JOURNAL OF ALGEBRA 21, 216–231 (1972)

The Dimension Subgroup Problem

ROBERT SANDLING

Department of Mathematics, The University, Manchester, U.K. M13 9PL

Communicated by D. Rees

Received August 4, 1970

Whether the terms of the lower central series of a group are associated with the powers of the augmentation ideal of its integral group ring is a question which has been open for over thirty years. This question, the dimension subgroup problem, has achieved notoriety for the number of false proofs it has elicited. In this paper, we record general observations on the problem, verify the conjecture for several new classes of groups and develop generalizations which indicate new lines of research. In a subsequent paper [20], we examine the subgroups attached to group rings over arbitrary coefficient domains.

The general properties of dimension subgroups are set forth in the first section. Several equivalent formulations of the conjecture are given. The subgroups are calculated in a number of special cases.

A minimal counterexample is a finite p-group with cyclic center. In the second section, we take the approach that such reductions make available. The conjecture is established for Abelian-by-cyclic groups and for split extensions of Abelian groups by groups satisfying the conjecture; it follows inductively that the Sylow subgroups of the symmetric groups satisfy the problem and so every p-group embeds in a p-group for which the conjecture is verified.

This analysis provides an unexpected bridge to the work of Passi who conjectured a strong result about the properties of factor sets of extensions of divisible groups by p-groups and showed how it would establish the dimension subgroup conjecture. Here another way of using Passi's conjecture to solve the problem is introduced and applied in a minimal counterexample to obtain new results.

The third section places the problem in a wider context: If G_n is associated with I^n, then G_n is associated with even larger ideals. It may be that these ideals will have to be identified before the dimension subgroup problem can be resolved affirmatively. Some such ideals are discovered by expanding the methods of Passi and Moran. The results obtained are used to establish the fact that the lower central series is associated with the Lie powers of the augmentation ideal for groups of class 5, for metabelian groups and for p-groups whose commutator subgroups have class strictly less than p.

Several results concerning the intersection of the powers of the augmentation ideal are stated in the last section.

1. Introduction

Let G be an arbitrary group and R a commutative ring with unit. Form the group ring RG as the free R-module on the set G with multiplication given as: Write an element γ of RG as a sum $\sum \gamma(x)x$, where $\gamma(x)$ is in R and x is in G; then the product $\gamma\delta$ is defined by

$$(\gamma\delta)(x) = \sum \gamma(y)\delta(z),$$

summed over all y and z in G with $yz = x$.

RG is functorial in R and G. The kernel of the augmentation RG to R induced by collapsing G to 1 is called the augmentation ideal and will be denoted as I or $I(G)$ or $I(R, G)$. Explicitly, I consists of all γ in RG for which $\sum \gamma(x) = 0$. If N is a normal subgroup of G, the projection G to G/N induces RG to RG/N whose kernel is the two-sided ideal $I(N)RG$.

Conversely, we may associate a subgroup of G with an ideal J of RG by considering all x in G for which $x - 1$ is in J; that is, the subgroup $G \cap 1 + J$. If J is two-sided, this subgroup is normal. $I(N)RG$ is the smallest two-sided ideal J for which $N = G \cap 1 + J$.

The problem of identifying the subgroup attached to an ideal is a difficult one. This chapter explores the problem for some familiar ideals. The subgroups attached to the powers of the augmentation ideal are known as the dimension subgroups; we denote them as

$$i_n = i_n(G) = i_n(R, G) = G \cap 1 + I^n(R, G).$$

$i_n(R, G)$ is also functorial in R and G so that it is a fully invariant subgroup of G. A ring homomorphism R to S induces an inclusion $i_n(R, G) \leqslant i_n(S, G)$, so that

$$i_n(\mathbf{Z}, G) \leqslant i_n(R, G)$$

for all R, where $\mathbf{Z}$ is the ring of integers. These facts, readily calculated, are apparent from the expression of $i_n(R, G)$ as the kernel of the natural monoid map G to RG/I^n defined by sending x to the coset of x.

The descending series $\{i_n\}$ in G is of the type studied intensively in Lazard's thesis [12]. Call a descending series $\{H_n\}$ of subgroups of G a Lazard series if

$$[H_n, H_m] \leqslant H_{n+m}.$$

LEMMA 1.1. *The dimension subgroups form a Lazard series.*

Proof. Take x in i_n and y in i_m. Then

$$[x, y] - 1 = x^{-1}y^{-1}(xy - yx) = x^{-1}y^{-1}((x - 1)(y - 1) - (y - 1)(x - 1))$$

which is in I^{n+m}.

As a corollary, we see that i_n contains G_n, the n-th term of the lower central series. Magnus [14] showed that, for G free, $i_n(\mathbf{Z}, G)$ is G_n. The conjecture that this remains true for all G is known as the dimension subgroup problem; it has had a stormy history [2; 4; 5; 13]. Magnus' result implies that the conjecture is equivalent to the proposition that the functor $i_n(\mathbf{Z},\ )$ preserves epimorphisms. In this direction is the following lemma of Jennings [11]:

LEMMA 1.2. *If N is a normal subgroup of G contained in $i_n(R, G)$ and $\bar{G} = G/N$, then $i_n(R, \bar{G}) = \overline{i_n(R, G)}$.*

Proof. We already know $\overline{i_n(R, G)} \leqslant i_n(R, \bar{G})$ by functoriality. For the opposite inclusion, it suffices to observe that $I(N)\, RG$ is in $I^n(R, G)$ so that the isomorphism between $R\bar{G}$ and $RG/I(N)\, RG$ induces one between $I^n(R, \bar{G})$ and $I^n(R, G)/I(N)\, RG$.

Functoriality also shows that $i_n(R,\ )$ respects (unlimited) direct products. The proof of this will be clear from the proof of the following related remark.

LEMMA 1.3. *If $G = HM$ splits over its normal subgroup M, $i_n(G) = i_n(H)(M \cap i_n(G))$.*

Proof. By functoriality, $i_n(H) \leqslant i_n(G)$ while the projection G to $\bar{G} = H$ induces $\overline{i_n(G)} \leqslant i_n(H)$.

