JOURNAL OF ALGEBRA 21, 250–265 (1972)

Dimension Subgroups over Arbitrary Coefficient Rings

ROBERT SANDLING

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

Communicated by D. Rees

Received August 25, 1970

0. INTRODUCTION

Let G be a group and R a commutative ring with unit. The augmentation ideal $I(R, G)$ is the kernel of the homomorphism (called the augmentation) from the group ring RG to 1 induced by collapsing G to the unit group. The n-th dimension subgroup modulo R, $i_n(R, G)$, is the set of group elements x such that $x - 1$ lies in the n-th power of $I(R, G)$, that is,

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

The dimension subgroup problem asks whether $i_n(\mathbf{Z}, G) = G_n$, the n-th term of the lower central series of G. Results on this problem have been set down in [11, 12]. This paper investigates the subgroups for the general ring R. If the dimension subgroup conjecture is true, this investigation is successful; that is, it is possible to express $i_n(R, G)$ in terms of certain canonical subgroups of G and certain dimension subgroups $i_n(\mathbf{Z}_{p^e}, G)$, where $\mathbf{Z}_{p^e}$ is the ring of integers modulo the prime power p^e. The expression depends upon the arithmetic of the ring R. The analysis of $i_n(R, G)$, carried out in Section 2, is largely a study of this arithmetic.

The first section examines the modular dimension subgroups $i_n(\mathbf{Z}_{p^e}, G)$. Using Lie-theoretic methods, Lazard calculated these subgroups for free groups. His subgroups are characterized here group-theoretically; they are not generally the appropriate subgroups but are seen to be closely related.

Next a systematic exposition is given of an old method of finding sets of generators for the powers of the augmentation ideal. Results of Jennings and of Lazard on $\mathbf{Z}_pG$ are established.

The section concludes with the calculation of the first three modular dimension subgroups. Included here is a new proof of the dimension subgroup conjecture for class 2 groups. The method used could solve simultaneously both the dimension subgroup problem and the integral group ring problem

for p-groups. For class 2 groups, the program is feasible and establishes as well the fact that G_2/G_3 is a summand of I^2/I^3, an analog of the familiar isomorphism between G/G' and I/I^2. For groups of higher class, the scheme becomes oppressively complex but perhaps not impossible.

1. Modular Coefficients

We turn now to the calculation of $i_n = i_n(e, G) = i_n(\mathbf{Z}_{p^e}, G)$. It will be seen in the next section that these subgroups are fundamental to the calculation of $i_n(R, G)$ for an arbitrary ring R. For a finite p-group, they filter the integral subgroups and so give hope of a solution of the dimension subgroup problem.

Lemma 1.1. *If G is a finite p-group, $i_n(\mathbf{Z}, G)$ is the intersection of all $i_n(e, G)$, $e \geqslant 1$.*

Proof. Since I/I^2 is isomorphic to G/G', there is an integer e for which p^eI is contained in I^n, $I = I(\mathbf{Z}, G)$. Since $\mathbf{Z}_{p^e}G$ is $\mathbf{Z}G/p^e\mathbf{Z}G$, $x - 1$ in $I^n(\mathbf{Z}_{p^e}, G)$ implies that $x - 1$ is in $I^n + p^eI$ which is I^n. Hence, $i_n(e, G)$ is contained in $i_n(\mathbf{Z}, G)$. The opposite inclusion is obvious.

We now establish a property of i_n which will enable us to uncover a large portion of i_n.

Lemma 1.2. *If $k \geqslant 0$, $i_n(e, G)^{p^{e+k}}$ is contained in $i_{np^{1+k}}(e, G)$.*

Proof. With $m = p^{e+k}$, $x^m - 1 = \sum \binom{m}{i}(x-1)^i$. For $i < p^{1+k}$, p^e divides $\binom{m}{i}$. Thus, if $x - 1$ is in I^n modulo p^e, $x^m - 1$ is in $I^{np^{1+k}}$ modulo p^e.

Since G_n is in i_n for all n, we see that, if $ip^j \geqslant np^{e-1}$, $G_i^{p^j}$ is in i_n. Denote by G_{n,p^e} the subgroup generated by G_n and all such $G_i^{p^j}$; so that

Lemma 1.3. *G_{n,p^e} is contained in $i_n(\mathbf{Z}_{p^e}, G)$.*

The subgroups G_{n,p^e} first appeared in Lazard's thesis. He showed that, if G is free, G_{n,p^e} is the n-th "groupe de dimension mod p^e" in his terminology [6, p. 125]. But his "dimension subgroups" are readily seen to contain those defined here; so 1.3 gives

Theorem 1.4. *If G is free, $i_n(\mathbf{Z}_{p^e}, G) = G_{n,p^e}$.*

For $e = 1$, 1.4 is already a result of Zassenhaus [13]. Lazard completed this by showing $i_n(\mathbf{Z}_p, G) = G_{n,p}$ for all G [6, p. 135]; we give a simplified version of his proof in 1.22. Jennings [4] had earlier shown that the series $\{i_n(\mathbf{Z}_p, G)\}$ is characterized as the smallest descending central series $\{H_n\}$ for which $H_n{}^p$ is in H_{np}.

Such a characterization of $\{G_{n,p^e}\}$ can be given for $e > 1$. The technique used, a generalization of Hall–Petrescu words due to Rex Dark, will establish group-theoretically a further property of $\{G_{n,p^e}\}$, that it forms a Lazard series (a descending series of subgroups $\{H_n\}$ is Lazard if $[H_n, H_m] \leqslant H_{n+m}$ for all n, m); this property is a consequence of the functoriality of the subgroups G_{n,p^e}, the fact that $\{i_n\}$ forms a Lazard series and Theorem 1.4 of Lazard, whose proof uses Lie theory. We show

THEOREM 1.5. *The series $\{G_{n,p^e}\}$ is characterized as the smallest descending central series $\{H_n\}$ in G for which $H_n^{p^{e+k}}$ is contained in $H_{np^{1+k}}$ for all k. Furthermore, $\{G_{n,p^e}\}$ is a Lazard series.*

Dark's result, Theorem C of his thesis [1], is the following.

