The class of a nilpotent wreath product

David Shield

Let G be a group with a normal subgroup H whose index is a
power of a prime p , and which is nilpotent with exponent a
power of p . Gilbert Baumslag (*Proc. Cambridge Philos. Soc.* 55
(1959), 224-231) has shown that such a group is nilpotent; the
main result of this paper is an upper bound on its nilpotency
class in terms of parameters of H and G/H . It is shown that
this bound is attained whenever G is a wreath product and H
its base group.

A descending central series, here called the cpp-series, is
involved in these calculations more closely than is the lower
central series, and the class of the wreath product in terms of
this series is also found.

Two tools used to obtain the main result, namely a useful basis
for a finite p-group and a result about the augmentation ideal
of the integer group ring of a finite p-group, may have some
independent interest. The main result is applied to the
construction of some two-generator groups of large nilpotency
class with exponents $8, 9$, and 25 .

Introduction

0.1 BACKGROUND

Baumslag showed in §3 of [1] that a wreath product A wr B of two groups is nilpotent if and only if for some prime p the "bottom group" A is nilpotent with exponent a power of p and the "top group" B is a finite p-group. The proof of the "if" part, in Lemma 3.8 of [1], applies to group extensions in general, not only to wreath products. Although an upper bound on the class of such extensions is implicit in the proof of Lemma 3.8, it is not stated, and is extremely high.

Liebeck [9] found the exact nilpotency class of a nilpotent wreath product A wr B in the special case where A and B are both abelian, and observed that his result provides a lower bound to the class in the general case. Since then, exact results in other special cases and improved upper and lower bounds in general have been given by Scruton [16], Meldrum [10, 11], and Morley [13] and [14]. Buckley [3] has pointed out that earlier work by Jennings [7] gives the exact class when A is cyclic of order p and B is an arbitrary finite p-group.

0.2 STATEMENT OF THE MAIN RESULT

The main results of this paper are an upper bound, in Theorem 4.6, on the class of those group extensions shown to be nilpotent by Baumslag, and the proof in Corollary 5.5 that every nilpotent wreath product has a class which attains this bound. A statement of the nilpotency class involves, for the relevant prime p , the cpp-series

$$G = \pi_1(G) \supseteq \pi_2(G) \supseteq \cdots \supseteq \pi_i(G) \supseteq \cdots$$

of a group, which is defined in 1.1 of the present paper. In a finite p-group B , this series is identical with the $\underline{K}$-series of Jennings [7]. The cpp-series of a group reaches the trivial subgroup in finitely many steps if and only if the group is nilpotent and has exponent a power of p . Such a group is said to be cpp-nilpotent, and the integer used to label the last non-trivial term of its cpp-series is called its cpp-class. Baumslag's Lemma 3.8 may thus be restated: every extension of a cpp-nilpotent group by a finite cpp-nilpotent group is cpp-nilpotent.

Suppose B is a finite p-group with cpp-class d , and for $1 \leq v \leq d$,

$$\left| \pi_v(B) \right| = p^{n(v)} \ .$$

Let $a = 1 + (p-1) \sum \{ n(v) : 1 \le v \le d \}$ and $b = (p-1)d$.

If A has nilpotency class r and cpp-class t , and if for $1 \le w \le r$ the maximum order of a commutator of weight w in A is $p^{s(w)}$, then the nilpotency class of $A \operatorname{wr} B$ is precisely

$$\max \{ aw + b(s(w)-1) : 1 \le w \le r \} \ ,$$

and the cpp-class of $A \operatorname{wr} B$ is

$$at = \max \{ awp^{s(w)} : 1 \le w \le r \} \ .$$

This result confirms the conjecture of Sandling [15] that for arbitrary positive integer e and (non-trivial) finite p-group J , the nilpotency class of $C_{p^{e-1}} \operatorname{wr} J$ is strictly less than that of $C_{p^e} \operatorname{wr} J$. Thus the "equivalent statements" of Theorem 1.3 in [15] all become theorems.

0.3 OUTLINE

In Section 1 some weight functions and associated descending central series of a group are defined. A standard basis for a finite p-group is constructed in Section 2, and in terms of this some results about products of elements in the augmentation ideal of the integer group ring are obtained in Section 3. In Section 4, these are applied to obtain the upper bounds on nilpotency class and cpp-class already described. In Section 5, non-trivial elements of maximal commutator weight and cpp-weight are constructed in a wreath product. In Section 6, it is shown that certain nilpotent wreath products have two-generator subgroups with the same nilpotency class as the whole group; hence two-generator groups of exponent 8, 9 , and 25 are constructed with nilpotency classes 39, 18 , and 11244 respectively.

0.4 NOTATION

As a general rule, lower case Greek letters are used for elements of groups and group rings, and lower case Roman letters for integers and integer-valued functions. The symbols Z, N , and N^+ respectively denote

the sets of integers, non-negative integers, and positive integers. For l in Z^+ , the underlined symbol $\underline{l}$ denotes the set $\underline{l} = \{i \in N : 0 < i < l\}$. Upper case Greek letters are used for index sets; in particular, unless otherwise specified, Γ, Δ , and Θ are *finite* index sets, *ordered* so that a product such as $\prod \{\delta_d : d \in \Delta\}$ is well-defined.

Each element, α , of a group is a commutator with one entry, α :

$$[\alpha] = \alpha .$$

If α and β are commutators in a group, then

$$[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$$

is a commutator; the family of its entries is the disjoint union of the families of entries of α and β . Left-normed notation is used; that is,

$$[\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n] = [\ldots [[\alpha_1, \alpha_2], \alpha_3], \ldots, \alpha_n] ;$$

and a sequence of repeated entries is shown as follows:

$$[\alpha, n\beta] = [\alpha, \underbrace{\beta, \ldots, \beta}_{n \text{ entries}}] .$$

1.   Weight subgroups

The definitions of this section are self-contained, but are equivalent to corresponding definitions in a more abstract setting in [17]. Some results from that reference are quoted here for later use.

1.1 DEFINITIONS

Let G be an arbitrary group, and a, b , and e integers satisfying $a \geq b \geq 0$, $a \geq 1$, and $e \in \{1, p\}$ where p is a fixed prime. These symbols will be used repeatedly with the same meaning.

A *weight relation* $\rho(a, b, e)$ is defined to be the least subset of $G \times N$ satisfying the conditions:

(i)   for all $\alpha \in G$, $(\alpha, a) \in \rho(a, b, e)$;

(ii) $(\alpha, u) \in \rho(a, b, e)$ and $(\beta, v) \in \rho(a, b, e)$ only if
      $([\alpha, \beta], u+v) \in \rho(a, b, e)$;

(iii) (a) $(\alpha, u) \in \rho(a, b, 1)$ only if $\left(\alpha^p, u+b\right) \in \rho(a, b, 1)$
and

(b) $(\alpha, u) \in \rho(a, b, p)$ only if $\left(\alpha^p, pu\right) \in \rho(a, b, p)$;

(iv) $(\alpha, u) \in \rho(a, b, e)$ and $(\beta, v) \in \rho(a, b, e)$ only if $(\alpha\beta, \min\{u, v\}) \in \rho(a, b, e)$; and

(v) $(\alpha, u) \in \rho(a, b, e)$ only if $\left(\alpha^{-1}, u\right) \in \rho(a, b, e)$.

A function $w^e_{a,b}$ from G to $Z^+ \cup \{\infty\}$ is then defined by the statement that for all φ in G ,

$$w^e_{a,b}(\varphi) = \begin{cases} \max\{u : (\varphi, u) \in \rho(a, b, e)\} \text{ if this maximum exists,} \\ \\ \infty \qquad\qquad\qquad\qquad \text{if no such maximum exists.} \end{cases}$$

The value $w^e_{a,b}(\varphi)$ is called the (a, b, e)-weight of φ .

For arbitrary v in Z^+ , the *weight subgroup* $\gamma^{a,b,e}_v(G)$ is defined by

$$\gamma^{a,b,e}_v(G) = \left\{\varphi \in G : w^e_{a,b}(\varphi) \geq v\right\} .$$

This set is readily checked to be a fully invariant subgroup.

Two special cases merit particular attention. Let $\gamma_i(G) = \gamma^{1,0,1}_i(G)$ and $\pi_i(G) = \gamma^{1,0,p}_i(G)$. Then $\gamma_i(G)$ is the ith term of the lower central series of G , and $\pi_i(G)$ is the ith term of the cpp-series mentioned in the introduction. From the definition,

$$\left[\pi_i(G), \pi_j(G)\right] \subseteq \pi_{i+j}(G)$$

and

$$\left(\pi_i(G)\right)^p \subseteq \pi_{ip}(G) ,$$

and it is not hard to show, by induction, that

$$G = \pi_1(G) \supseteq \pi_2(G) \supseteq \cdots \supseteq \pi_i(G) \supseteq \cdots$$

is the most rapidly-descending series with the properties.

If for some positive integer d ,

$$\pi_d(G) \supset \pi_{d+1}(G) = \{1\} \ ,$$

then G is said to be *cpp-nilpotent* with *cpp-class* d . It is easy to
see that a group is cpp-nilpotent if and only if it is nilpotent and has
exponent a power of p . In this case, each (a, b, e)-series reaches the
trivial subgroup in a finite number of steps, and the index of the last
non-trivial subgroup is called the (a, b, e)-class of the group.