This can be refined to

PROPOSITION 1.4. *If $G = HM$ splits over its normal subgroup M and G centralizes M/M', then $i_n(G) = i_n(H)\, i_n(M)$.*

Proof. It suffices to show that $I^n(M) = I^n(G) \cap RM$. We first establish that $I^n(G) = \sum_{i+j=n} I^i(H) I^j(M)$, where $i, j \geqslant 0$ and $I^0(X) = RX$. The identity

$$hm - 1 = (h - 1) + h(m - 1)$$

shows this to be the case for $n = 1$.

For $n > 1$, use induction and the fact that

$$I(M)\, I(H) \subseteq I(H)\, I(M) + I^2(M),$$

a consequence of the hypothesis that $M' = [M, G]$(so $I([M, G]) \subseteq I^2(M)$) and of the identity:

1.5

$$\begin{aligned}(m-1)(h-1) &= (h-1)(m-1) + hm(x-1),\ x = [m, h] \\ &= (h-1)(m-1) + (h-1)(x-1) + (m-1)(x-1) \\ &\quad + (h-1)(m-1)(x-1) + (x-1).\end{aligned}$$

Lastly, if γ is in $I^n(G) \cap RM$, $\gamma = \sum \alpha_k \beta_k$ where α_k is in $I^{i_k}(H)$ and β_k is in $I^{j_k}(M)$, $i_k + j_k = n$.

$$\begin{aligned}\gamma(m) &= \sum \gamma(hm) \text{ summing over } h \text{ in } H \\ &= \sum_h \sum_k \alpha_k(h)\, \beta_k(m) = \sum_k \left(\sum_h \alpha_k(h)\right) \beta_k(m).\end{aligned}$$

But, if $i_k > 0$, $\sum \alpha_k(h) = 0$, so we have $\gamma = \sum(\sum_h \alpha_k(h))\, \beta_k$ summed over all k with $j_k = n$, which is in $I^n(M)$.

Observe that, for G as in 1.4, $G_n = H_n M_n$ so that this lemma verifies the dimension subgroup conjecture for G if it is verified for H and M. An example of such a G is M extended by a group H of inner automorphisms.

We have seen that $i_n(R, G)$ is the kernel of a monoid map G to $\overline{RG/I^n}$. If A is an R-algebra, $\mathfrak{A}$ a two-sided ideal of A, $\bar{A} = A/\mathfrak{A}^n$, then $\overline{1 + \mathfrak{A}}$ forms a group of units in $\bar{A}$; if $A = RG$ and $\mathfrak{A} = I$, the above is a group homomorphism G to $\overline{1 + \mathfrak{A}}$.

LEMMA 1.6. $i_n(R, \overline{1 + \mathfrak{A}}) = 1$. *Consequently, $i_n(R, G)$ is the intersection of the kernels of all homomorphisms G to $\overline{1 + \mathfrak{A}}$, taken over all R-algebras A and ideals $\mathfrak{A}$.*

Proof. Let $H = \overline{1 + \mathfrak{A}}$. Since $H \subseteq \bar{A}$, $\bar{A}$ is an RH-algebra by right multiplication. But $\bar{A} I^n(R, H) = 0$ since $I^n(R, H)$ is generated by products $\gamma = \prod_{1 \leqslant i \leqslant n} (\overline{1 + \alpha_i} - \bar{1})$, α_i in $\mathfrak{A}$, while, if $\bar{\alpha}$ is in $\bar{A}$, $\bar{\alpha}\gamma = \bar{\alpha} \prod_{1 \leqslant i \leqslant n} \bar{\alpha}_1 = 0$. If $\overline{1 + \alpha}$ is in $i_n(R, H)$, then, in $\bar{A}$, $0 = \bar{1}(\overline{1 + \alpha} - \bar{1}) = \bar{\alpha}$.

We have seen that $i_n(R, G)$ is such a kernel. Let N be the kernel of a homomorphism G to $\overline{1 + \mathfrak{A}}$ for some $\mathfrak{A}$ and A. Let $\bar{G} = G/N$. Then $\overline{i_n(R, G)} \leqslant i_n(R, \bar{G})$ but $\bar{G}$ is a subgroup of $\overline{1 + \mathfrak{A}}$ so

$$\overline{i_n(R, G)} \leqslant i_n(R, \overline{1 + \mathfrak{A}}) = 1.$$

This gives another formulation of the dimension subgroup problem: Given a group G, there is a ring A and an ideal $\mathfrak{A}$ with G/G_n a subgroup of $1 + \mathfrak{A}/\mathfrak{A}^n$. The free group case can be established in this manner:

THEOREM 1.7. *If G is a free group, $i_n(\mathbf{Z}, G) = G_n$.*

Proof. We may assume that G is finitely generated (see 2.1). Let A be the free associative ring on the same number of elements and $\mathfrak{A}$ the ideal generated by all elements of weight $\geqslant 1$, in Hall's notation [7]. Hall then shows that G/G_n is a subgroup of $1 + \mathfrak{A}/\mathfrak{A}^n$.

2. INTEGRAL COEFFICIENTS

LEMMA 2.1. *A minimal counterexample to $i_n(\mathbf{Z}, G) = G_n$ is a finite p-group G of class less than n whose center is cyclic.*

Proof. Take x in $i_n(\mathbf{Z}, G)$ but not G_n; $x - 1$ is a sum of products $(x_1 - 1) \cdots (x_n - 1)$, x_i in G; letting H be the subgroup generated by the elements of G appearing in this sum, we see that x is in $i_n(\mathbf{Z}, H)$ but not H_n. We may assume that G is finitely generated. Since $i_n(\mathbf{Z}, G)/G_n \leqslant i_n(\mathbf{Z}, G/G_n)$, we may assume that $G_n = 1$; so class G is less than n.

