Proc. Camb. Phil. Soc. (1972), **71**, 25
PCPS 71–4
Printed in Great Britain

Modular augmentation ideals

By ROBERT SANDLING
The University, Manchester

(*Received* 13 *August* 1970)

An ideal of an integral group ring is divisible by a given integer if all of its elements share this common factor; the ideals most often encountered are rarely divisible in this sense. Only in the case of finite p-groups are powers of the augmentation ideal of the integral group ring ever divisible. For every e, there is some n for which the nth power of the augmentation ideal is divisible by p^e. The smallest such integer n arises in many contexts; this paper describes its properties and interpretations.

We advance a conjecture about the augmentation ideal of p-groups and introduce a technique for dealing with the group rings of cyclic p-groups. The conjecture asserts that the sequence of powers of p dividing the powers of the augmentation ideal increases by at most one step at a time. It is a conjecture that appears under many guises; seven equivalent versions are given. It is true for Abelian groups and can be established, arduously, for the unlikely class of p-groups whose commutator quotients have smallest invariant of order p. The first section concludes with calculations and estimates of the nilpotence class of the augmentation ideal in modular group rings.

For group rings of cyclic p-groups, non-standard generators for the powers of the augmentation ideal prove efficient in establishing known results about these group rings, such as Liebeck's computation of the nilpotence class of wreath products of Abelian p-groups and theorems of Bachmuth and others, and in finding new Engel-like commutator identities for their modules. The second section ends with a complete determination of the extent to which the familiar identity, $pI = I^p$, for the augmentation ideal of the cyclic group of order p, generalizes to cyclic groups of higher order.

1. *Arbitrary p-groups.* The content of a subset of RG is the ideal of R generated by all coefficients of all elements in the subset. Content is independent of the basis chosen for RG; furthermore, the content of an ideal J of RG is the smallest ideal of R which divides J. We shall examine the content of the powers of the augmentation ideal $I(\mathbf{Z}, G)$.

It is a consequence of the following lemma that $I^n(\mathbf{Z}, G)$ has non-trivial content only when G is finite p-group; in this case the content is $p^e\mathbf{Z}$ for some e.

Lemma 1·1. *The augmentation ideal of RG is nilpotent if and only if G is a finite p-group and R has characteristic a power of p.*

Proof. If $I = I(R, G)$ is nilpotent, I has non-trivial annihilator so that G must be finite. We may assume that $R = \mathbf{Z}_r$, where r is the characteristic of the ring R. It

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

suffices to show that, if p divides the order of G, then r is a power of p. For this, we may assume that G is a p-group.

If $r = 0$, I/I^2 is isomorphic to G/G' so that, for all n, there is an e for which p^eI is in I^n but p^eI is non zero a contradiction. If a prime q, not equal to p, divides r, we may assume that $r = q$; but then I/I^2 is isomorphic to $G/G'G^q = 1$ so that $I = I^2 = \ldots = 0$, also a contradiction.

The sufficiency of the second condition follows from the fact that : If P is a finite p-group, the intersection of all I^n, $n \geqslant 0$, equals the intersection of all p^eI, $e \geqslant 0$, where $I = I(\mathbf{Z}, P)$.

Proof. There is a familiar isomorphism of I/I^2 with P/P' a group of exponent a power of p. Hence, given n, there is some e for which p^eI is contained in I^n.

To show that, given e, there is some n for which I^n is contained in p^eI, it suffices to assume $e = 1$. We induct on the order of P. For P cyclic of order p, generated by x, $I^n(P)$ is generated as right ideal by $(x-1)^n$ so we may taken $n = p$. In the general case, take N a non-trivial normal subgroup of P; by induction and the isomorphism of $\mathbf{Z}P/N$ with $\mathbf{Z}P/I(N)\mathbf{Z}P$, there is an n for which $I^n(P)$ is in $pI(P) + I(N)\mathbf{Z}P$; again induction gives an m for which $I^m(N)$ is in $pI(N)$ so that $I^{nm}(P)$ is in $pI(P)$.