Each of the next two results follows from the corresponding result in
[17] by application of Lemma 3.4 of [17].

1.2   LEMMA   ([17], Theorem 6.6)

Every element φ of G may be expressed in the form

$$\varphi = \prod \left\{ \kappa_g p^{h(g)} \ : \ g \in \Gamma \right\}$$

where each κ_g is a commutator in G with

$$w_{1,0}^1(\kappa_g) = w(g) \ ,$$

*and $h(g)$ is a non-negative integer such that for all a and b
described earlier,*

$$w_{a,b}^1(\varphi) \le aw(g) + bh(g)$$

and

$$w_{a,b}^p(\varphi) \le aw(g)p^{h(g)} \ .$$

1.3   COROLLARY   ([17], Corollary 6.7)

*The weight subgroup $\gamma_i^{a,b,e}(G)$ is generated modulo $\gamma_{i+1}^{a,b,e}(G)$ by
elements of the form κ^{p^h} where κ is a commutator of weight u in G
and, for $e = 1$,*

$$au + bh = i \ ,$$

or, for $e = p$,

$$aup^h = i \ .$$

2. A basis for a finite p-group

This section leads up to the proof that every finite p-group has a basis with certain desirable properties (Theorem 2.4).

2.1 DEFINITIONS AND NOTATION

Throughout Section 2, let p be an arbitrary prime and P a group of p-power order with cpp-class $\big((1,\, 0,\, p)\text{-class}\big)$ d . For $1 \leq v \leq d$, define $n(v)$ by the relation

$$\big|\pi_v(P)\big| = p^{n(v)} \ .$$

Further, let

$$a = 1 + (p\text{-}1) \sum \{n(v) \,:\, 1 \leq v \leq d\}$$

and

$$b = (p\text{-}1)d \ .$$

A *basis* for P is a set $\big\{\big(\tau_i,\, h(i)\big) \,:\, i \in M\big\}$ where M is a finite ordered index set and for i in M , $\tau_i \in P$ and $h(i) \in Z^+$, such that every element of P may be written uniquely in the form

$$\textstyle\prod \left\{\tau_i^{e(i)} \,:\, i \in M\right\}$$

with $0 \leq e(i) < p^{h(i)}$ for i in M . This will be called the standard form of the element relative to the basis.

It was shown by Sylow [18] (Théorème III, p. 588) that every group of order p^n , for n in Z^+ , has a basis with $|M| = n$ and $h(i) = 1$ for i in M .

Let $T = \big\{\big(\tau_i,\, h(i)\big) \,:\, i \in M\big\}$ be a basis for P . For each i in M , let

$$q(i) = p^{h(i)} \ ,$$

$$q^*(i) = p^{h(i)-1} ,$$

and

$u(i)$ be the integer such that $\tau_i \in \gamma_{u(i)}(P) \setminus \gamma_{u(i)+1}(P)$.

Corresponding to a basis T of P and a term $\pi_v(P)$ of the cpp-series of P , let $m(v, T)$ be the cardinality of the set of ordered pairs

$$\{(i, j) : i \in M, j \in \underline{h(i)}, \text{ and } u(i)p^j \geq v\} .$$

$\left(\text{Note that for each pair } (i, j) \text{ in this set, } \tau_i^{p^j} \in \pi_v(P) .\right)$ From the independence of the basis elements, $m(v, T) \leq n(v)$. From this it follows that:

$$a = 1 + (p-1) \sum \{n(v) : 1 \leq v \leq d\}$$

$$\geq 1 + (p-1) \sum \{m(v, T) : 1 \leq v \leq d\}$$

$$= 1 + (p-1) \sum \{v\big(m(v, T)-m(v+1, T)\big) : 1 \leq v \leq d\}$$

$$= 1 + \sum \{(p-1)u(i)p^j : i \in M, j \in \underline{h(i)}\}$$

$$= 1 + \sum \{u(i)\big(q(i)-1\big) : i \in M\} .$$

A basis is said to be π-respecting if the relation

$$\prod \left\{\tau_i^{e(i)} : i \in M\right\} \in \pi_v(P)$$

implies that for all i in M , $\tau_i^{e(i)} \in \pi_v(P)$. Such a basis can clearly be constructed by combining coset representatives of bases for the factors in the cpp-series.

A stronger property is defined as follows:

A basis T for P is π-form-respecting if the relation $\prod \left\{\tau_i^{e(i)} : i \in M\right\} \in \pi_v(P)$ implies that for each i in M there exists an integer $s(i)$ such that $p^{s(i)} | e(i)$ and $u(i)p^{s(i)} \geq v$.

Clearly a basis T for P is π-form-respecting if and only if for $1 \leq v \leq d$, $m(v, T) = n(v)$; whence

$$a = 1 + \sum \left\{ u(i)\big(q(i)-1\big) \; : \; i \in M \right\} \; .$$

Also, this definition requires that each basis element τ_i have

$(1, 0, 1)$-weight equal to its $(1, 0, p)$-weight.

In general, a permutation of a basis for a finite p-group is not

necessarily a basis. For example, the dihedral group of order 8 ,

$$\langle a, b \; : \; a^4 = b^2 = (ab)^2 = 1 \rangle$$

has a basis with $\tau_1 = ab$, $\tau_2 = a$, $\tau_3 = a^2 b$, and $h_1 = h_2 = h_3 = 1$;

yet setting $\tau_1 = a$, $\tau_2 = ab$, and $\tau_3 = a^2 b$ does not give a basis. On

the other hand, though this will not be proved here, every permutation of a

π-respecting basis is again a π-respecting basis. In Section 5 the

following property will be used.

A basis is *ordered* if

$$i, j \in M \; , \quad i < j \; , \quad \text{only if} \;\; u(i)q(i) \leq u(j)q(j) \; .$$

2.2   THE REFINED cpp-SERIES

In order to prove the existence of an ordered, π-form-respecting

basis for an arbitrary finite p-group, it appears necessary to prove the

existence of a basis with an even stronger property. A refinement of the

cpp-series is defined by setting, in an arbitrary group G ,

$$\lambda_{w,v}(G) = \left\{ \varphi \in G \; : \; \text{either} \;\; w_{1,0}^p(\varphi) > v \;\; \text{or} \;\; w_{1,0}^p(\varphi) = v \;\; \text{and} \;\; w_{1,0}^1(\varphi) \geq w \right\} \; .$$

This gives:

$$\pi_v(G) = \lambda_{1,v}(G) \supseteq \lambda_{2,v}(G) \supseteq \cdots \supseteq \lambda_{v,v}(G) \supseteq \lambda_{v+1,v}(G) = \pi_{v+1}(G) \; .$$

If $v = up^s$ where $p \nmid u$, then at most s distinct new subgroups can be

introduced between $\pi_v(G)$ and $\pi_{v+1}(G)$, since Corollary 1.3 makes it

clear that for $0 \leq t \leq s$, the subgroup $\lambda_{up^t,v}(G)$ is generated modulo

$\lambda_{up^{t+1},v}(G)$ by the p^{s-t}th powers of commutators with $(1, 0, 1)$-weight

up^t . All subgroups $\lambda_{w,v}(G)$ with $1 \leq w \leq u$ are equal to $\pi_v(G)$, and

for $1 \leq t \leq s$, all subgroups $\lambda_{w,v}$ with $up^{t-1} < w \leq up^t$ are equal to $\lambda_{up^t,v}(G)$.

A basis T for P will be called a *standard basis* if it has the properties:

(a)   it is *ordered* in the sense defined at the end of 2.1;

(b)   each element τ_i is a commutator of weight $u(i)$ in P ; and

(c)   the relation $\prod \left\{ \tau_i^{e(i)} : i \in M \right\} \in \lambda_{w,v}(P)$ implies that for each i in M there exists an integer $s(i)$ such that $p^{s(i)} | e(i)$ and either $u(i)p^{s(i)} > v$ or $u(i)p^{s(i)} = v$ and $u(i) \geq w$.

Property (c) (which could be called being "λ-form-respecting") implies the property of being π-form-respecting. Properties (a) and (b) require negligible extra effort in the existence proof, and are convenient to have.

A generalisation of Theorem 3.2 of Hall [4] is required; a proof is given in Lemma 3.4 of [17].

2.3   LEMMA

Let $\{\varphi_i : i \in \Gamma\}$ *be a set of elements of a group* G *, and* h *a positive integer. Then*

$$\left[\prod \{\varphi_i : i \in \Gamma\} \right]^{p^h} = \prod \left\{ \varphi_i^{p^h} : i \in \Gamma \right\} \prod \left\{ \delta_d^{p^{h(d)}} : d \in \Delta \right\} ,$$

where each δ_d *is a commutator with at least* $\max\{2, p^{h-h(d)}\}$ *entries from the set* $\{\varphi_i : i \in \Gamma\}$.   □

The main theorem of this section follows.

2.4 THEOREM

Every finite p-group has a standard basis.