If $i_n(\mathbf{Z}, P) = 1$ for all finite p-groups P of class less than n, $i_n(\mathbf{Z}, G) \leqslant N$ for every normal subgroup N whose quotient G/N is a finite p-group. But it is a theorem of Hirsch [17, p. 80] that the intersection of such subgroups is trivial. Hence, we may assume that G is a finite p-group of class less than n.

By minimality, $i_n(\mathbf{Z}, G) \leqslant N$ for every nontrivial normal subgroup N of G. But these subgroups intersect trivially unless G has cyclic center.

This reduction shows that the dimension subgroup problem is essentially a problem about finite p-groups.

As an example of the use of 2.1, we give a proof of

LEMMA 2.2. *$i_2(\mathbf{Z}, G) = G'$ for all G.*

Proof. We may assume G is Abelian. Since $\mathbf{Z}G$ is free Abelian, we can define a map $\mathbf{Z}G$ to G by sending x to x. Under this map, $(x - 1)(y - 1)$ goes to $xyx^{-1}y^{-1} = 1$, so that I^2 is in the kernel. Since $x - 1$ goes to x, no $x - 1$ can be in I^2 unless $x = 1$.

We shall generalize this method of proof to solve other cases of the problem. Many diverse methods have been used to establish the following cases:

Free groups, Magnus [14]; groups of class 2, G. Higman [6, 18], Hoare [8]; p-groups of class 3, $p > 2$, Passi [18], Moran [15]; p-groups of class less than p, Moran [16]; p-groups of exponent p, Jennings [11]. We establish the case of Abelian-by-cyclic groups and also verify the conjecture for a class of split extensions large enough to show that every p-group is contained in a p-group which satisfies the conjecture. A new and easy proof for the class 2 case appears in [20].

Let A be a normal Abelian subgroup of an arbitrary group G and let T be a set of left coset representatives. Define a map ρ from $\mathbf{Z}G$ to A by sending $x = ta$ to a. A typical generator of $I(G)\,I(A)$ is of the form $(ta - 1)(a' - 1)$ which goes to 1; thus, $I(G)\,I(A)$ is in the kernel. Working modulo this ideal, we see that

$$I^n(G) \equiv I^n(T) + I([A, (n-1)G]),$$

where $[A, mG]$ is inductively defined as $[[A, (m-1)G], G]$ and where $I(T)$ denotes the subgroup of $\mathbf{Z}G$ generated by all $t - 1$, t in T, for:

A typical generator of $I^n(G)$ is $\gamma = \prod_{1 \leqslant i \leqslant n}(t_i a_i - 1)$. But

$$t_i a_i - 1 \equiv (t_i - 1) + (a_i - 1); \text{ so } \gamma \equiv \prod_{1 \leqslant i \leqslant n}((t_i - 1) + (a_i - 1))$$

so that $\gamma \equiv \prod_{1 \leqslant i \leqslant n}(t_i - 1) + (a_1 - 1)\prod_{2 \leqslant i \leqslant n}(t_i - 1)$. By identity 1.5 and induction on n, the latter term is equivalent to $[a_1, t_2, \ldots, t_n] - 1$.

THEOREM 2.3. *If G is Abelian-by-cyclic, $i_n(\mathbf{Z}, G) = G_n$ for all n.*

Proof. We may assume $G_n = 1$. Let A be a normal Abelian subgroup with $\bar{G} = G/A$ cyclic; select t in G so that $\bar{t}$ is a generator of $\bar{G}$ and let T consist of powers of t. If $a - 1$ is in $I^n(G)$, an analysis as above shows $a - 1 \equiv (t-1)\alpha$, α in $I(G)$ (we assume $n > 1$). Passing to $\mathbf{Z}\bar{G}$, $0 = (\bar{t} - 1)\bar{\alpha}$ so that $\bar{\alpha}$ is in the intersection of $I(\bar{G})$ and its annihilator, which is trivial, so that $\bar{\alpha} = 0$, whence α is in $I(A)\,\mathbf{Z}G$. This shows that $a - 1$ is in $\ker \rho$ although, by definition, it is sent to a. Hence, $a = 1$.

The foregoing analysis may be elaborated for metabelian groups but does not seem conclusive except for class 2 groups and a few others. The next application of the map ρ is to the case in which G splits over A; in this case, T may be chosen as a subgroup of G so that $I^n(T)$ is contained in $I(T)$ which is in the kernel of ρ. Then $I^n(G) \equiv I([A, (n-1)G])$, so we have

THEOREM 2.4. *If G splits over a normal Abelian subgroup A, then $i_n(\mathbf{Z}, G) = i_n(\mathbf{Z}, T)[A, (n-1)G]$, where T is a complement to A. If*

$$i_n(\mathbf{Z}, T) = T_n\,,\; i_n(\mathbf{Z}, G) = G_n\,.$$

Proof. By 1.3, it suffices to calculate $A \cap i_n(\mathbf{Z}, G)$ which contains $[A, (n-1)G]$ and, by the above remarks, is contained in $[A, (n-1)G]$.

Theorem 2.4 allows us to embed groups in groups which satisfy the dimension subgroup problem. This is in general a pointless endeavour since any group embeds in a simple group which satisfies the dimension subgroup problem by default. However, for p-groups, the concept has more substance as the dimension subgroup conjecture is equivalent to the proposition that every p-group embeds in a p-group of the same class which satisfies the conjecture.

The wreath product structure of the Sylow subgroups of the symmetric groups [10, p. 379] shows them to satisfy the conjecture. Let p^d be the order of the smallest set on which the p-group G acts faithfully; equivalently, p^d is the index of the largest core-free subgroup of G. Then G is a subgroup of the symmetric group of degree p^d, which has class p^{d-1} (see [21] for a new proof). Hence,

LEMMA 2.5. *If* $n = p^{d-1}$, *then* $i_{n+1}(\mathbf{Z}, G) = 1$.