If J is a nilpotent ideal, the class of J is $n-1$ where n is minimal such that $J^n = 0$. Define $\nu(e, G)$ for a finite p-group G by the condition that the class of $I(\mathbf{Z}_{p^e}, G)$ is $\nu(e, G) - 1$. Thus $\nu(e, G)$ is the smallest integer n for which $I^n(\mathbf{Z}, G)$ is in $p^e\mathbf{Z}G$. For $e \leqslant 0$, let $\nu(e, G) = 0$.

If A is cyclic of order p^e, the wreath product W of A by G may be realized as the group ring $\mathbf{Z}_{p^e}G$ extended by G in its right regular representation. Making this identification, we see that $W_n = G_n I^{n-1}$, $I = I(\mathbf{Z}_{p^e}, G)$; W_n and G_n are the nth terms of the lower central series of W and G respectively. Thus

LEMMA 1·2. *If A is cyclic of order p^e, $e > 0$, and G is a finite p-group, $\nu(e, G)$ is the class of $A \sim G$.*

The remainder of this section will concern only finite p-groups. Unless stated otherwise, I and ν will denote $I(\mathbf{Z}_{p^e}, G)$ and $\nu(e, G)$.

If B is a proper subgroup of the cyclic group A, it seems reasonable that $B \sim G$ has class strictly less than that of $A \sim G$. Equivalently, by 1·2, $\nu(e-1, G) < \nu(e, G)$. This conjecture is true for Abelian groups, as will be seen in section 2; it can also be established for an unusual class of groups (see 1·10). We state next several equivalent forms of this conjecture.

THEOREM 1·3. *Let G be a non-trivial p-group, $e \geqslant 1$, $\nu = \nu(e, G)$ and $I = I(\mathbf{Z}_{p^e}, G)$. The following are equivalent:*

(1) $\nu > \nu(e-1, G)$.

(2) *If A is a cyclic group of order p^e and B its subgroup of order p^{e-1}, then $A \sim G$ has class strictly greater than the class of $B \sim G$.*

(3) *G^p is contained in $l_{\nu-2}(e, G)$.*

(4) *$I^{\nu-1}$ is the unique minimal ideal of $\mathbf{Z}_{p^e}G$.*

(5) *There is a normal subgroup N of order p for which $\nu > \nu(e, G/N)$.*

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

(6) *For all normal subgroups N of order p, $\nu > \nu(e, G/N)$.*

The quantified version: for all e, $\nu(e, G) > \nu(e-1, G)$; is equivalent to the assertion that, for all e, the class of $I(\mathbf{Z}_{p^e}, G)$ is equal to the class of the radical of $\mathbf{Z}_{p^e}G$.

That 1 and 2 are equivalent has already been remarked. We show the equivalence of 1 with each of the others in turn through a series of lemmas. 3 involves the subgroup $l_n(e, G)$ defined as the set of all x such that $I^i(x-1)I^j = 0$ for all i, j with $i+j = n$; these subgroups are studied in (9); they appear in the upper central series of the wreath product W.

LEMMA 1·4. *Let $m < p$ and $n = \nu - 1 - m$. Then $\nu \geqslant \nu(e-1, G) + m$ if and only if G^p is in $l_n(e, G)$.*

Proof. Let $I = I(\mathbf{Z}_{p^e}, G)$. If x is in G, modulo I^{m+1} there is a unit α for which $x^p - 1 \equiv p(x-1)\alpha$. Let $i+j = n$; then $I^i(x^p-1)I^j = pI^i(x-1)I^j$. The equivalence of the two statements is immediate.

This lemma suggests that $\nu(e, G) \geqslant \nu(e-1, G) + p - 1$ might be true; such is the case for G Abelian. The number $p-1$ is involved in another question concerning the powers of the augmentation ideal of p-groups: if G is any finite group, the Jordan–Zassenhaus theorem ((3), p. 563) implies that I^n, $I = I(\mathbf{Z}, G)$, is isomorphic to I^m as $\mathbf{Z}G$-modules for some $n < m$; but then I^{n+1} is isomorphic to I^{m+1}, and so forth. The smallest such $m-n$ is the period of I. For G cyclic, I has period 1 but, for G a non-cyclic p-group, it seems likely that $p-1$ divides the period and that considerations involving $\nu(e, G)$ are involved in the computation of the period.