Proof. In the finite p-group, P, let

$$|\lambda_{w,v}(P)| = p^{n(w,v)} .$$

The proof proceeds by induction in the reverse direction along the refined cpp-series of P to show that each term $\lambda_{w,v}(P)$ of that series has a

basis $T_{w,v} = \left\{ \left(\tau_i^{t(w,v,i)}, h(w,\ v,\ i) \right) : i \in M_{w,v} \right\}$ such that

(a) for all i in $M_{w,v}$, τ_i is a commutator of weight $u(i)$

in P ;

(b) for all i in $M_{w,v}$, there exists a non-negative integer

$r(w,\ v,\ i)$ such that $t(w,\ v,\ i) = p^{r(w,v,i)}$;

(c) for all i in $M_{w,v}$, either

(i) $v \leq u(i)t(w,\ v,\ i) < pv$, or

(ii) $u(i)t(w,\ v,\ i) = pv$ and $u(i) < w$, or

(iii) $t(w,\ v,\ i) = 1$;

(d) if i precedes j in $M_{w,v}$, then

$$u(i)t(w,\ v,\ i)p^{h(w,v,i)} \leq u(j)t(w,\ v,\ j)p^{h(w,v,j)} ;$$

and

(e) for all $(y,\ x)$ such that $\lambda_{y,x}(P) \subseteq \lambda_{w,v}(P)$,

$$m\big(y,\ x,\ T_{w,v}\big) = n(y,\ x) .$$

Here $m\big(y,\ x,\ T_{w,v}\big)$ is defined to be the cardinality of the set of ordered pairs:

$$\left\{ (i,\ j) : i \in M_{w,v},\ j \in \underline{h}(w,\ v,\ i),\ \text{and either}\ u(i)t(w,\ v,\ i)p^j > x \right.$$

$$\left. \text{or}\ u(i)t(w,\ v,\ i)p^j = x\ \text{and}\ u(i) \geq y \right\} .$$

Conditions (b) and (c) show that for all i in $M_{1,1}$,

$t(1, 1, i) = 1$; so that by condition (a), each basis element of $T_{1,1}$ may be written as a commutator of weight $u(i)$ in P , as required. Condition (d) shows that $M_{1,1}$ is ordered in the way required of M . Finally, condition (e) for the basis $T_{1,1}$ is equivalent to the condition that $T_{1,1}$ is λ-form-respecting. Thus if $T_{1,1}$ is constructed with the properties claimed for it, then the choice $M = M_{1,1}$, $h(i) = h(1, 1, i)$ for each i in M , and hence $T = T_{1,1}$, establishes the truth of the theorem.

The inductive hypothesis is vacuously true for $\lambda_{1,d+1}(P) = E$.

Let $\lambda_{w,v}(P)$ be an arbitrary non-trivial term of the refined cpp-series of P , and suppose the hypothesis established for all terms $\lambda_{w',v'}(P)$ of the series such that either $v' > v$ or $v' = v$ and $w' > w$.

Consider first of all the case $w = v + 1$, and recall that $\lambda_{v+1,v}(P) = \pi_{v+1}(P) = \lambda_{1,v+1}(P)$. By assumption, $\lambda_{1,v+1}(P)$ has a basis $T_{1,v+1}$ with appropriate properties. Let $M_{v+1,v} = M_{1,v+1}$, and for i in $M_{v+1,v}$ let $t(v+1, v, i) = t(1, v+1, i)$ and $h(v+1, v, i) = h(1, v+1, i)$. Then $T_{v+1,v}$ is identical with $T_{1,v+1}$, and so is a basis for $\lambda_{v+1,v}(P)$. Clearly $T_{v+1,v}$ inherits properties (a), (b), (d), and (e) from $T_{1,v+1}$; that it also inherits property (c) will now be shown. All indices i in $M_{1,v+1}$ satisfying condition (c) (iii) for $T_{1,v+1}$ satisfy the corresponding condition for $T_{v+1,v}$. No index i can satisfy condition (c) (ii) for $T_{1,v+1}$, since $u(i) \geq 1$ for all i in $M_{1,v+1}$. So if $t(1, v+1, i) \neq 1$, then $v + 1 \leq u(i)t(1, v+1, i) < p(v+1)$. Also by condition (b), $p \mid t(1, v+1, i)$, whence

$$v + 1 \leq u(i)t(1, v+1, i) \leq p(v+1) - p = pv .$$

If $u(i)t(1, v+1, i) < pv$, then i satisfies condition (c) (i) for $T_{v+1,v}(P)$. Otherwise,

$$u(i)t(1,\ v\text{+}1,\ i) = pv$$

and

$$u(i) = pv/t(1,\ v\text{+}1,\ i) \leq pv/p < v + 1\ ,$$

so that condition (c) (ii) for $T_{v\text{+}1,v}(P)$ is satisfied.

A step of the type considered involves only a change in notation. Consider now the case $1 \leq w \leq v$, where a basis $T_{w\text{+}1,v}$ for $\lambda_{w\text{+}1,v}(P)$ is known to exist and to have appropriate properties. As the second subscript on each symbol $T,\ M,\ t,\ r,\ h$, and m remains equal to v throughout the following construction, it will be omitted for the sake of reducing the notational complexity. The construction of T_w now takes place in two stages.

In the first stage, let

$$\Gamma = \big\{i \in M_{w\text{+}1}\ :\ u(i) = w,\ u(i)t(w,\ i) = pv\big\}$$

and note that for i in Γ , $t(w,\ i) \geq p$ since $w \leq v$. For i in Γ , let $r(w,\ i) = r(w\text{+}1,\ i) - 1$ and $h(w,\ i) = h(w\text{+}1,\ i) + 1$, and for i in $M_{w\text{+}1}\backslash\Gamma$, let $r(w,\ i) = r(w\text{+}1,\ i)$ and $h(w,\ i) = h(w\text{+}1,\ i)$. For all i in $M_{w\text{+}1}$, let $t(w,\ i) = p^{r(w,i)}$. Now define

$$T_w^* = \left\{\left(\tau_i^{t(w,i)},\ h(w,\ i)\right)\ :\ i \in M_{w\text{+}1}\right\}\ .$$

Let $\lambda_{w,v}^*(P)$ be the set of elements of P which may be written in the form $\prod\left\{\tau_i^{t(w,i)e(i)}\ :\ i \in M_{w\text{+}1}\right\}$, where for i in $M_{w\text{+}1}$, $0 \leq e(i) < p^{h(w,i)}$. Then $\lambda_{w,v}^*(P)$ contains $\lambda_{w\text{+}1,v}(P)$ and is a subgroup of P ; in fact a normal subgroup, since $\lambda_{w,v}^*(P)$ is contained in $\lambda_{w,v}(P)$ and

$$\lambda_{w,v}(P)/\lambda_{w\text{+}1,v}(P) \quad \text{is central in} \quad P/\lambda_{w\text{+}1,v}(P)\ .$$

If $\lambda_{w,v}^*(P)$ were equal to $\lambda_{w,v}(P)$, then M_w would be chosen equal to $M_{w\text{+}1}$, and the construction of $T_w = T_w^*$ would be complete. Otherwise,

the elementary abelian subgroup $\lambda_{w,v}(P)/\lambda_{w,v}^*(P)$ is generated by cosets

each having as a representative the p^rth power of a commutator of weight

w in P, where $wp^r = v$ (Lemma 1.3). In the second stage of the

construction, a subset $\left\{\tau_i^{t(i)} : i \in M_w \backslash M_{w+1}\right\}$ of these representatives is

selected in such a way that the corresponding cosets constitute a basis for

$\lambda_{w,v}(P)/\lambda_{w,v}^*(P)$. Here M_w is an ordered set such that all elements of

$M_w \backslash M_{w+1}$ precede all elements of M_{w+1}. For i in $M_w \backslash M_{w+1}$, let

$u(i) = w$ (the weight of the commutator τ_i in P), let

$t(w, i) = p^{r(w,i)} = p^r$, and let $h(w, i) = 1$. Then the construction of

$$T_w = \left\{\left(\tau_i^{t(w,i)}, h(w, i)\right) : i \in M_w\right\}$$

is complete.

The next stage of the proof is to show that T_w^* is a basis for

$\lambda_{w,v}^*(P)$. For this, it is sufficient to show that the elements

$\left\{\tau_i^{t(w,i)} : i \in \Gamma\right\}$ are independent modulo $\lambda_{w+1,v}(P)$, that is, to show

that if

(*) $\prod \left\{\tau_i^{t(w,i)e(i)} : i \in \Gamma\right\} \in \lambda_{w+1,v}(P)$

with $0 \le e(i) < p$ for each i in Γ, then $e(i) = 0$ for each i in

Γ. Lemma 2.3 shows that

$$\left[\prod \left\{\tau_i^{t(w,i)e(i)} : i \in \Gamma\right\}\right]^p = \prod \left\{\tau_i^{pt(w,i)e(i)} : i \in \Gamma\right\} \prod \{\psi_d : d \in \Delta\},$$

where for d in Δ, $\psi_d \in \lambda_{pw,pv}(P) \subseteq \lambda_{w+1,pv}(P)$. The same lemma gives:

$$\left(\lambda_{w+1,v}(P)\right)^p \subseteq \lambda_{w+1,pv}(P) .$$

Hence from the relation (*) it follows that

$$\prod \left\{\tau_i^{pt(w,i)e(i)} : i \in \Gamma\right\} = \prod \left\{\tau_i^{t(w+1,i)e(i)} : i \in \Gamma\right\} \in \lambda_{w+1,pv}(P) .$$

Now property (e) of T_{w+1} shows that for all i in Γ, $p|e(i)$; so if

$0 \leq e(i) < p$, then $e(i) = 0$, as required.