Jennings' result [11] provides another bound on the extent to which the conjecture may fail. Let $G_{k,p} = G_k \prod G_i^{p^j}$, the product taken over all i, j with $ip^j \geqslant k$; let d_k be the rank of $G_{k,p}/G_{k+1,p}$ and $n = (p-1)\sum kd_k$. Then $i_{n+1}(\mathbf{Z}, G) = 1$.

Kaloujnine's embedding of a group G, given as an extension of a normal subgroup A by its quotient H, in the wreath product $A \sim H$ [10, p. 99] provides a more interesting application of 2.4. Taking A Abelian, we have by induction that H is contained in a group H^* satisfying the conjecture. But $G \leqslant A \sim H \leqslant A \sim H^*$, and $A \sim H^*$ satisfies the dimension subgroup problem by 2.4; so we have again suceeded in embedding a p-group in another which satisfies the conjecture.

This embedding holds out another possibility. For G a minimal counterexample, we may take A to be cyclic and central and H to be of class less than class G. The usual embedding $G \leqslant A \sim H$ depends upon the choice of factor set f from $H \times H$ to A; we may hope to solve the problem by choosing f so that G is contained in a split subgroup of class equal to class G. The largest such subgroup in which G could be so embedded can be calculated by viewing $A \sim H$ as the group ring $\mathbf{Z}_{p^e}H$, p^e the order of A, extended by H in its right regular representation; it is the right annihilator of $I^n(\mathbf{Z}_{p^e}, H)$ extended by H. The proposition that f can be chosen to embed G in this subgroup is, up to possible extension of G by central product over A (see 3.11), equivalent to Passi's conjecture [18] that any factor set $H \times H$ to $\mathbf{Q}/\mathbf{Z}$ is cohomologous to another which, when extended by linearity to $\mathbf{Z}H \times \mathbf{Z}H$ to $\mathbf{Q}/\mathbf{Z}$, kills the subgroup $I^n(\mathbf{Z}, H) \times \mathbf{Z}H$, $n = 1 +$ class H. Passi verified his conjecture for class $H = 1$ and for class $H = 2$, $p > 2$; he used this to prove cases of the dimension subgroup problem in a manner quite different from the above.

3. THE LIE POWERS OF THE AUGMENTATION IDEAL

If A and B are subsets of $\mathbf{Z}G$, define the Lie bracket (A, B) as the subgroup of $\mathbf{Z}G$ generated by all

$$(\alpha, \beta) = \alpha\beta - \beta\alpha,$$

α in A, β in B. Even if A and B are ideals of $\mathbf{Z}G$, (A, B) need not be an ideal.

LEMMA 3.1. *If H and K are subgroups of G,*

$$(I(H), I(K))\mathbf{Z}G = I([H, K])\mathbf{Z}G.$$

Proof. As right ideals, the left is generated by all $(h-1, k-1) = (h, k)$, h in H, k in K while the right by all $[h, k] - 1$. But

$$[h, k] - 1 = (h^{-1}, k^{-1})\, hk.$$

Define the Lie powers of I as $I_1 = I$ and, inductively, $I_n = (I_{n-1}, I)\mathbf{Z}G$. Denote $G \cap 1 + I_n$ as $i_{(n)} = i_{(n)}(\mathbf{Z}, G)$. That $G_n \leqslant i_{(n)}$ is a Corollary of 3.1. On the other hand, I_n is contained in I^n so that $i_{(n)} \leqslant i_n$. Thus the dimension subgroup conjecture implies the conjecture that $G_n = i_{(n)}$. To prove this, we may again assume that G is a finite p-group of class $< n$ with cyclic center.

The methods used in establishing cases of the dimension subgroup problem may be extended to solve this problem in roughly twice as many cases (because class G is roughly twice class G'). We shall establish the following cases of $G_n = i_{(n)}(\mathbf{Z}, G)$:

THEOREM 3.2. *G arbitrary and $n \leqslant 6$.*

THEOREM 3.3. *G p-group with class $G' < p$ and n arbitrary.*

COROLLARY 3.4. *G p-group and $n \leqslant 2p$.*

COROLLARY 3.5. *G metabelian and n arbitrary.*

The last two are immediate consequences of 3.3, although 3.5 can be obtained readily without 3.3. These cases provide some evidence for the dimension subgroup problem; their proofs provide a larger context in which to understand this problem. The conjecture is $G_n = G \cap 1 + I^n$; we shall see that $G_n = G \cap 1 + J$, for ideals J generally strictly greater than I^n.

The key to these results is a description of I_n by sums of products of the augmentation ideals of the terms of the lower central series of G. This requires several preliminary observations. The first serves as a model and is of interest for the integral group ring problem:

LEMMA 3.6. *If N and M are normal subgroups of G,*

$$\begin{aligned}(I(N)\mathbf{Z}G, I(M)\mathbf{Z}G)\mathbf{Z}G &= I([N, M])\mathbf{Z}G + I(N)I(M)I(G')\mathbf{Z}G \\ &\quad + I(N)I([M, G])\mathbf{Z}G + I([N, G])I(M)\mathbf{Z}G\end{aligned}$$

Furthermore, $[N, M]$ *may be characterized as*

$$G \cap 1 + (I(N)\mathbf{Z}G, I(M)\mathbf{Z}G)\mathbf{Z}G.$$

Proof. The left is generated as right ideal by all $(\alpha x, \beta y)$, α in $I(N)$, β in $I(M)$, x and y in G. But

$$(\alpha x, \beta y) = \alpha(x, \beta) y + \alpha\beta(x, y) + (\alpha, \beta) yx + \beta(\alpha, y)x,$$

which is seen to be in the right by use of 3.1 and its corollary that $I(H)I(K)\mathbf{Z}G$ is in $I(K)I(H)\mathbf{Z}G + I([H, K])\mathbf{Z}G$.