LEMMA 1·5. *Let $f \leqslant e$. $\nu(e-f, G) < \nu = \nu(e, G)$ if and only if the exponent of $I^{\nu-1}$ divides p^f.*

Proof. $p^f I^{\nu-1}$ is 0 if and only if $I^{\nu-1}$ is in $p^{e-f}I$ if and only if $\nu(e-f, G) \leqslant \nu - 1$.

This has the immediate corollary, because G/G' is isomorphic to I/I^2, $I = I(G, \mathbf{Z})$, that $\nu(e-a, G) < \nu(e, G)$ where p^a is the exponent of G/G'.

The ideal $I^{\nu-1}$ is contained in the annihilator of I. Let η_S denote the sum in RG of all the elements of the subset S of G; η_G is called the norm element of RG; the annihilator of $I(R, G)$ is $R\eta_G$. Thus, $I^{\nu-1}$ is generated by $p^{e-f}\eta_G$, where p^f is the exponent of $I^{\nu-1}$. Since $p^{e-1}\eta_G$ generates the unique minimal ideal of $\mathbf{Z}_{p^e}G$, we have

LEMMA 1·6. *$\nu(e-1, G) < \nu$ if and only if $I^{\nu-1}$ is the unique minimal ideal of $\mathbf{Z}_{p^e}G$.*

LEMMA 1·7. *Let N be a normal subgroup of G of order p^i. $\nu(e-i, G) < \nu$ if and only if $\nu(e, G/N) < \nu$.*

Proof. It suffices to observe that, under the projection $\mathbf{Z}_{p^e}G$ to $\mathbf{Z}_{p^e}G/N$, η_G goes to $p^i\eta_{G/N}$.

The situation with respect to subgroups is much clearer.

LEMMA 1·8. *If H is a proper subgroup of G, $\nu(e, H) < \nu$.*

Proof. Suppose $\nu(e, H) = \nu$. Let T be a set of coset representatives for H in G, and let p^i be the index of H in G. Then $\eta_G = \eta_H\eta_T$ while $\eta_T = p^i + \alpha$, some α in I.

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

By assumption, $p^{e-1}\eta_H$ is in $I^{\nu-1}$. By hypothesis, $i \geqslant 1$ so $p^{e-1}\eta_G = p^{e-1}\eta_H \alpha$ which is in $I^\nu = 0$, which is a contradiction.

The radical of $\mathbf{Z}_{p^e}G$ is the ideal $I + p\mathbf{Z}_{p^e}G$; its annihilator is the ideal $p^{f-1}I^{\nu-1}$, f as above.

LEMMA 1·9. *The class of the radical of* $\mathbf{Z}_{p^e}G$ *equals the class of* I *for all* e *if and only if* $\nu(e-1, G) < \nu(e, G)$ *for all* e.

Proof. It suffices to observe that the nth power of the radical is the sum of the ideals $p^i I^{n-i}$.

This concludes the series of lemmas which comprise the proof of Theorem 1·3. We next state a result verifying the conjecture in a special case. The proof is more elaborate than the case warrants and is therefore omitted; it consists of 1·17, 1·19 and 1·20 of (8) (see (7)). These theorems give a systematic analysis of generators for the powers of the augmentation ideal and provide a powerful technique for the study of $\nu(e, G)$. Proposition 1·11 is also obtained from these methods.

We have seen that $\nu(e-a, G) < \nu$ if p^a is the exponent of G/G', that is, the largest invariant of the Abelian group G/G'.

THEOREM 1·10. *If* p^a *is the smallest invariant of the Abelian group* G/G', *then*

$$\nu(e-a, G) < \nu.$$

Jennings (5) (see 1·22 of (8)) gave an explicit expression for $\nu(1, G)$, namely

PROPOSITION 1·11. *Let* $G_{n,p} = G_n \Pi G_i^{p^j}$, *the product taken over all* i, j *such that* $ip^j \geqslant n$. $G_{n,p}/G_{n+1,p}$ *is Abelian; let* d_n *be its rank. Then* $\nu(1, G) - 1 = (p-1)\Sigma n d_n$.