The fact that T_w is a basis for $\lambda_{w,v}(P)$ is now an immediate consequence of the fact that

$$\left\{ \prod \left\{ \tau_i^{t(w,i)e(i)} \; : \; i \in M_w \backslash M_{w+1} \right\} \; : \; 0 \leq e(i) < p \quad \text{for} \quad i \in M_w \backslash M_{w+1} \right\}$$

is a complete set of coset representatives for $\lambda_{w,v}^*(P)$ in $\lambda_{w,v}(P)$.

The final stage of the proof is a verification that the basis T_w has the properties (a) to (e) listed at the start of this proof. It is clear from the construction that (a), (b), and (d) are satisfied. For j in Γ or in $M_w \backslash M_{w+1}$, it is clear that $u(j)t(w, j) = v$, so that condition (c) (i) is satisfied. Those j in M_{w+1} which satisfy condition (c) (i) or (c) (iii) for T_{w+1} clearly satisfy the same condition for T_w , and those which satisfy condition (c) (ii) for T_{w+1} either satisfy the same condition for T_w or are contained in Γ .

It is clear from the way in which the basis elements were constructed that

$$m\left(w, \; v, \; T_{w,v}\right) = n(w, \; v) \; ;$$

and if $\lambda_{y,x}(P) \subseteq \lambda_{w+1,v}(P)$, then

$$m\left(y, \; x, \; T_{w,v}\right) = m\left(y, \; x, \; T_{w+1,v}\right)$$
$$= n(y, \; x) \; ,$$

so that condition (e) is also satisfied.   □

3.   Some results in the integer group ring of a finite p-group

A standard basis for a finite p-group, constructed in Section 2, gives rise to standard sets of generators for the integer group ring of the group, and for its augmentation ideal. Most of the following lemmas discuss products of these generators, particularly products with repeated factors.

3.1   PRELIMINARIES

Again let P be a group whose order is a power of a prime, p, and let $T = \left\{\left(\tau_i, h(i)\right) : i \in M\right\}$ be a standard basis for P. Let S be the ordered set of "permissible powers" of basis elements

$$S = \left\{\tau_i^{p^r} : i \in M \text{ and } r \in \underline{h(i)}\right\}$$

with lexicographical order on the pairs (i, r). For $1 \le v \le d$, let S_v be the sub-ordered-set of S containing those $n(v)$ elements $\tau_i^{p^r}$ such that $u(i)p^r \ge v$. Each element of S may be paired with the integer 1 to give a basis which is a "refinement" of T, say

$$T' = \left\{\left(\theta_j, 1\right) : j \in \underline{n}\right\}$$

where $n = n(1)$ so that p^n is the order of P. Now every element of P may be written uniquely in the form

$$\prod \left\{\theta_j^{e(j)} : j \in \underline{n}\right\} \text{ where for } j \text{ in } \underline{n}, \ 0 \le e(j) < p.$$

The basis T' is π-respecting, but not π-form-respecting.

In the integer group ring $\mathbb{Z}P$, the augmentation ideal I is generated additively by the set $\{\varphi - 1 : \varphi \in P\}$. It is well-known that if $\{\delta_i : i \in \Delta\}$ is an arbitrary finite ordered set of elements in a ring, then

$$(*) \qquad \prod \{\delta_i : i \in \Delta\} - 1 = \sum \left\{\prod \{\delta_i - 1 : i \in \Gamma\} : \Gamma \subseteq \Delta\right\},$$

the sum on the right-hand side being over all sub-ordered-sets Γ of Δ. Hence I is generated additively by the $p^n - 1$ non-trivial elements in the set

$$(**) \qquad \left\{\prod \left\{(\theta_i - 1)^{e(i)} : i \in \underline{n}\right\} : 0 \le e(i) < p \text{ for } i \text{ in } \underline{n}\right\};$$

in fact, these constitute a basis for I. If the element 1 is adjoined to this set, still with 0 omitted, then it constitutes a basis for $\mathbb{Z}p$.

Thus I is generated as a ring by the set

$$S^* = \{(\theta - 1) : \theta \in S\} \; .$$

A (possibly empty) product of elements of S^* without restriction on their order will be called a *monomial* in I ; but it should be noted that the empty product is, by convention, the element 1 which is not in I .

The *weight* of a monomial

$$\chi = \left(\tau_{i(1)}^{p^{r(1)}} - 1 \right) \left(\tau_{i(2)}^{p^{r(2)}} - 1 \right) \; \cdots \; \left(\tau_{i(m)}^{p^{r(m)}} - 1 \right)$$

is defined to be

$$w(\chi) = \sum \left\{ u(i(l)) p^{r(l)} : 1 \le l \le m \right\} \; .$$

The *profile* of the same monomial χ is defined to be a function f from the set $\{v \in \mathbb{Z} : 1 \le v \le d\}$ to $\mathbb{N}$ such that for $1 \le v \le d$ there are precisely $f(v)$ factors $\left(\tau_{i(l)}^{p^{r(l)}} - 1 \right)$ in χ such that $u(i(l)) p^{r(l)} = v$. Note that $\sum \{f(v) : 1 \le v \le d\} = m$ and

$\sum \{v f(v) : 1 \le v \le d\} = w(\chi)$.

A profile f_1 is *heavier* than profile f_2 if there exists an integer v such that $1 \le v \le d$ and if $v < v' \le d$, then $f_1(v') = f_2(v')$ and $f_1(v) > f_2(v)$.

The first result to be proved is quite trivial. It is given here for easy reference in the proof of later lemmas.

3.2 LEMMA

Let χ_1 *and* χ_2 *be monomials in* I *and* ψ *an arbitrary element of* $\mathbb{Z}P$. *Then*

$$\chi_1 \psi \chi_2 = \sum \{\chi_g : g \in \Gamma\}$$

where for each g *in* Γ , χ_g *is a monomial with weight at least* $w(\chi_1) + w(\chi_2)$ *and profile at least as heavy as the (pointwise) sum of the profiles of* χ_1 *and* χ_2 .

Proof. The element ψ may be expressed as a linear combination of 1 and elements of the form $\psi_i - 1$ where $\psi_i \in G$. Each ψ_i may then be expressed in standard form relative to the basis T, and by the relation (*) in 3.1, each $(\psi_i - 1)$ is expressed as a sum of monomials in I. When the resulting expression for ψ is substituted into $\chi_1 \psi \chi_2$, the distributive laws immediately give the required result.   □

3.3 LEMMA

Let θ be an arbitrary element of $\pi_v(P)$. Then

$$\theta - 1 = \sum \{\chi_g : g \in \Gamma\} ,$$

where each χ_g is a monomial with profile f_g such that

$$f_g(u) = 0 \quad for \quad 1 \le u \le v ,$$

and

$$v \le w(\chi_g) \le a - 1 .$$

Proof. If $\theta = 1$ then Γ is empty. If $\theta \ne 1$, then in the standard expression for θ in terms of the bases T', each factor $\theta_j^{e(j)}$ is such that the monomial $(\theta_j - 1)$ has weight at least v. The required result follows immediately from the identity (*) in 3.1 above and the definition of the integer a in 2.1.   □

3.4 LEMMA

Let θ and τ be elements of S_u and S_v respectively. Then

$$(\tau - 1)(\theta - 1) = (\theta - 1)(\tau - 1) + \sum \{\chi_g : g \in \Gamma\} ,$$

where each χ_g is a monomial, with profile f_g, and there exists an integer x_g such that

$$x_g \ge u + v$$

and

$$f(x_g) \geq 1 \; .$$

Consequently, the weight of χ_g *is at least that of* $(\tau-1)(\theta-1)$ *, and its profile is heavier.*

Proof. Note that $[\tau, \theta] \in \pi_{u+v}(G)$. The well-known identity

$$(\tau-1)(\theta-1) = (\theta-1)(\tau-1) + \theta\tau([\tau, \theta]-1) \; ,$$

together with Lemmas 3.2 and 3.3, gives the required result.   □

3.5 COROLLARY

Let $\chi = \prod \{(\theta_{j(i)}-1) : i \in \underline{m}\}$ *be a monomial,* $\underline{\delta}$ *a permutation of* $\underline{m}$ *, and* $\chi' = \prod \{(\theta_{j(i\underline{\delta})}-1) : i \in \underline{m}\}$ *.   Then*

$$\chi = \chi' + \sum \{\chi_g : g \in \Gamma\} \; ,$$

where each χ_g *is a monomial such that* $w(\chi_g) \geq w(\chi)$ *and the profile of* χ_g *is heavier than the profile of* χ *.*

Proof. The permutation $\underline{\delta}$ is equal to a product of transpositions of adjacent integers in $\underline{m}$. For each such transposition, Lemma 3.4 and then the distributive law is applied.   □

Note that if the permutation has the purpose of gathering together factors equal to $(\theta-1)$ where $\theta \in S_v$, then each transposition involves a factor $(\theta-1)$, and the profile of each χ_g differs from that of χ on an integer greater than v .