The opposite inclusion is established term by term: the first by 3.1; the second, being generated by all $\alpha\beta(x, y)$ since $I_2 = I(G')\mathbf{Z}G$ by 3.1, will follow from the above equation once the last two terms are settled; the third follows from the equation $\alpha(\beta, x) = (\alpha, \beta x) + (\beta x, \alpha x)x^{-1}$ and the fact that M is normal; the fourth by symmetry since, mod $I([N, M])\mathbf{Z}G$, $I([N, G]) I(M)\mathbf{Z}G$ may be replaced by $I(M) I([N, G])\mathbf{Z}G$.

To prove the last assertion, we may assume that $[N, M] = 1$. But then we can show that $1 = G \cap 1 + I(N) I(M)\mathbf{Z}G$ which suffices. For this we may assume that $G = NM$ by the following principle:

LEMMA 3.7. *If H is a subgroup of G and J a right ideal of $\mathbf{Z}H$ contained in $I(H)$, then $G \cap 1 + J\mathbf{Z}G = H \cap 1 + J$.*

To prove this, let T be a set of coset representatives for H in G; then $J\mathbf{Z}G$ is the direct sum of all Jt, t in T.

If $G = NM$, $A = N \cap M$ is central and $I(N) I(M)$ is already an ideal of $\mathbf{Z}G$. It suffices to choose coset representatives for A so that the associated map ρ from $\mathbf{Z}G$ to A has $I(N) I(M)$ in its kernel. Let S be a set of representatives for A in N and T a set for A in M, both containing 1; then the set ST is a set of representatives for A in G. Taking sa in N and ta' in M, we see that $(sa - 1)(ta' - 1)$ goes to $aa'a^{-1}a'^{-1} = 1$ under ρ.

The next lemma is technical, its proof little more than that of 3.1:

LEMMA 3.8. *If N_i are normal subgroups of G, $1 \leqslant i \leqslant k$, then $(\prod I(N_i), I(M))\mathbf{Z}G$ is contained in the sum of all products*

$$\prod_{i<j} I(N_i)\, I([N_j, M]) \prod_{i>j} I(N_i)\, \mathbf{Z}G.$$

Proof. Taking x_i in N_i and y in M, we have

$$\Big(\prod (x_i - 1), y - 1\Big) = \sum_j \prod_{i<j} (x_i - 1)(x_j - 1)(y - 1) \prod_{i>j} (x_i - 1).$$

We come now to the main result of this section:

THEOREM 3.9. *$I_n = I(G_n)\mathbf{Z}G + \sum \prod_j I(G_{n_j})\mathbf{Z}G$, sum over all n_j, $n \geqslant n_j > 1$, for which $\sum (n_j - 1) = n - 1$.*

Proof. We show that the right is contained in the left by showing that $\prod I(G_{n_j})\mathbf{Z}G$ is in I_n, where $1 \leqslant j \leqslant k$, $n \geqslant n_j \geqslant 1$ and $\sum (n_j - 1) = n - 1$; we allow $n_j = 1$ to simplify the induction, which is on k and then on n_k.

For $k = 1$, this is $I(G_n)\mathbf{Z}G$ is in I_n. For $k > 1$ and $n_k = 1$, we conclude by induction on k. We assume that $k > 1$ and $n_k > 1$. By 3.1, $\prod I(G_{n_j})\mathbf{Z}G$ is generated by all $\alpha(\beta, x)$ where α is in $\prod_{1 \leqslant j < k} I(G_{n_j})$, β is in $I(G_{n_k - 1})$ and x is in G. But $\alpha(\beta, x) = (\alpha\beta, x) - (\alpha, x)\beta$. $(\alpha\beta, x)$ is in $(\prod_{1 \leqslant j < k} I(G_{n_j}) I(G_{n_k - 1}), I)$ which is in $(I_{n-1}, I)\mathbf{Z}G = I_n$ by induction on n_k while $(\alpha, x)\beta$ is in $(\prod_{1 \leqslant j < k} I(G_{n_j}), I) I(G_{n_k - 1})$ which, by 3.8, is in

$$\sum_{1 \leqslant i < k} \prod_{1 \leqslant j < i} I(G_{n_j}) I(G_{n_i + 1}) \prod_{i < j < k} I(G_{n_j}) I(G_{n_k - 1})$$

which is in I_n by induction on n_k.

To show that the left is in the right, we induct on n, the statement being clear for $n = 2$. Assuming equality for $n - 1$, it suffices to show that, for $n - 1 \geqslant n_j > 1$, $\sum (n_j - 1) = n - 2$, $(\prod_j I(G_{n_j})\mathbf{Z}G, I)$ is in I_n. By the identity $(\alpha x, y) = \alpha(x, y) + (\alpha, x)y$, we see that this Lie bracket is contained in

$$\prod_j I(G_{n_j}) I(G') \mathbf{Z}G + \left(\prod I(G_{n_j}), I\right) \mathbf{Z}G.$$

The first product is in the right by definition, the second by use of 3.8.

I_n admits other expressions which we state but shall not use. The first is clear from 3.9 while the second requires a little proof which we omit.

COROLLARY 3.10.

$$I_n = I(G_n)\, \mathbf{Z}G + \sum \prod_j I_{n_j},$$

sum over all n_j, $n > n_j > 1$, *for which* $\sum (n_j - 1) = n - 1$.

$$I_n = I(G_n)\, \mathbf{Z}G + \sum \prod I^{t_j}(G_j)\, \mathbf{Z}G,$$

sum over all $t_j \geqslant 0$ *for which* $\sum_{n \geqslant j > 1} t_j(j - 1) = n - 1$.

We can now prove the results 3.2 to 3.5. Since $I_2 = I(G')\mathbf{Z}G$, Lemma 3.6 shows directly that $i_{(n)}(\mathbf{Z}, G) = G_n$ for all G and $n \leqslant 3$. The other results follow indirectly by translating the question of I_n in $\mathbf{Z}G$ to a question about ideals of $\mathbf{Z}G'$, a process which leads to suggestive generalizations of the dimension subgroup conjecture. The following proof of the metabelian case will serve as model:

Proof of 3.5. Let G be metabelian. To prove $i_{(n)}(\mathbf{Z}, G) = G_n$, we may assume $G_n = 1$. We assume $n > 2$. By 3.7 and 3.9, $i_{(n)}(\mathbf{Z}, G) = G' \cap 1 + J$ where $J = \sum \prod_j I(G_{n_j})\mathbf{Z}G'$, sum over all n_j, $n \geqslant n_j \geqslant 2$, for which $\sum (n_j - 1) = n - 1$. But $n > 2$; so J is contained in $I^2(G')$; so

$$i_{(n)}(\mathbf{Z}, G) \leqslant i_2(\mathbf{Z}, G') = 1$$

since G' is Abelian.