For Abelian groups, $\nu(e, G)$ can be computed exactly but in general we can give only broad results and inequalities.

LEMMA 1·12. *Let* G *be the direct product of its subgroups* H_i. *Then* $\nu(e, G) - 1$ *is the maximal among all sums* $\Sigma(\nu(e_i, H_i) - 1)$, *where* $\Sigma(e_i - 1) = e - 1$.

Proof. Modulo p^{e_i}, $p^{e_i-1}\eta_{H_i}$ is in $I^{n_i}(\mathbf{Z}, H_i)$, where $n_i = \nu(e_i, H_i) - 1$; modulo p^e, their product $p^{e-1}\eta_G$ is in $I^n(\mathbf{Z}, G)$, $n = \Sigma(\nu(e_i, H_i) - 1)$. Thus, $\nu(e, G) - 1$ is greater than or equal to all such sums.

For the converse, assume that $\nu - 1$ is strictly greater than all such sums. $I^{\nu-1}$ is the sum of all products $\Pi I^{n_i}(H_i)\mathbf{Z}G$, where $\Sigma n_i = \nu - 1$. For $i > 1$, choose e_i via $\nu(e_i - 1, H_i) \leqslant n_i < \nu(e_i, H_i)$. Let $e_1 - 1 = e - 1 - \Sigma(e_i - 1)$, sum over $i > 1$. By assumption, $\Sigma n_i > \Sigma(\nu(e_i, H_i) - 1)$ so $n_1 \geqslant \nu(e_1, H_1)$. Thus, p^e divides $I^{\nu-1}$, a contradiction.

It is clear that $\nu(e, G) \leqslant e\nu(1, G)$. This gives a crude estimate for the magnitude of ν as $\nu(e, G) \leqslant e|G|$ since the proof of 1·1 implies that

$$\nu(1, G) \leqslant \nu(1, G/N)\,\nu(1, N) \leqslant |G:N|\,|N|$$

by induction. We give several other estimates here and more appear in (9).

PROPOSITION 1·13. *If* N *is a central subgroup of* G,

$$\nu(e, G) \leqslant \nu(1, G/N)\,\nu(e, N).$$

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

Proof. Let $\nu_1 = \nu(1, G/N)$, $\nu_2 = \nu(e, N)$, $J = I(N)\mathbf{Z}_{p^e}G$. Then I^{ν_1} is in $pI+J$ so $I^{\nu_1\nu_2}$ is in the sum of all ideals $p^iI^iJ^j$ where $i+j = \nu_2$. But, by the results of the following section, $\nu(e, N)-i \geqslant \nu(e-i, N)$ so that p^e divides $I^{\nu_1\nu_2}$.

The next upper bound is a consequence of a well-known lemma of Fitting ((4), p. 276), applied to the wreath product W via 1·2.

PROPOSITION 1·14. *Let G be the product of its normal subgroups H_i. Then*

$$\nu(e, G) \leqslant \Sigma\nu(e, H_i).$$

Our last result gives a lower bound for ν.

PROPOSITION 1·15. *Let H_1 and H_2 be subgroups of G whose intersection is trivial. Then $\nu(e, G)-1$ is greater than or equal to all sums $\Sigma(\nu(e_i, H_i)-1)$, where $\Sigma(e_i-1) = e-1$.*

Proof. With the observation that $\eta_{H_1}\eta_{H_2} = \eta_{H_1}\eta_{H_2}$, the proof of the first part of 1·12 applies.

2. *Cyclic p-groups.* In this section, we calculate $\nu(e, G)$ for G Abelian. This had already been done by Liebeck(6), who worked in the wreath product context where the problem becomes rather involved. By 1·12, it suffices to calculate $\nu(e, G)$ for G cyclic.

Let G be cyclic of order p^n and $\eta_i = \eta_i(n)$ be the norm element of the subgroup of order p^i. If x is a generator of G, $(x-1)^m$ is a generator for the ideal I^m, $I = I(\mathbf{Z}, G)$; for this problem, such a natural generator is unsuitable. Let $\alpha = \alpha(n)$ be the product of all $x-1$ over all generators x of G; then α is a generator of I^m, $m = p^n-p^{n-1}$, whose coefficients can be more readily determined.