The next step is to consider powers of a monomial factor $\theta - 1$ in the two succeeding lemmas. The first is not restricted to monomials.

3.6 LEMMA

For arbitrary θ *in* $\mathbb{Z}P$ *, there exists* ψ *in* $\mathbb{Z}P$ *such that*

$$(\theta-1)^p = (\theta^p-1) + p(\theta-1)\psi \; .$$

Proof. When $p = 2$, the result holds with $\psi = -1$. When p is odd, the first and last terms in a binomial theorem expansion of the left-hand side give $\theta^p - 1$, and the coefficients of the intermediate terms are

all divisible by p and have zero sum. Thus p and $(\theta-1)$ are both
factors of the sum of the intermediate terms, as required.   □

3.7   LEMMA

Let χ be a monomial with $l \geq p$ factors equal to $\theta - 1$, where
$\theta \in S_v$. Then

$$\chi = \sum \{\chi_g : g \in \Gamma\} + p \sum \{\chi_d : d \in \Delta\} ,$$

where each χ_g is a monomial with a profile heavier than that of χ ,
differing from it on an integer greater than v , and $w(\chi) \leq w(\chi_g)$;
and each χ_d is a monomial with at least as many factors equal to $\varphi - 1$
as has χ for each φ in $S\backslash\{\theta\}$, and with at least $l - p + 1$ factors
equal to $(\vartheta-1)$, so that

$$w(\chi) - (p-1)v \leq w(\chi_d) .$$

Proof. By Lemma 3.5 and the comment following it, the factors of χ
may be rearranged so that those equal to $\theta - 1$ are together, modulo a
sum of monomials satisfying the conditions required of monomials χ_g .

Lemma 3.6 is applied to a factor $(\theta-1)^p$, and the distributive law to the

resulting expression. Since $\theta^p \in \pi_{pv}(P)$, Lemma 3.3 shows that the

monomial with $\theta^p - 1$ as a factor satisfies the conditions required of
monomials χ_g . The remaining expression is a product of p with an
element ψ in P and a monomial which satisfies the conditions required
of χ_d . The proof of Lemma 3.2 shows that this whole product may be
expressed in the required form.   □

For the statement of the next lemma, recall that a and b are the
parameters for P defined in 2.1.

3.8   LEMMA

If χ is a monomial with $w(\chi) \geq a$, then $\chi = p \sum \{\chi_d : d \in \Delta\}$
where each χ_d is a monomial with

$$w(\chi) - b \leq w(\chi_d) .$$

Proof. Since

$$w(\chi) \geq a = 1 + (p\text{-}1) \sum \{u(i)p^r : i \in M, \; r \in \underline{h(i)}\} \; ,$$

there must be at least one pair (i, r) such that χ has more than $p - 1$ factors equal to $\left[\tau_i^{p^r} \text{-}1 \right]$. Let (i, r) be such a pair, chosen so that $u(i)p^r$ is maximal.

Proceed by induction on the profile, f , of χ . If $f(d) > (p\text{-}1)n(d)$, then $u(i)p^r = d$. When Lemma 3.7 is applied, since the profile of each resulting χ_g cannot differ on an integer greater than d , the set Γ must be empty; and the result follows immediately when it is noted that $b = (p\text{-}1)d$.

If $f(d) \leq (p\text{-}1)n(d)$, suppose the result already established for all monomials with profiles heavier than f . Lemma 3.7, together with this inductive hypothesis, gives the required result, since $(p\text{-}1)v \leq b$.   □

4.   An upper bound on the nilpotency class and cpp-class of some group extensions

The relevance of the integer group ring results of Section 3 to the problem at hand is shown in Sub-section 4.1 and Lemma 4.2. The restriction there to splitting extensions is avoided in the main result, Lemma 4.5, by an appeal to an embedding theorem quoted here as Lemma 4.4. Theorem 4.6 restates the main result in more useful terms.

4.1 PRELIMINARIES

Let G be a group which splits over a normal subgroup H whose index is a power of a prime p , and let J be a complement for H in G . Elements of J act naturally on H ; in particular if $\rho \in H$ and $\tau \in J$ then

$$[\rho, \tau] = \rho^{-1+\tau} \; .$$

However, if H is not abelian, these actions with the natural definitions of addition and multiplication do not generate a ring; addition is not commutative, and the distributive laws fail.

Let a and b be the values taken on the finite p-group J by the parameters described in 2.1. Since $a > b \geq 0$, weight subgroups $\gamma_v^{a,b,e}(H)$ as described in 1.1 are defined. For arbitrary positive integer l, define

$$\gamma(l) = \gamma_l^{a,b,1}(H) \cap \gamma_l^{a,b,p}(H) \; .$$

Note that

$$\gamma(a) = H \; ,$$

$$[\gamma(l), H] \subseteq \left[\gamma_l^{a,b,1}(H), H\right] \cap \left[\gamma_l^{a,b,p}(H), H\right]$$

$$\subseteq \gamma_{l+a}^{a,b,1}(H) \cap \gamma_{l+a}^{a,b,p}(H)$$

$$= \gamma(l+a) \; ,$$

and

$$\left(\gamma(l)\right)^p \subseteq \gamma_{l+b}^{a,b,1}(H) \cap \gamma_{pl}^{a,b,p}(H)$$

$$\subseteq \gamma(l+b) \; ,$$

since $b < a$ and it may be assumed that $a \leq l$.

The factor $\gamma(l)/\gamma(l+a)$ is central in $H/\gamma(l+a)$, and the integer group ring ZJ acts naturally on this factor. Thus if $\rho \in \gamma(l)$ and $\varphi \in ZJ$, the coset $\rho^\varphi \gamma(l+a)$ of $\gamma(l+a)$ in H is well-defined, though in general the element ρ^φ is not.

In the next lemma, an expression $[C, \alpha]$ where C is a coset and α an element of a group, is to be interpreted simply as a set $\{[\varphi, \alpha] : \varphi \in C\}$.

4.2   LEMMA

With the notation described in 4.1, let l be an arbitrary positive integer. If, for $1 \leq i \leq l$, $\alpha_i = \psi_i \eta_i$ is an arbitrary element of G with $\psi_i \in J$ and $\eta_i \in H$, then

$$[\alpha_1, \ldots, \alpha_l] \in [\psi_1, \ldots, \psi_l] \prod \left\{\rho_g^{\chi_g} : g \in \Gamma_l\right\} \gamma(l+a) \; ,$$

where Γ_l *is a finite ordered index set, each* χ_g *is monomial in the augmentation ideal* I *of* $\mathbb{Z}J$ *, with* $0 \le w(\chi_g) \le a - 1$ *, and there exists an integer* $m(g)$ *such that* $\rho_g \in \gamma(m(g))$ *and* $m(g) + w(\chi_g) \ge l + a - 1$ *.*

Proof. The lemma is clearly true when $l = 1$, since $\eta_1 \in \gamma(a)$. Suppose $l > 1$, and the result for $l - 1$ established. Then

$$[\alpha_1, \ldots, \alpha_{l-1}, \alpha_l] \in \left[[\psi_1, \ldots, \psi_{l-1}] \prod \left\{\rho_g^{\chi_g} : g \in \Gamma_{l-1}\right\}\gamma(l+a-1), \psi_l\eta_l\right]$$

which, by repeated application of commutator identities (for example, [6], p. 253, Hilfssatz 1.2) is contained in

$$[\psi_1, \ldots, \psi_{l-1}, \eta_l][\psi_1, \ldots, \psi_{l-1}, \psi_l][\psi_1, \ldots, \psi_{l-1}, \psi_l, \eta_l]$$

$$\prod \left\{\left[\rho_g^{\chi_g}, \psi_l\right] : g \in \Gamma_{l-1}\right\} \prod \{\rho_d : d \in \Delta_l\}\gamma(l+a) .$$

Note that $\rho_g \in \gamma(l+1)$ for each g in Γ_{l-1} ; and that every element of $\gamma(l+a-1)$ is automatically in a coset of $\gamma(l+a)$ with the required form, with the empty monomial acting on it. In the last product above, the second factor $[\psi_1, \ldots, \psi_l]$ is one specifically required. The first factor is trivial if $l-1 > c$; otherwise $l \le c+1 < a$ and the factor is the inverse of $\eta_l^{(-1+[\psi_1, \ldots, \psi_{l-1}])}$, which is shown by Lemma 3.3 to be, modulo $\gamma(l+a-1)$, a product of terms of the form η_l^χ where $\eta_l \in \gamma(a)$ and $l-1 \le w(\chi) \le a-1$, which satisfies the required conditions. The third factor is treated similarly. Each factor in the product indexed by Δ_l is

a commutator with at least one entry from the set $\left\{\rho_g^{\chi_g} : g \in \Gamma_{k-1}\right\}$ and at least one equal to η_l , and thus is contained in $\gamma(l+a-1)$. Finally, for g in Γ_{l-1} , Lemma 3.3 and the distributive law show that $\chi_g(-1+\psi_l)$ is a sum of monomials in I , each of weight at least $w(\chi_g) + 1$. Modulo terms

already discussed, $\left[\rho_g^{\chi_g}, \psi_l\right]$ is expressed as a product of terms ρ_g^χ which are of the required form provided that the weight of the monomial χ is less than a .