This has the corollary that $i_{(n)}(\mathbf{Z}, G) = G_n$ for all G and $n \leqslant 4$. To stretch this to the whole of 3.2, we again use 3.7 and 3.9 as above and observe that, upon substitution of G' for H, it suffices to prove:

THEOREM 3.11. *For an arbitrary group H with center $Z(H)$,*

$$H_3 = H \cap 1 + I^3(H) + I(H)I(Z(H)).$$

Proof. The usual reductions show that we may assume H to be a finite p-group of class 2 with cyclic center. Furthermore, we may assume that H can be expressed as an extension of its center $Z(H)$ (write $Z(H) = A$) by an Abelian quotient $\bar{H}$ defined by a factor set f from $\bar{H} \times \bar{H}$ to A, where f is a bilinear map; since f is a factor set, bilinearity is equivalent to $I^2(\mathbf{Z}, \bar{H}) \times \mathbf{Z}\bar{H}$ being killed by f extended to a map $\mathbf{Z}\bar{H} \times \mathbf{Z}\bar{H}$ to A:

Embedding A in $\mathbf{Q}/\mathbf{Z}$, we extend f to a cocycle $\bar{H} \times \bar{H}$ to $\mathbf{Q}/\mathbf{Z}$. As remarked at the end of Section 2, Passi [18] has proved that f is cohomologous to a factor set g from $\bar{H} \times \bar{H}$ to $\mathbf{Q}/\mathbf{Z}$ for which $I^2(\mathbf{Z}, \bar{H}) \times \mathbf{Z}\bar{H}$ is killed by the extended g. But $\bar{H}$ is finite; so we may view g as a factor set $\bar{H} \times \bar{H}$ to some cyclic p-group A^* containing A. Since g and f are cohomologous, the group H^* defined by g is the central product of A^* and H with the central subgroup A amalgamated. But then $I^3(H) + I(H)I(Z(H))$ is in

$$I^3(H^*) + I(H^*)I(Z(H^*));$$

so we may assume $H = H^*$ to prove 3.11; that is, we may assume f is bilinear.

f is defined by a set T of coset representatives for A in H; as before, T defines a map ρ from $\mathbf{Z}H$ to A. We conclude by showing that ker ρ contains $I^3(H) + I(H)I(Z(H))$.

Since $Z(H) = A$, a typical generator of $I(H)I(Z(H))$ is $(ta - 1)(a' - 1)$ where t in T, a, a' in A. But this goes to $aa'a^{-1}a'^{-1} = 1$ under ρ.

A typical generator of $I^3(H)$ is $(t_1a_1 - 1)(t_2a_2 - 1)(t_3a_3 - 1)$ which ρ sends to $f(\overline{t_1t_2}, \bar{t}_3)f(\bar{t}_1, \bar{t}_3)^{-1}f(\bar{t}_2, \bar{t}_3)^{-1}$ by the definition of a factor set. But this is 1 by the assumed bilinearity of f.

We now come to the proof of 3.3, which relies upon a clever application by Moran [16] of a substantial theorem of Lazard. We first prove a special case which provides a model for the general case and whose proof is selfcontained. This is the case of class 2-by-Abelian p-groups, p odd. Using 3.7 and 3.9 as before, it suffices to show:

LEMMA 3.12. *Let H be a p-group, p odd. Then*

$$H_3 = H \cap 1 + I^3(H) + \sum (x-1)(y-1)\mathbf{Z}H,$$

the sum taken over all pairs x, y of commuting elements.

Proof. As usual, we may assume $H_3 = 1$. Since p is odd, we may define the operation $x + y = xy[x, y]^{-1/2}$ on H; that $L = H$ under the operation $+$ forms an Abelian group is an observation which apparently originated with Hopkins [9] and which is easy to verify. Define a map μ from $\mathbf{Z}H$ to L by sending x to x for all x in H. If x and y commute, $(x-1)(y-1)$ is sent to $xyx^{-1}y^{-1} = 1$; so it suffices to show that I^3 is also in the kernel of μ.

Taking x, y, z in H, we see that

$$(x-1)(y-1)(z-1) = (xyz - yz) + (z - xz) + ((-xy + x) + y)$$

is sent by μ to $x[x, y]^{1/2}[x, z]^{1/2} + x^{-1}[z, x]^{1/2} + [y, x]^{1/2}$ in L which is readily seen to be 1.

The Abelian group L above admits another operation derived from H, namely, $(x, y) = [x, y]$, under which it becomes a Lie ring. This is a small portion of a theory of Lazard, the inversion of the Campbell–Hausdorff formula, which asserts [12, p. 178 and preceding]:

THEOREM 3.13. *If G is a p-group of class $< p$, the set G may be considered as a Lie ring L of class $=$ class G under the operations*

$$x + y = xy[x, y]^{-1/2}[x, y, y]^{-1/12}[y, x, x]^{-1/12} \cdots,$$
$$(x, y) = [x, y][x, y, y]^{1/2} \cdots.$$

If L is p-Lie ring of class $<p$, the set L may be considered as a p-group H of class $=$ class L under the operation of Campbell–Hausdorff multiplication

$$xy = x + y + 1/2[x, y] + \cdots.$$

Furthermore, if L is so obtained from a p-group G and H is so obtained from L, then H is isomorphic to G.