LEMMA 2·1. *There are integers a_i for which $\alpha = \Sigma a_i\eta_i$. If $n > 0$,*

$$a_0 = p, \quad a_i = (p^{p^i}-p^{p^{i-1}})/p^i, \quad 0 < i < n, \quad \text{and} \quad a_n = -p^{p^{n-1}}/p^n.$$

Proof. There are integers b_y, all y in G, for which $\alpha = \Sigma b_y(y-1)$. The automorphism group of G fixes α and acts transitively on elements of a given order; thus, b_y is constant on a set of such elements. But $\eta_i-\eta_{i-1}$ is the sum of all elements of order p^i, $i > 0$, whence such a_i exist for $i > 0$; a_0 is determined by the fact that α has zero augmentation.

Induct on i that a_i has the value claimed; assume, therefore, that this is so for all $j < i$. Under the projection $\mathbf{Z}G$ to $\mathbf{Z}G/G^{p^{n-i}}$, $\alpha(n)$ goes to $\alpha(n-i)^{p^i}$ while $\eta_j(n)$ goes to $p^j\eta_0(n-i)$ if $0 \leqslant j \leqslant i$, and to $p^i\eta_{j-i}(n-i)$ if $i < j \leqslant n$. Hence,

$$\alpha(n-i)^{p^i} = \Big(\sum_{0\leqslant j\leqslant i} p^ja_j\Big)\eta_0(n-i) + \sum_{i<j\leqslant n} p^ia_j\eta_{j-i}(n-i).$$

Let ω be a p^{n-i}th root of unity. It follows from familiar facts about $\mathbf{Z}[\omega]$ that, under the projection from $\mathbf{Z}G/G^{p^{n-i}}$ to $\mathbf{Z}[\omega]$, $\alpha(n-i)$ goes to p if $i < n$ and to 0 if $i = n$ while $\eta_k(n-i)$ goes to 1 if $k = 0$ and to 0 if $k > 0$. Applying this map to the above equation, we see that:

If $i = 0$, $a_0 = p$;

If $0 < i < n$, we obtain

$$\begin{aligned} p^{p^i} &= \sum_{0\leqslant j<i} p^ja_j + p^ia_i \\ &= p^{p^{i-1}} + p^ia_i \end{aligned}$$

by the induction hypothesis;

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

If $i = n$, $0 = p^{p^{n-1}} + p^n a_n$.

This result admits a more intelligible expression. Let $\epsilon_i = \eta_{i-1}/p^{i-1} - \eta_i/p^i$, $1 \leqslant i \leqslant n$. Since $\eta_i \eta_j = p^i \eta_j$, $i \leqslant j$, the set of ϵ_i forms a set of orthogonal idempotents in $\mathbf{Q}G$. Using the orthogonality, 2·1 may be generalized to

THEOREM 2·2. *$\alpha^e = \Sigma p^{ep^{i-1}} \epsilon_i$, sum over $1 \leqslant i \leqslant n$. If we write $\alpha^e = \Sigma a_{i,e} \eta_i$ for integers $a_{i,e}$, we see that*

$$a_{i,e} = \begin{cases} p^e & (i = 0) \\ (p^{ep^i} - p^{ep^{i-1}})/p^i & (0 < i < n) \\ -p^{ep^{n-1}}/p^n & (i = n). \end{cases}$$

We can now prove Liebeck's result.

THEOREM 2·3. *If G is cyclic of order p^n,*

$$\nu(e, G) = p^n + (e-1)(p^n - p^{n-1}) = p^{n-1} + e(p^n - p^{n-1}).$$

If G is a direct sum of cyclic groups of order p^{n_i},

$$\nu(e, G) - 1 = \Sigma(p^{n_i} - 1) + (e-1)(p^n - p^{n-1})$$

where n is the largest n_i.

Proof. Let x be a generator of the cyclic group G. $(1-x)^{p^{n-1}} \equiv \eta_G$ modulo p while $(1-x)^{p^n} \equiv \eta_G(1-x) = 0$ modulo p so the first result is correct for $e = 1$.