If ρ_g^χ is a term in this product such that $w(\chi) \geq a$, then by Lemma 3.8,

$$\chi = p \sum \{\chi_d : d \in \Theta\} ,$$

where each χ_d is a monomial such that

$$w(\chi_d) \geq w(\chi) - b \geq a - b .$$

Since $\rho_g^p \in \gamma(l-1+b)$, this again gives an expression of the required form provided $w(\chi_d) < a$. If, for some d in Θ , $w(\chi_d) \geq a$, then application of Lemma 3.8 is repeated as often as necessary. The process must terminate after at most r applications of the lemma where r is the least integer such that $rb \geq a$, since then

$$\rho_g^{p^r} \in \gamma(l+a-1) .$$

The truth of the lemma follows by induction.   □

4.3 COROLLARY

With the notation of 4.1, *suppose that* c *is the nilpotency class of* G/H , *and that* $l > c$. *Then every commutator in* G *with weight at least* l *is contained in* $\gamma(l)$.

Proof. Every commutator in G with weight at least l is a product of left-normed commutators in G with weight at least l . By Lemma 4.2, each of these may be expressed as the product of a commutator in J (which is trivial for $l > c$) with elements of $\gamma(l)$.   □

One further preliminary is needed before the main result.

4.4 LEMMA (Frobenius, Kaloujnine and Krasner).

Let M *be an arbitrary group with a normal subgroup* N . *Then* N Wr M/N *has a subgroup isomorphic with* M .   □

Here N Wr M/N is the unrestricted standard wreath product of the two groups, as defined by Huppert [6], Kapitel I, 15.6 (p. 97) and by Neumann [14] at the beginning of Section 2.2 (p. 45). The result stated above is Theorem 22.21 (pp. 46-47) in the latter reference; a simple proof and

further references are given there.

An upper bound for the nilpotency class and cpp-class of an extension of a cpp-nilpotent group by a finite p -group may now be stated.

4.5   LEMMA

If G is a group with a normal subgroup H such that for some p , the index of H is a power of p and H is cpp-nilpotent, then G is nilpotent (and hence cpp-nilpotent). If a and b are the values for G/H of the invariants defined in 2.1, then the nilpotency class of G is bounded above by the $(a, b, 1)$ -class of H , and the cpp-class of G is bounded above by the (a, b, p) -class of H .

Proof. Let K be the base group of the wreath product $W = H \operatorname{wr} G/H$. Then K is a direct power of H , and for e in $\{1, p\}$, has the same (a, b, e) -class as H ; and $W/K \cong G/H$. Further, since W splits over K , Lemma 4.3 shows that if c is the nilpotency class of G/H and $l > c$, then

$$\gamma_l(W) = \gamma_l^{1,0,1}(W) \subseteq \gamma(l) \subseteq \gamma_l^{a,b,1}(K) ,$$

and the p^r th power of a commutator of weight l in K is contained in $(\gamma(l))^{p^r} \subseteq \gamma_{lp^r}^{a,b,p}(K)$, whence, by Corollary 1.3 with $v = lp^r$,

$$\pi_v(W) = \gamma_v^{1,0,p}(W) \subseteq \gamma_v^{a,b,p}(K) .$$

Thus the nilpotency class and cpp-class of W are bounded above by the $(a, b, 1)$ -class and (a, b, p) -class respectively of K , and hence of H . By Lemma 4.4, G is isomorphic with a subgroup of W , so the same upper bounds apply to the nilpotency class and cpp-class of G . $\square$

Lemma 1.2 may be used to re-state this result in terms that avoid reference to (a, b, e) -classes:

4.6   THEOREM

Let G be a group with a normal subgroup H whose index is a power of p , such that H is nilpotent of class r and for $1 \leq w \leq r$, every

commutator of weight w in H has order dividing $p^{s(w)}$. Let a and
b be the values for the finite p-group G/H of the invariants defined in
2.1. Then G is nilpotent, with class bounded above by

$$\max\{aw+b(s(w)-1) : 1 \le w \le r\} ,$$

and is cpp-nilpotent, with cpp-class bounded above by

$$\max\{awp^{s(w)} : 1 \le w \le r\} = at ,$$

where t is the cpp-class of H.   □

The simplicity of the expression comparing cpp-classes of H and G, as well as the fact that the cpp-series of the "top group" was involved in all the calculations, make it appear that the cpp-series is a more useful tool than the lower central series in the present context.

5.   The classes of a wreath product

In Lemma 5.4, lower bounds on the nilpotency class and cpp-class of a wreath product are obtained. Since they are equal to the corresponding upper bounds given by Theorem 4.6, they show that the result is best possible, and give (Corollary 5.5) the exact nilpotency class and cpp-class of a wreath product.

5.1 COEFFICIENTS

Let h be a positive integer, $q = p^h$ (where of course p is the same prime already being considered), and $q^* = p^{h-1}$. Let C be the cyclic group of order q generated by τ, and $\mathbb{Z}C$ the integer group ring of C.

Define $R(q, x, k)$ to be the coefficient of τ^k in the standard expression for $(-1+\tau)^x$ in $\mathbb{Z}C$; that is,

$$(-1+\tau)^x = \sum \{R(q, x, k)\tau^k : k \in \underline{q}\} .$$

This coefficient is, apart from sign, the same as the integer $\lambda_{x,k}$ defined by Liebeck in [9], 4.1 and 4.2; note that the choice of sign is not consistently maintained between 4.1 and 4.2. Liebeck's Theorem 4.3 is still valid, and is quoted now in the notation of the present paper.

5.2   LEMMA   (Liebeck, [9], Theorem 4.3).

Let   s   be a positive integer.

(a)   If $x \geq q + (s-1)(q-q^*)$, then

$$p^s \mid R(q, x, k) \quad \text{for all   } k \text{   in   } \underline{q} \; .$$

(b)   If $x = q + s(q-q^*) - 1$, then

$$p^{s+1} \nmid R(q, x, k) \quad \text{for all   } k \text{   in   } \underline{q} \; . \qquad \square$$

5.3   LEMMA

Let $W = H \text{ wr } J$ be the wreath product of two groups, and let $\rho \in H(1)$, the first coordinate subgroup in the base group K of W .
Then for arbitrary χ in ZJ , the element ρ^χ in K is well-defined.

Proof.   Since ρ is contained in one coordinate subgroup of K , its conjugates by distinct elements of J are in distinct coordinate subgroups, and commute. $\square$

This contrasts with the general situation where, if
$\rho \in \gamma_l^{a,b,1}(K) \cap \gamma_m^{a,b,p}(K)$, then the expression ρ^χ can be given a well-defined meaning only as a coset of $\gamma_{l+a}^{a,b,1}(K) \cap \gamma_{m+a}^{a,b,p}(K)$ in K or W , not as an element of the group.

5.4   THEOREM

Let J be a group with order a power of a prime p , on which the invariants defined in 2.1 *take values a and b . Let H be a cpp-nilpotent group, with $(a, b, 1)$-class l and (a, b, p)-class m . Then in the wreath product $H \text{ Wr } J$ there exist*

(a)   a non-trivial commutator of weight l , and

(b)   a non-trivial element of the form λ^{p^r} where λ is a commutator of weight m' , and $m'p^r = m$.

Proof.   The construction used here is an adaptation of that used by Scruton [16], Theorem 3.5.

(a)   By hypothesis, there exists in H a non-trivial element of the

form κ^{p^s} , where $\kappa = \begin{bmatrix} \alpha_1, & \ldots, & \alpha_w \end{bmatrix}$ is a left-normed commutator of weight w in H , and where

$$aw + bs = l .$$

Use the same symbols κ and α_i , $1 \leq i \leq w$, to denote the corresponding elements in the first coordinate subgroup $H(1)$ of the base group K of $W = H \text{ Wr } J$.

Let $T = \left\{ \left(\tau_i, h(i) \right) : i \in M \right\}$ be an ordered, π-form-respecting basis for J , and adopt the associated notation from Section 2. Let z be the last element of the ordered set M , and M^* the sub-ordered-set of M with this element removed. Let ω and ω^* be the elements of the integer group ring $\mathbb{Z}J$ given by

$$\omega = \prod \left\{ (\tau_i-1)^{q(i)-1} : i \in M \right\}$$

and

$$\omega^* = \prod \left\{ (\tau_i-1)^{q(i)-1} : i \in M^* \right\} .$$

Note that if $\rho \in H(1)$, then ρ^ω and ρ^{ω^*} are elements of K whose components in the first coordinate subgroup are either ρ or ρ^{-1} .