The Campbell–Hausdorff formula is defined in the context of free Lie rings over $\mathbf{Q}$ by means of formal power series for log and exp, as

$$xy = \log((\exp x)(\exp y))$$

which Dynkin [3] expanded as

$$xy = \sum_k ((-1)^{k-1}/k) \sum \psi(x^{a_{11}} y^{a_{12}} \cdots x^{a_{1k}} y^{a_{2k}}) / \prod (a_{ij}!),$$

where the sum is over all $a_{ij} \geqslant 0$, $1 \leqslant i \leqslant 2$, $1 \leqslant j \leqslant k$, such that $a_{1_j} + a_{2_j} > 0$ for all j, and where

$$\psi(y_1 \cdots y_n) = 1/n(\cdots (y_1, y_2), \cdots, y_n).$$

It applies to p-Lie rings of class $<p$ because p appears in the denominator of a coefficient of a Lie bracket only if the Lie bracket has weight $\geqslant p$ when, by assumption, it is 0.

Lazard's theorem allows us to consider any p-group H of class $<p$ as a Lie ring L under Campbell–Hausdorff multiplication. Moran observed that calculation in $\mathbf{Z}H$ can be carried out more readily in this context than if H is considered only as an abstract group. For example, the proof of 3.12 uses the inverse process but the calculations become unwieldy for class greater than 2. The key to Moran's results is the expression for the product of any number of elements, namely,

LEMMA 3.14.

$$\begin{aligned} x_1 \cdots x_n &= \log(e^{x_1} \cdots e^{x_n}) \\ &= \sum_k ((-1)^{k-1}/k) \sum \psi(x_1^{a_{11}} \cdots x_n^{a_{n1}} x_1^{a_{12}} \cdots x_1^{a_{1k}} \cdots x_n^{a_{nk}}) / \prod (a_{ij}!), \end{aligned}$$

where the sum is over all $a_{ij} \geqslant 0$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant k$, *such that* $\sum_i a_{ij} > 0$ *for all* j.

Moran then shows that, if $c =$ class H, I^{c+1} is in the kernel of the map μ from $\mathbf{Z}H$ to L defined by sending x to x, x in H. We give his exposition here, the introduction of Lazard series and Lemma 3.16 being new.

THEOREM 3.15. *Let H be a p-group and $n \leqslant p$. Then*

$$H_n = H \cap 1 + \sum \sum \prod_j I(K_{i_j}) \, \mathbf{Z}G,$$

where the first sum is over all Lazard series $\{K_i\}$ *in* H *and the second sum is over all sets of integers* $i_j \geqslant 1$, *for which* $K_c \leqslant H_n$ *where* $c = \sum i_j$.

Proof. We may assume $H_n = 1$ so that class $H < p$ and H may be viewed as a Lie ring L as above. Thus the map μ from $\mathbf{Z}H$ to L is available. It suffices to show that $\prod_{1 \leqslant j \leqslant m} I(K_{i_j})$ is in ker μ for all Lazard series $\{K_i\}$ and integers

i_j as described. This is generated as Abelian group by all products $(1 - x_1) \cdots (1 - x_m)$, where x_j is in K_{i_j}. $\gamma = (1 - x_1) \cdots (1 - x_m) = \sum (-1)^S x_S$, sum over all subsets S of $\{1,..., m\}$, where, if S consists of integers s_i, $1 \leqslant s_1 < \cdots < s_d \leqslant m$, $(-1)^S = (-1)^d$ and $x_S = x_{s_1} x_{s_2} \cdots x_{s_d}$.

Under μ, γ goes to $\sum (-1)^S \mu(x_S)$. Let T be a proper subset of $\{1,..., m\}$; choose integers $a_{ij} \geqslant 0$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant k$, such that $a_{sj} = 0$ for all j if s is not in T. Thus the term

$$w(a_{ij}) = (-1)^{k-1} \psi(x_1^{a_{11}} \cdots x_m^{a_{mk}})/k \prod (a_{ij}!)$$

does not involve the element x_s for s not in T. $w(a_{ij})$ appears in the expression for $\mu(x_S)$ given by 3.14 if and only if T is a subset of S; but it appears with the coefficient $(-1)^S$ so that, in the expression for $\mu(\gamma)$, $w(a_{ij})$ appears with the coefficient $\sum (-1)^S$, sum over all subsets S which contain T. Since T is proper, this coefficient is 0.

To show $\mu(\gamma) = 0$, it remains to dispose of those terms which involve x_i for all i. It suffices to show:

LEMMA 3.16. *Let $\{K_i\}$ be a Lazard series in a p-group H of class $<p$. Let i_j be integers, $1 \leqslant j \leqslant k$, such that $K_c = 1$, where $c \leqslant \sum i_j$. Take $x_j \in K_{i_j}$. Then, in the associated Lie ring, $(...(x_1, x_2),..., x_k) = 0$.*

Proof. We use reverse induction on the following lists of integers $(s, m_c, m_{c-1},..., m_1)$ under dictionary ordering where $s = \sum i_j$ and m_n is the number of $i_j \geqslant n$, to show that $(...(x_1, x_2),..., x_k) = 0$ for all choices of x_j in K_{i_j}.

If $s \geqslant cd$, $d =$ class H, this is so as either $k > d$ or there is some $i_j > c$.

To proceed with the induction we use the fact that $[x, y]$ in H is $(x, y) +$ terms of weight $\geqslant 3$, which may be readily calculated from the first few terms of the Campbell–Hausdorff formula. But then

$$\begin{aligned}(...(x_1, x_2), x_3),..., x_k) &= (...([x_1, x_2], x_3),..., x_k) \\ &+ \text{terms involving at least three } x_i\text{'s}, i = 1 \text{ or } 2.\end{aligned}$$

The induction hypothesis shows immediately that the latter terms are 0 since s increases. The first term is eliminated because $[x_1, x_2]$ is in

$$[K_{i_1}, K_{i_2}] \leqslant K_n, \qquad n = i_1 + i_2;$$

so that m_n increases.

