{a \mid a \in M$ *and* I^k *annihilates* $a\}$.

We conclude this section with a corollary which follows immediately from Theorem 2.2.

COROLLARY 2.3. *If E is a nilpotent split extension of an abelian group M by a nilpotent group B of class c and k is the smallest integer for which I^k annihilates M, then* nil $E = \max(k, c)$.

3. Wreath products

Let A, B be arbitrary groups. $A^{(B)}$ denotes the set of those functions f from B to A for which $f(b) = 1$ for all but a finite number of b in B. That is, $A^{(B)}$ can be considered as the restricted direct product of A with itself over the index set B. The group B operates on $A^{(B)}$ in the following way. If $b \in B$ and $f \in A^{(B)}$, $f^b(x) = f(xb^{-1})$. In this way B can be regarded as a subgroup of the automorphism group of $A^{(B)}$. The standard, restricted wreath product of A by B denoted $A\,wr B$ is by definition the relative holomorph of $A^{(B)}$ by B. That is, the elements of $A\,wr B$ can be written bf where $b \in B$ and $f \in A^{(B)}$ and multiplication is given by: $(b_1 f_1)\cdot(b_2 f_2) = (b_1 b_2)(f_1^{b_2} f_2)$. We now apply the results on polynomial functions and nilpotent extensions to give a new proof of the following theorem of Baumslag [1].

THEOREM 3.1. *$AwrB$ is nilpotent if and only if B is a finite p-group and A is a nilpotent p-group of finite exponent.*

Proof. We first assume that $AwrB$ is nilpotent and proceed to show that the conditions on A and B are satisfied. We shall denote $AwrB$ by W and $A^{(B)}$ by F. Since it is almost immediate that W has trivial center when B is infinite we can assume from the beginning that B is finite. Since A and B can both be identified with sub-groups of W, A and B are nilpotent. We now proceed by induction on the class of A. Let nil $A = 1$; that is, let A be abelian. Here the results on polynomial functions enter in. W is an extension of the abelian group F by the (finite) nilpotent group B. Since W is nilpotent we conclude by Theorem 2.1 that some power I^k of the augmentation ideal in $Z[B]$ annihilates F. Since B is finite, F is the group of *all* functions from B to A. By Theorem 1.1 we conclude that *every* function $f : B \to A$ is a polynomial function of degree $\leq k - 1$. Let $r = k - 1$. Then B, A must be p-groups for the same prime p because otherwise it would be easy to produce a function f with $f(1) = 0$ but not taking p-elements to p-elements contradicting Theorem 1.2. Furthermore A must have finite exponent, because if B has exponent p^s (we have shown B is a finite p-group), then A must have exponent dividing p^{rs}. Otherwise it would be possible to produce a function $f : B \to A$ violating Theorem 1.2 again. Suppose now that the conditions on A and B are satisfied when nil $A < n$. Assume that nil $A = n$ and $W = AwrB$ is nilpotent. Having a natural epimorphism $AwrB \to A/A_2\, wrB$ we can conclude that A/A_2 is nilpotent. Applying the case $n = 1$, we conclude that B is a finite p-group and A/A_2 is a p-group of finite exponent p^t say. We already know A is nilpotent. It is well known and easy to prove that A also has finite exponent dividing p^{nt}. This concludes the first half of the theorem. To go in the other direction we again use induction on nil A. We begin by assuming B is a finite p-group and A is an abelian p-group of finite exponent p^m. Because of Theorem 2.1 we need only show that some power I^k annihilates $F = A^B$. Since B is a finite p-group it is well known that $I^r \subset pZ[B]$ for some positive integer r. (This is the content of a theorem of Jennings [2] describing the radical of the group algebra of B over the modular field of p-elements.) Hence some power $I^k \subset p^m Z[B]$. Since F is an abelian group of exponent p^m, I^k annihilates F and consequently W is nilpotent. Suppose $AwrB$ is nilpotent when nil $A < n$ and the other conditions on A, B hold. Let A, B satisfy the conditions and nil $A = n$. We consider the extension

$$1 \to Z(A)^B \to AwrB \to A/Z(A)wrB \to 1$$

where $Z(A)$ denotes the center of A. Since nil $A/Z(A) = n - 1$ our induction hypothesis tells us that $A/Z(A)wrB$ is nilpotent. If $g \in Z(A)^B$ and

$bf \in AwrB$ then

$$g^{(bf-1)} = g^{(b-1)}. \tag{3.1}$$

This follows immediately using the fact that

$$(bf - 1) = (b - 1)(f - 1) + (b - 1) + (f - 1)$$

together with the fact that g commutes with all functions. Let I denote the augmentation ideal of $A/Z(A)wrB$ and $I(B)$ the augmentation ideal of B. By the case $n = 1$, $Z(A)wrB$ is nilpotent and hence some power $I(B)$ annihilates $Z(A)^B$. Because of (3.1) above the same power of I annihilates $Z(A)^B$. Consequently by Theorem 2.1 $AwrB$ is nilpotent. This completes the proof of Baumslag's theorem.

Before discussing the class of these nilpotent wreath products let us make some observations about the upper and lower central series of $W = AwrB$ when A is abelian and B is any finite group. Let $\mathrm{Pol}_k(B, A)$ denote the group of all polynomial functions $B \to A$ of degree $\leq k$. Here $F = A^B$ again.

THEOREM 3.2.
(i) $W_{k+1} = [FI^k]B_{k+1}$.
(ii) $Z_{k+1}(W) \cap F = \mathrm{Pol}_k(B, A)$.

Proof. W is a split extension of F by B. Hence (i) follows immediately from Theorem 2.2 and (ii) from Theorem 2.2 and Theorem 1.1. We also note that similar facts hold when B is infinite if one works with the *unrestricted* wreath product.