The commutator in W ,

$$\begin{bmatrix} \alpha_1, & \left(q(1)-1\right)\tau_1, & \ldots, & \left(q(z)-1\right)\tau_z \end{bmatrix} = \begin{bmatrix} \alpha_1, & \chi \end{bmatrix} \quad \text{say,}$$

has weight precisely a , and is equal to α_1^ω . Hence

$$\begin{bmatrix} \alpha_1, & \chi, & \alpha_2 \end{bmatrix} = \begin{bmatrix} \alpha_1^\omega, & \alpha_2 \end{bmatrix}$$

has component $\begin{bmatrix} \alpha_1^t, & \alpha_2 \end{bmatrix}$, where $t \in \{+1, -1\}$, in the first coordinate subgroup of K , and trivial component in each other subgroup. This process is repeated to show that the commutator

$$\begin{bmatrix} \alpha_1, & \chi, & \alpha_2, & \ldots, & \chi, & \ldots, & \alpha_w \end{bmatrix} \quad \text{has} \quad \begin{bmatrix} \ldots & \begin{bmatrix} \alpha_1^t, & \alpha_2 \end{bmatrix}^t, & \ldots, & \alpha_w \end{bmatrix} = \beta$$

as its component in the first coordinate subgroup, and trivial component in each other coordinate subgroup. If χ^* represents the sequence of commutator entries

$$\bigl(q(1)-1\bigr)\tau_1, \ \bigl(q(2)-1\bigr)\tau_2, \ \ldots, \ \bigl(q(z-1)-1\bigr)\tau_{z-1} \ ,$$

then

$$[\alpha_1, \ \chi, \ \alpha_2, \ \ldots, \ \alpha_w, \ \chi^*] = \beta^{\omega^*} \ .$$

Let $r = q(z) + s\bigl(q(z)-q^*(z)\bigr) - 1$, and recall that the ordering of M has been chosen so that $u(z)q^*(z) = d$ and so $\tau_z^{q(z)} = 1$. Now

$$\lambda = \bigl[\alpha_1, \ \chi, \ \alpha_2, \ \ldots, \ \alpha_w, \ \chi^*, \ r\tau_z\bigr]$$

$$= \beta^{\omega^* \bigl(\tau_z-1\bigr)^n}$$

$$= \beta^{\omega^* \Sigma \{R(q(z)),r,k)\tau_z^k : k \ \in \ \underline{q(z)}\}} \ .$$

Now the $(a, b, 1)$-weight of β^{p^s} in H is maximal, so for some t' in $\{-1, 1\}$, $\beta^{p^s} = \kappa^{t'p^s}$. Lemma 5.2 shows that for all k in $\underline{q(z)}$,

$$p^s \mid R\bigl(q(z), r, k)\bigr) \ \text{and} \ p^{s+1} \nmid R\bigl(q(z), r, k\bigr) \ ;$$

and the coefficient of 1 in the element

$$w^* \sum \left\{ R\bigl(q(z), \ r, \ k\bigr)\tau_z^k \ : \ k \in \underline{q(z)} \right\}$$

is $\pm R\bigl(q(z), r, 0\bigr)$; so the component of λ in $H(1)$ is $\kappa^{\pm R\bigl(q(z),r,0\bigr)}$, which is non-trivial. Thus the element λ is itself non-trivial, but λ is a commutator of weight

$$aw + su(z)\bigl(q(z)-q^*(z)\bigr) = aw + bs = l$$

in W.

(b) Similarly, from the hypothesis, there exists in H a non-trivial element of the form κ^{p^s} where $\kappa = \bigl[\alpha_1, \ \ldots, \ \alpha_w\bigr]$ is a left-normed commutator of weight w in H and $awp^s = m$. As in the proof of part

(a), the commutator

$$\lambda = [\alpha_1, \chi, \alpha_2, \chi, \ldots, \alpha_w, \chi]$$

of weight aw in W has as its component in the first coordinate subgroup of κ,

$$\left[\ldots \left[\alpha_1^t, \alpha_2\right]^t, \ldots, \alpha_w\right]^t .$$

Hence λ^{p^s} , which has cpp-weight $awp^s = m$ in W , has

$$\left[\ldots \left[\alpha_1^t, \alpha_2\right]^t, \ldots, \alpha_w\right]^{tp^s} = [\alpha_1, \alpha_2, \ldots, \alpha_w]^{t'p^s} ,$$

which is non-trivial, as its component in the first coordinate subgroup of κ , and so is itself non-trivial, as required.   □

5.5 COROLLARY

  Let J be a group whose order is a power of a prime p , with invariants as described in 2.1 *taking values a and b ; and let H be a nilpotent p-group of class r , such that for $1 \le w \le r$ the maximum order of a commutator of weight w is $p^{s(w)}$. Then H wr J is nilpotent, with class precisely $\max\{aw + b(s(w)-1) : 1 \le w \le r\}$. The cpp-class of H wr J is precisely $\max\{awp^{s(w)} : 1 \le w \le r\}$, which is a times the cpp-class of H .*   □

6. An application

  The results of this paper make a small contribution to understanding the restricted Burnside problem by showing (Corollary 6.3) the existence of two-generator groups of exponents 8, 9 , and 25 with nilpotency classes 39, 18 , and 11244 respectively. If there exists a largest finite two-generator group with one of these exponents, its nilpotency class is bounded below by that of the corresponding group described here. There is no reason to suppose that these bounds are "good" - in fact there is considerable reason to suspect the contrary - but they appear to be the best available at present.

  The first sub-section simply applies Corollary 5.5 to some examples.

Lemma 6.2 shows the existence of appropriate two-generator subgroups of these wreath products.

Notation for varieties and product varieties is taken from Hanna Neumann's book [14]. In particular, $\underline{\underline{B}}_n$ and $\underline{\underline{A}}_n$ denote the varieties of all groups and all abelian groups of exponent dividing n; and when p is a prime, $\underline{\underline{K}}_p$ denotes the Kostrikin variety of all locally finite groups of exponent p.

6.1 EXAMPLES OF NILPOTENT WREATH PRODUCTS

(a) Let $B(2, 4)$ be the free group on two generators with exponent 4. This group has order 2^{12}; relevant details about it are easily deduced from the presentation for $B(3, 4)$ given by Bayes, Kautsky, and Wamsley [2]. If it has generators α and β, then a standard basis is given by:

$$\tau_1 = \alpha \qquad\qquad h(1) = 2 ,$$
$$\tau_2 = \beta \qquad\qquad h(2) = 2 ,$$
$$\tau_3 = [\beta, \alpha] \qquad\qquad h(3) = 1 ,$$
$$\tau_4 = [\beta, \alpha, \alpha, \alpha] \qquad h(4) = 1 ,$$
$$\tau_5 = [\beta, \alpha, \alpha, \beta] \qquad h(5) = 1 ,$$
$$\tau_6 = [\beta, \alpha, \beta, \beta] \qquad h(6) = 1 ,$$
$$\tau_7 = [\beta, \alpha, \alpha] \qquad\quad h(7) = 2 ,$$
$$\tau_8 = [\beta, \alpha, \beta] \qquad\quad h(8) = 2 .$$

From this it can be seen that

$$n(1) = 12 , \quad n(2) = 10 , \quad n(3) = 7 ,$$
$$n(4) = 5 \quad , \quad n(5) = 2 \quad , \quad n(6) = 2 ;$$

whence

$$a = 1 + (12+10+7+5+2+2) = 39$$

and

$$b = 6 .$$

Consider two wreath products,

$$W_1 = \left(C_2 \times C_2\right) \text{ wr } B(2, 4) \quad \text{and} \quad W_2 = B(2, 4) \text{ wr } B(2, 4) \ .$$

The nilpotency class of the former is equal to the $(39, 6, 1)$-class of $C_2 \times C_2$, which is 39 ; that of the latter is equal to the $(39, 6, 1)$-class of $B(2, 4)$, which is 195 since $B(2, 4)$ has a non-trivial commutator of weight 5 .

(b) Let $B(2, 3)$ be the free group on two generators with exponent 3 . This group has order 3^3 , and a standard basis given by

$$\tau_1 = \alpha \ , \quad \tau_2 = \beta \ , \quad \tau_3 = [\beta, \alpha] \ , \quad h_1 = h_2 = h_3 = 1 \ .$$

Clearly, $m(1) = 3$, $m(2) = 1$,

$$a = 1 + (p{-}1)(3{+}1) = 9 \ ,$$

and

$$b = (p{-}1)2 = 4 \ .$$

The nilpotency class of $B(2, 3) \text{ wr } B(2, 3)$ is equal to the $(9, 4, 1)$-class of $B(2, 3)$, which is 18 .

$\Big($The free group $F_2\left(\underline{\underline{B}}_3\underline{\underline{B}}_3\right)$ in the product variety $\underline{\underline{B}}_3\underline{\underline{B}}_3$ has a normal subgroup of exponent 3 and nilpotency class 3 , and the quotient to this normal subgroup is isomorphic with $B(2, 3)$. Theorem 4.6 gives an upper bound of 27 for the nilpotency class of $F_2\left(\underline{\underline{B}}_3\underline{\underline{B}}_3\right)$.$\Big)$

(c) Let $K(2, 5)$ be the largest finite group of exponent 5 on two generators (shown to exist by Kostrikin, [8]). From the presentation for this group given by Havas, Wall, and Wamsley [5], it can be calculated that

$$\begin{aligned}
n(1) &= 34 \ , & n(2) &= 32 \ , & n(3) &= 31 \ , \\
n(4) &= 29 \ , & n(5) &= 26 \ , & n(6) &= 24 \ , \\
n(7) &= 20 \ , & n(8) &= 16 \ , & n(9) &= 12 \ , \\
n(10) &= 6 \ \ , & n(11) &= 3 \ \ , & n(12) &= 1 \ \ .
\end{aligned}$$

Hence

$$a = 1 + 4 \times 234 = 937 \ ,$$

and

$$b = 4 \times 12 = 48 \ .$$

The nilpotency class of $K(2, 5) \text{ wr } K(2, 5)$ is equal to the

$(937, 48, 1)$-class of $K(2, 5)$, namely $12 \times 937 = 11244$.