If $e > 1$, $(1-x)^{p^{n-1}-1} \equiv \Sigma x^i$, $0 \leqslant i < p^{n-1}$, modulo p while, by 2·2, $\alpha^e \equiv -p^{e-1}\eta_1$ modulo p^e. Thus $\alpha^e(1-x)^{p^{n-1}-1} \equiv -p^{e-1}\eta_G$ modulo p^e and so $\alpha^e(1-x)^{p^{n-1}} \equiv 0$ modulo p^e which completes the first result.

The second result is an immediate consequence of 1·12.

The point of view adopted in taking α^e as generator of I^m,

$$I = I(\mathbf{Z}, G), \quad m = e(p^n - p^{n-1}),$$

is useful in other computations involving powers of I. Theorem 2·2 provides systematic proofs for the following results of Bachmuth and others, the first appears in (2), the second in (1):

THEOREM 2·4. *If x is a generator of the cyclic group G of order p^n,*

$$(x-1)^{p^n} = p(x-1)^{p^{n-1}}\gamma + p\eta_1\beta,$$

where β is in $I(\mathbf{Z}, G)$ and γ is a unit modulo p^e for all e.

THEOREM 2·5. *Let J be the cyclotomic ideal of $\mathbf{Z}G$, the ideal generated by all sums Σx^i, $0 \leqslant i < p^n$, for all x in G, the cyclic group of order p^n. If $m = e(p^n - p^{n-1})$, then $p^{n-e} I^m$ is in J but $p^{n-e} I^{m-1}$ is not in J, $I = I(\mathbf{Z}, G)$.*

The following are immediate corollaries of Theorem 2·2.

COROLLARY 2·6. *If G is a cyclic group of order p^n generated by an element x and $I = I(\mathbf{Z}, G)$, then*

$$(x^{p^{n-1}} - 1) I^{e(p^n - p^{n-1})} = p^e (x^{p^{n-1}} - 1)\mathbf{Z}G,$$

whence

$$(x^{p^{n-1}} - 1) I^{ep^n} = p^e (x^{p^{n-1}} - 1) I^{ep^{n-1}};$$

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

furthermore, modulo p^{ep^j-j},

$$I^{e(p^n-p^{n-1})}(\mathbf{Z}, G) \equiv I^{e(p^j-p^{j-1})}(\mathbf{Z}, G^{p^{n-j}}).$$

If A is a $\mathbf{Z}G$*-module, these results may be expressed as suggestive Engel-like commutator identities in the group* GA:

If a is in A, then there is an a′ in A such that

$$[a, x, \ldots, x^{p^{n-1}}] = [a', x^{p^{n-1}}]^{p^e},$$

where the first commutator involves $e(p^n-p^{n-1})$ *entries of* x.

If A has exponent dividing p^{ep^j-j}, *and a is in A, there is an a′ in A such that*

$$[a, x, \ldots, x] = [a', x^{p^{n-j}}, \ldots, x^{p^{n-j}}],$$

where the first commutator involves $e(p^n-p^{n-1})$ *entries of* x *and the second* $e(p^j-p^{j-1})$ *entries of* $x^{p^{n-j}}$.

Corollary 2·6 has the familiar corollary that, if G is cyclic of order p and $I = I(\mathbf{Z}, G)$, then $I^p = pI$. Bachmuth asked the extent to which a similar equation holds in the general case; this section concludes with an answer to his question.

PROPOSITION 2·7. *If G is cyclic of order* p^n *and* $I = I(\mathbf{Z}, G)$, *then* I^{p^n} *is equivalent to* $pI^{p^{n-1}}$ *modulo* p^e *if and only if* $n = 1$ *or* $e \leqslant 2$.

Proof. We have seen that $I^{p^n} \equiv pI^{p^{n-1}}$ if $n = 1$ (2·6) or if $e = 1$ (2·3). To see this for $e = 2$, we first observe that, modulo p^k, $I^{p^k}(G) \equiv I^{p^{k-1}}(G^p)\,\mathbf{Z}G$ since, modulo p^k, $(x-1)^{p^k} \equiv (x^p-1)^{p^{k-1}}$ because $(y-1)^p = (y^p-1)+p\alpha$, some α, in general. We have established the case of $n = 1$ so we assume $n > 1$. Modulo p^2,

$$I^{p^n}(G) \equiv I^{p^{n-1}}(G^p)\,\mathbf{Z}G \equiv pI^{p^{n-2}}(G^p)\,\mathbf{Z}G$$

by induction, which is equivalent to $pI^{p^{n-1}}(G)$.