With 3.15 proved, we can see that the dimension subgroup problem is true for p-groups of class $<p$, that is, $i_n(\mathbf{Z}, H) = H_n$ for all p-groups H and $n \leqslant p$. Choose the lower central series as a Lazard series $\{K_i\}$ and integers $i_j = 1$, $1 \leqslant j \leqslant n$; so 3.15 implies that $H_n = H \cap 1 + I^n(H)$.

Returning to the proof of 3.3, we see by 3.7 and 3.9 that, assuming $G_n = 1$,

$$i_{(n)}(\mathbf{Z}, G) = G' \cap 1 + \sum \prod_j I(G_{n_j})\, \mathbf{Z}G'.$$

But we are assuming that class $G' < p$, so that 3.15 applies to $H = G'$. Let $K_i = G_{i+1}$; then $[K_i, K_j] \leqslant K_{i+j+1}$; so $\{K_i\}$ is a Lazard series and $i_{(n)}(\mathbf{Z}, G) = G' \cap 1 + \sum \prod_j I(K_{i_j})\mathbf{Z}G'$, sum over integers i_j, $n > i_j > 1$, for which $\sum i_j = n - 1$. Let $c = 1 +$ class G' which is $\leqslant p$; since $K_{n-1} = G_n = 1$, $K_{n-1} \leqslant G_c' = 1$; so 3.15 gives

$$1 = G_c' \geqslant G' \cap 1 + \sum \prod_j I(K_{i_j})\, \mathbf{Z}G' = i_{(n)}(\mathbf{Z}, G).$$

4. The Transfinite Powers of the Augmentation Ideal

If the dimension subgroup conjecture is true, then G_ω, the intersection of all G_n, is the subgroup attached to the ideal I^ω, the intersection of all I^n, $I = I(\mathbf{Z}, G)$. Buckley [1] showed that this was the case for finite groups; thus, by the usual reductions we have

Theorem 4.1. *Let G be finitely generated. Then*

$$i_\omega = G \cap 1 + I^\omega = G_\omega .$$

If the dimension subgroup conjecture is false, a search for counterexamples to $i_\omega = G_\omega$ among infinite groups might well be more promising than a search for a minimal counterexample to $i_n = G_n$ among finite p-groups.

A proof of 4.1 for finite groups may be obtained from the following decomposition of I^ω.

Lemma 4.2. *$I^\omega = I(G_\omega)\mathbf{Z}G + \sum I(P)I(Q)\mathbf{Z}G$, the sum taken over all p-subgroups P and q-subgroups Q where $p = q$ and $[P, Q] = 1$.*

This lemma and methods of Gruenberg and Roseblade lead to a calculation of $i_{\omega+n} = G \cap 1 + I^\omega I^n$ (see [19]).

Theorem 4.3. *Let $N = G_\omega$ and N_p be a Sylow p-subgroup of N and S_p a Sylow p-subgroup of G for all p. Then*

$$i_{\omega+n} = N' \prod [N_p, S_q, S_r] \prod [N_p, nS_p],$$

where the first product is taken over all triples of district primes p, q, r and the second over all primes p. Furthermore, $I^\omega/I^\omega I^n$ is isomorphic to $i_\omega/i_{\omega+n}$.

ACKNOWLEDGMENT

We wish to thank James Roseblade and John Thompson for their help and encouragement, the N.S.F. for its support and Cambridge University for its hospitality.

REFERENCES

1. J. BUCKLEY, On the D-series of a finite group, *Proc. Amer. Math. Soc.* **18** (1967), 185–186.
2. P. COHN, Generalization of a theorem of Magnus, *Proc. London Math. Soc.* (3) **2** (1952), 297–310.
3. E. B. DYNKIN, Normed Lie algebras and analytic groups, *Uspehi Mat. Nauk (N.S.)* **5** (1950), 135–186 (Russian); Amer. Math. Soc. Translations 97, Providence, R.I., 1953.
4. R. H. FOX, Free differential calculus I, *Ann. of Math.* **57** (1953), 547–560.
5. O. GRÜN, Zusammenhang zwischen Potenzbildung und Kommutatorbildung, *J. Reine Angew. Math.* **182** (1940), 158–177.
6. K. W. GRUENBERG, "Some cohomological topics in group theory," Queen Mary College Math. Notes, London, 1968; Lecture Notes in Math. 143, Springer, Berlin, 1970.
7. P. HALL, "Nilpotent Groups," Cand. Math. Congress, Univ. of Alberta, 1957; Queen Mary College Math. Notes, London, 1970.
8. A. H. M. HOARE, Group rings and lower central series, *J. London Math. Soc.* (2) **1** (1969), 37–40.
9. C. HOPKINS, Metabelian groups of order p^m, $p > 2$, *Trans. Amer. Math. Soc.* **37** (1935), 161–195.
10. B. HUPPERT, "Endliche Gruppen I," Springer, Berlin, 1967.
11. 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.
12. M. LAZARD, Sur les groupes nilpotents et les anneaux de Lie, *Ann. École Norm. Sup.* **71** (1954), 101–190.
13. G. LOSEY, On dimension subgroups, *Trans. Amer. Math. Soc.* **97** (1960), 474–486.
14. W. MAGNUS, Über Beziehungen zwischen höheren Kommutatoren, *J. Reine Angew. Math.* **177** (1937), 105–115.
15. S. MORAN, to appear.
16. S. MORAN, Dimension subgroups modulo n, *Proc. Camb. Phil. Soc.* **68** (1970), 579–582.
17. H. NEUMANN, "Varieties of Groups," Springer, Berlin, 1967.
18. I. B. S. PASSI, Dimension subgroups, *J. Algebra* **9** (1968), 152–182.
19. R. SANDLING, The modular group rings of p-groups, Thesis, Univ. of Chicago, Chicago, Ill., 1969.
20. R. SANDLING, Dimension subgroups over arbitrary coefficient rings, *J. Algebra* **21** (1972), 250–265.
21. R. SANDLING, Subgroups dual to dimension subgroups, *Proc. Camb. Phil. Soc.* **71** (1972), 33–38.