In the case where B is a finite abelian p-group and A is an abelian p-group of finite exponent, the class of $AwrB$ has been computed by Liebeck [3] and Meldrum [4]. Meldrum first develops a necessary and sufficient condition for a function $f : B \to A$ to be in $Z_k(W)$. His Lemma 3.2 is equivalent to a special case of Theorem 3.2 (ii) above and follows immediately from it. The computation of the class of $AwrB$ when both A and B are abelian shows that the class of $AwrB$ depends only on B and the exponent of A. We now show that this is also true when B is non-abelian by interpreting this class in an appropriate group ring of B. We first have a preliminary result.

THEOREM 3.3. *Let A be an abelian p-group of finite exponent and let B be any finite p-group. Then* nil $(AwrB)$ *is the smallest integer k such that I^k annihilates A^B.*

Proof. Since $AwrB$ is the split extension of A^B by B we have by Corollary 2.3 the fact that nil $(AwrB) = \max(k, c)$ where c is the class of B. Hence we need only show that $k \geq c$. Now making use of Theorem 1.1 again k can also be described as the smallest integer such that all functions $B \to A$ are polynomial functions of degree $\leq k - 1$. Suppose $c > k$. Then there exists $b \in B_k$, $b \neq 1$. Hence $b - 1 \neq 0$ and $b - 1 \in I^k$. Let $f : B \to A$ be any function for which $f(b) \neq f(1)$. Then $f^*(b - 1) \neq 0$. Hence $I^k \not\subset \operatorname{kernel} f^*$. This contradicts the fact that all functions $B \to A$ have degree $\leq k - 1$. Hence $c \leq k$.

We now show that k depends only on B and the exponent of A. First we collect some notation. $Z[B]$ and I are as before. $Z_{p^m}[B]$ denotes the group ring of B over Z_{p^m} the integers mod p^m and $I(p^m)$ the augmentation ideal in $Z_{p^m}[B]$, that is, the image of I under the natural homomorphism $Z[B] \to Z_{p^m}[B]$. Jennings [2] has shown that when $m = 1$ and B is a finite p-group, $I(p)$ is the radical of $Z_p[B]$ and $I(p)^l = 0$ for some l. Hence one easily concludes that $I(p^m)$ is also a nilpotent ideal in $Z_{p^m}[B]$. Let k be the smallest integer such that $I(p^m)^k = 0$. We call k the class of $I(p^m)$.

THEOREM 3.4.[6] *Let B be a finite p-group and A an abelian p-group of finite exponent p^m. Then* nil $(AwrB)$ = *class of $I(p^m)$.*

Proof. By Theorem 3.3, nil $(AwrB)$ is the smallest k such that I^k annihilates A^B. We claim that this k is just the smallest j such that $I^j \subset p^m Z[B]$ which in turn is clearly the class of $I(p^m)$. Now k is the smallest integer such that all functions $B \to A$ are polynomial functions of degree $\leq k - 1$. If $I^j \subset p^m Z[B]$ then $I^j \subset \text{kernel} f^*$ for all $f : B \to A$ and hence all functions $B \to A$ are polynomial functions of degree $\leq j - 1$. Hence $j \geq k$. Suppose $j > k$. Then $I^k \not\subset p^m Z[B]$. Since $Z[B]$ is a free abelian group on the set B, we can then produce an additive homomorphism $Z[B] \to A$ not containing I^k in its kernel and hence a function $B \to A$ of degree $> k - 1$. Hence $j = k$ and the proof is complete.

We now consider the special case $m = 1$. Let B be a finite p-group and $I(p)$ the augmentation ideal in $Z_p[B]$. We state some results of Jennings [2] adapting the notation slightly. Let

$$R_\lambda = \{x \mid x \in B \text{ and } x \equiv 1 \bmod I^\lambda(p)\}.$$

Jennings [2] characterizes the series $\{R_\lambda\}$ as the minimal central series of B

$$B = R_1 \supseteq R_2 \supseteq \cdots$$

such that $R_\lambda^p \subseteq R_{\lambda p}$. He also proves the following.

THEOREM (Jennings [2]). *If* d_λ = rank $R_\lambda / R_{\lambda+1}$, *then the class of* $I(p) = (p - 1) \sum \lambda\, d_\lambda + 1$.

Combining Theorem 3.4 with this theorem of Jennings we obtain the

COROLLARY 3.5. *Let B be a finite p-group and A an abelian group of exponent p. Then*

$$\text{nil } (AwrB) = (p - 1) \sum \lambda\, d_\lambda + 1.$$

Remarks. The determination of the class of $I(p^m)$ for $m > 1$ seems to be a

[6] Mr. Robert Sandling of the University of Chicago has recently informed me that he also has obtained this result.

much more difficult problem. On the other hand, Mr. Robert Sandling of the University of Chicago has recently informed me that he has obtained the class of $AwrB$ when B is a finite p-group and A has elementary center. Namely

$$\text{nil } (AwrB) = (\text{class } A)\cdot(\text{class } I(p)).$$

REFERENCES

1. G. BAUMSLAG, *Wreath products and p-groups*, Proc. Cambridge Philos. Soc., vol. 55 (1959), pp. 224–231.
2. S. A. JENNINGS, *The structure of the group ring of a p-group over a modular field*, Trans. Amer. Math. Soc., vol. 50 (1941), pp. 175–185.
3. H. LIEBECK, *Concerning nilpotent wreath products*, Proc. Cambridge Philos. Soc., vol. 58 (1962), pp. 443–451.
4. J. D. P. MELDRUM, *Central series in wreath products*, Proc. Cambridge Philos. Soc., vol. 63 (1967), pp. 551–567.

UNIVERSITY OF MASSACHUSETTS
AMHERST, MASSACHUSETTS