If $n > 1$, we conclude the proof by showing that I^{p^n} is not $pI^{p^{n-1}}$ modulo p^3. First observe that I^{p^n} is not in $pI^{p^{n-1}}$. If so, there is an element α in $\mathbf{Z}G$ for which

$$(x-1)^{p^n} = p(x-1)^{p^{n-1}}\alpha.$$

We pull this equation back to the polynomial ring $\mathbf{Z}[t]$, t an indeterminate, as $(t-1)^{p^n} = p(t-1)^{p^{n-1}}a + (t^{p^n}-1)\,b$, a, b polynomials. But $t^{p^n}-1 = (t-1)\,\phi c$ where $c = \Sigma t^i$, $0 \leqslant i < p^{n-1}$, and ϕ is the cyclotomic polynomial, $\phi = \Sigma t^{ip^{n-1}}$, $0 \leqslant i < p$. Since $t-1$ does not divide ϕ or c, there is a polynomial d for which $b = (t-1)^{p^{n-1}-1}d$ and so $(t-1)^{(p-1)p^{n-1}} = pa + \phi cd$. In $\mathbf{Z}_p[t]$, $(1-t)^{p-1} = \Sigma t^i$, $0 \leqslant i < p$, so that

$$(t-1)^{(p-1)p^{n-1}} = \phi.$$

Comparing these expressions, we see that, in $\mathbf{Z}_p[t]$, $1 = cd$ which is a contradiction because c has degree > 1.

We now induct on n that I^{p^n} is not in $pI^{p^{n-1}}$ modulo p^3 for $n > 1$.

For $n = 2$, if this were so, I^{p^2} is in $pI^p + p^3I$. But p^2I is in I^p (as, for example, in 1·9 of (8)) so that I^{p^2} is in pI^p; a contradiction.

For $n > 2$, modulo p^3, $I^{p^n}(G) \equiv I^{p^{n-1}}(G^p)\,\mathbf{Z}G$ and $pI^{p^{n-1}}(G) \equiv pI^{p^{n-2}}(G^p)\,\mathbf{Z}G$. If $I^{p^n}(G)$

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press

is in $pI^{p^{n-1}}(G)$ modulo p^3, then $I^{p^{n-1}}(G^p)$ is in $pI^{p^{n-2}}(G^p)$ modulo p^3, which would contradict the induction hypothesis.

We thank the N.S.F. for its support and Cambridge University for its hospitality.

REFERENCES

(1) BACHMUTH, S., HEILBRONN, H. A. and MOCHIZUKI, H. Y. Burnside metabelian groups. *Proc. Roy. Soc.* A **307** (1968), 235–250.
(2) BACHMUTH, S. and HUGHES, I. Centers of certain presentations of finite groups. *Notices Amer. Math. Soc.* **13** (1966), 576.
(3) CURTIS, C. and REINER, I. *Representation theory of finite groups and associative algebras* (Interscience, New York, 1962).
(4) HUPPERT, B. *Endliche Gruppen I* (Springer, Berlin, 1967).
(5) JENNINGS, S. A. The structure of the group ring of a p-group over a modular field. *Trans. Amer. Math. Soc.* **50** (1941), 175–185.
(6) LIEBECK, H. Concerning nilpotent wreath products. *Proc. Cambridge Philos. Soc.* **58** (1962), 443–451.
(7) SANDLING, R. The modular group rings of p-groups. Thesis, Univ. of Chicago, 1969.
(8) SANDLING, R. Dimension subgroups over arbitrary coefficient rings, to appear. *J. Algebra.*
(9) SANDLING, R. Subgroups dual to dimension subgroups. *Proc. Cambridge Philos. Soc.* **71** (1972), 33–38.

https://doi.org/10.1017/S0305004100050210 Published online by Cambridge University Press