6.2 LEMMA

Let p be a prime, m a positive integer, and J a finite two-
generator group of exponent p^m with a standard basis
$T = \{(\tau_i, h(i)) : i \in M\}$ such that, where ρ and σ generate J ,

$$\tau_1 = \rho , \quad \tau_2 = \sigma ,$$

and for each i in M , τ_i is a commutator with $u(i)$ entries from the
set $\{\rho, \sigma\}$. Let H be a nilpotent two-generator group of exponent p .
Then the standard wreath product $W = H \operatorname{wr} J$ has a two-generator subgroup
whose nilpotency class is the same as that of W .

Proof. Let H be generated by α and β , and have nilpotency class
r . Let a and b be the parameters for J defined in 2.1. The
nilpotency class and cpp-class of W are both equal to ar ; and from the
proof of Theorem 5.4, with the sequence of commutator entries χ defined
as it was there, it can be seen that there exists a non-trivial commutator

$$\begin{aligned}
\nu &= \left[\beta, \; \left(p^{h(1)}-1\right)\tau_1, \; \left(p^{h(2)}-1\right)\tau_2, \; \ldots, \; \left(p^{h(z)}-1\right)\tau_z, \; \boldsymbol{\alpha}, \; \ldots\right] \\
&= [\beta, \chi, \alpha, \chi, \ldots, \chi]
\end{aligned}$$

of weight ar in W . The goal of this proof is the construction of a
non-trivial commutator of the same weight ar in a two-generator subgroup
of W .

Let X be the subgroup of W generated by the elements $\rho\alpha$ and
$\sigma\beta$. Let μ be the element of X obtained by substituting for each entry
of ν equal to either α or ρ the entry $\rho\alpha$ and for each entry of ν
equal to either β or $\dot{\sigma}$ the entry $\sigma\beta$. For example, if $\tau_3 = [\sigma, \rho]$,
then

$$\mu = \left[\sigma\beta, \; \left(p^{h(1)}-1\right)\rho\alpha, \; \left(p^{h(2)}-1\right)\sigma\beta, \; \left(p^{h(3)}-1\right)[\sigma\beta, \rho\alpha], \; \ldots, \; \rho\alpha, \; \ldots\right] .$$

Since ν has maximal c-weight and cpp-weight in W ,

$$\mu = \textstyle\prod \{\mu_g : g \in \Gamma\} ,$$

where $|\Gamma| = 2^{ar}$ and each μ_g is a commutator with the same bracketing

arrangement as ν and μ , and precisely ar entries: either α or ρ in each position where ν has either α or ρ , and either β or σ in each position where ν has either β or σ . One such commutator μ_g is equal to ν , and so is non-trivial; it will be shown that all the others are trivial.

If a commutator μ_g has among the entries in its first segment of weight a (corresponding to the first $[\beta, \chi]$ in ν) two entries from the set $\{\alpha, \beta\}$, then this segment is contained in $\gamma(2a)$ in the notation defined in 4.1. Hence, by a similar procedure to that in the proof of Lemma 4.2 and Corollary 4.3,

$$\mu_g \in \gamma(ar+1) = \{1\} \ .$$

A similar argument shows that if, for some integer w such that $1 \le w \le r$, the initial segment by μ_g with weight aw contains $w + 1$ entries from $\{\alpha, \beta\}$, then $\mu_g = 1$.

On the other hand, if μ_g has an initial segment of weight greater than c with no entry from the set $\{\alpha, \beta\}$, it is clearly again equal to the identity.

Hence the initial segment of weight a in each non-trivial commutator μ_g must contain one and only one entry from the set $\{\alpha, \beta\}$. Let η be the entry in the left-normed bracketting of μ_g (corresponding to a τ_i entry of ν) which has, as an entry of its own, α or β . If η is not the first entry in μ_g , then

$$\mu_g = [\sigma, \theta_1, \ldots, \theta_{l-1}, \eta, \theta_{l+1}, \ldots]$$
$$= [\eta, [\sigma, \theta_1, \ldots, \theta_{l-1}], \theta_{l+1}, \ldots]^{-1} \ .$$

If $l = 2$, this is

$$\mu_g = [\eta, \sigma, (q(1)-2)\rho, (q(2)-1)\sigma, \ldots]^{-1} \ ,$$

which has $q(2) = p^{h(2)}$ entries equal to σ and, for i in $M\backslash\{1, 2\}$, has $q(i) - 1$ entries equal to τ_i in its initial segment of weight a . Lemma 5.3 shows that this commutator may be interpreted directly in terms

of the corresponding element of ZJ , and by repeated application of Lemma 3.7 this is seen to have a factor of p ; hence μ_g is trivial. If $l > 2$, then Lemma 3.3 must first be applied to the element $[\sigma, \theta_1, \ldots, \theta_{l-1}] - 1$ of ZJ , and then Lemma 3.7 is used to give the same result as before.

Hence, if μ_g is non-trivial, then its first entry must be β , and this must be followed by the sequence χ of entries. However, by Lemmas 5.3 and 3.8, μ_g cannot have a sequence of consecutive entries all belonging to J with total weight a . Thus the first entry in each of the r segments of weight a must be from the set $\{\alpha, \beta\}$, and every other entry must be from $\{\rho, \sigma\}$; that is, $\mu_g = \nu$. $\square$

6.3 COROLLARY

There exist in the product varieties $\underline{\underline{B}}_3\underline{\underline{B}}_3$, $\underline{\underline{A}}_2\underline{\underline{B}}_4$, *and* $\underline{\underline{K}}_5\underline{\underline{K}}_5$ *two-generator groups of nilpotency classes* 18, 39 , *and* 11244 *respectively.*

Proof. This is immediate from the examples in 6.1 and Lemma 6.2. $\square$

The significance of this Corollary has been discussed in the introduction to Section **6**.

References

[1]   Gilbert Baumslag, "Wreath products and p-groups", *Proc. Cambridge Philos. Soc.* **55** (1959), 224-231.

[2]   A.J. Bayes, J. Kautsky and J.W. Wamsley, "Computation in nilpotent groups (application)", *Proc. Second Internat. Conf. Theory of Groups*, Canberra 1973, 82-89 (Lecture Notes in Mathematics, **372**. Springer-Verlag, Berlin, Heidelberg, New York, 1974).

[3]   Joseph T. Buckley, "Polynomial functions and wreath products", *Illinois J. Math.* **14** (1970), 274-282.

[4]   P. Hall, "A contribution to the theory of groups of prime-power order", *Proc. London Math. Soc.* (2) **36** (1934), 29-95.

[5]   George Havas, G.E. Wall, and J.W. Wamsley, "The two generator
        restricted Burnside group of exponent five", *Bull. Austral.
        Math. Soc.* 10 (1974), 459-470.

[6]   B. Huppert, *Endliche Gruppen I* (Die Grundlehren der mathematischen
        Wissenschaften, 134. Springer-Verlag, Berlin, Heidelberg, New
        York, 1967).

[7]   S.A. Jennings, "The structure of the group ring of a p-group over a
        modular field", *Trans. Amer. Math. Soc.* 50 (1941), 175-185.

[8]   А.И. Костринин [A.I. Kostrikin], "О проблеме Бернсайда" [The Burnside
        problem], *Izv. Akad. Nauk SSSR Ser. Mat.* 23 (1959), 3-34; *Amer.
        Math. Soc. Transl.* (2) 36 (1964), 63-99.

[9]   Hans Liebeck, "Concerning nilpotent wreath products", *Proc. Cambridge
        Philos. Soc.* 58 (1962), 443-451.

[10]   J.D.P. Meldrum, "On nilpotent wreath products", *Proc. Cambridge
        Philos. Soc.* 68 (1970), 1-15.

[11]   J.D.P. Meldrum, "Correction to a paper on wreath products", *Proc.
        Cambridge Philos. Soc.* 76 (1974), 21.

[12]   Larry Morley, "Bounds on the nilpotency class of certain semidirect
        products", *Trans. Amer. Math. Soc.* 159 (1971), 381-390.

[13]   Larry J. Morley, "A commutator relation in a wreath product of
        p-groups", preliminary report, *Notices Amer. Math. Soc.* 22
        (1975), A-675, abstract no. 728-A31.

[14]   Hanna Neumann, *Varieties of groups* (Ergebnisse der Mathematik und
        ihrer Grenzgebiete, 37. Springer-Verlag, Berlin, Heidelberg,
        New York, 1967).

[15]   Robert Sandling, "Modular augmentation ideals", *Proc. Cambridge
        Philos. Soc.* 71 (1972), 25-32.

[16]   Teresa Scruton, "Bounds for the class of nilpotent wreath products",
        Proc. Cambridge Philos. Soc. 62 (1966), 165-169.

[17]   David Shield, "Power and commutator structure of groups", *Bull.
        Austral. Math. Soc.* 17 (1977), 1-52.

[*18*] L. Sylow, "Théorèmes sur les groupes de substitutions", *Math. Ann.*
         5 (1872), 584-594.

Goroka Teachers College,

Goroka,

Papua New Guinea.