THEOREM 1.6. *Let Y_i be a subset of G, $1 \leqslant i \leqslant m$. Let π be a word in letters from the sets Y_i. If $\alpha = (\alpha_1, \ldots, \alpha_m)$ is a list of m nonnegative integers, define $\pi(\alpha)$ to be the element of G obtained by replacing each appearance in π of a letter y in Y_i by y^{α_i}. Then*

$$\pi(\alpha) = \prod \theta(\beta)^{\binom{\alpha}{\beta}},$$

where the product is taken over all $\beta = (\beta_1, \ldots, \beta_m)$ less than or equal to α; that is, $\beta_i \leqslant \alpha_i$ for all i, where $\binom{\alpha}{\beta}$ is the product $\prod \binom{\alpha_i}{\beta_i}$ and where $\theta(\beta)$ is a product of manifold commutators, each containing at least β_i components which are elements, or inverses of elements, of Y_i.

Proof of 1.5. We have seen in the proof of 1.3 that $\{G_{n,p^e}\}$ is contained in any such series $\{H_n\}$; so it suffices to show that $\{G_{n,p^e}\}$ is itself such a series. To show that it forms a Lazard series, it suffices to show

$$[G_i^{p^j}, G_m] \text{ is in } G_{n+m,p^e} \quad \text{if} \quad ip^j \geqslant np^{e-1} \tag{1}$$

and

$$[G_i^{p^j}, G_k^{p^l}] \text{ is in } G_{ip^j+kp^l,p} \tag{2}$$

The relevance of (2) is seen from the fact that $G_{np^f,p^{e-f}} \leqslant G_{n,p^e}$ for $0 \leqslant f \leqslant e$.

To prove these, we may assume that the subgroups on the right are trivial, and then establish that generators of the subgroups on the left commute. For (1), we apply Dark's Theorem to the word $\pi = [x, y]$ with x in G_i, y in G_m, and set $\alpha = (p^j, 1)$. For (2), again use $\pi = [x, y]$, x in G_i, y in G_k, and set $\alpha = (p^j, p^l)$. In both cases, $\pi(\alpha) = 1$ follows in a straightforward manner.

We include all the details of the proof of the remaining assertion, that p^{e+k}-th powers of elements of G_{n,p^e} lie in G_{np^{1+k},p^e}. A typical element of

G_{n,p^e} is of the form $x = \prod x_r^{c_r}$, $1 \leqslant r \leqslant t$, where x_r is in G_{i_r} and $c_r = p^{j_r}$ where, if $i_r < n$, $i_r p^{j_r} \geqslant np^{e-1}$.

We use the word $\pi = \prod y_{q,r}$, $1 \leqslant q \leqslant p^{e+k}$, $1 \leqslant r \leqslant t$, where each $y_{q,r}$ is in a distinct set; that is, $m = tp^{e+k}$. Set $y_{q,r} = x_r$ and define α by setting $\alpha_{q,r} = p^{j_r}$. Then $\pi(\alpha) = x^{p^{e+k}}$; so, by Dark's Theorem,

$$x^{p^{e+k}} = \prod \theta(\beta)^{\binom{\alpha}{\beta}}, \qquad 0 \leqslant \beta \leqslant \alpha,$$

where $\theta(\beta)$ is in G_u, $u = \sum i_r \beta_{q,r}$, summed over all q and r. Write $\beta_{q,r} = b_{q,r} p^{a_{q,r}}$, where p does not divide $b_{q,r}$, and let $v = \sum (j_r - a_{q,r})$, summed over all q and r.

We conclude the proof by showing that $\theta(\beta)^{\binom{\alpha}{\beta}}$ is in G_{np^{1+k},p^e} for all β; it suffices to show that $up^v \geqslant np^{e+k}$. If $\beta = 0$, $\theta(\beta) = 1$; if x is in G_n, $x^{p^{e+k}}$ is in G_{np^{1+k},p^e}; thus, we may assume that $\beta_{q,r}$ is not 0 for all q and r and that some $i_r < n$.

Case 1. $v < p^{e+k}$. Choose r so that $i_r < n$. Since $a_{q,r} = j_r$ for at least $p^{e+k} - v$ values of q, we have $u \geqslant i_r p^{j_r}(p^{e+k} - v)$; so $up^v \geqslant np^{e-1}p^{e+k}$.

Case 2. $v \geqslant p^{e+k}$. We may assume that there is an r for which $i_r < n$ and $\sum \beta_{q,r} > 0$ summed over all q. Choose q so that $d = j_r - a_{q,r}$ is minimal. If $d = 0$, $u \geqslant ip^{j_r} \geqslant np^{e-1}$. If $d > 0$, $v \geqslant dp^{e+k}$, so that $p^v \geqslant p^d p^{e+k}$. But $u \geqslant i_r p^{a_{q,r}}$ so that $up^v \geqslant i_r p^{j_r} p^{e+k} \geqslant np^{e-1}p^{e+k}$.

Since the two series $\{G_{n,p^e}\}$ and $\{i_n(e, G)\}$ share such important properties, one might hope that they coincided; Lazard [6, p. 141] asked whether this were the case. If G is a finite p-group of exponent p^e, $G_n = G_{n,p^e}$ so that, if they coincided, 1.1 would settle the dimension subgroup problem.

Moran [7], however, has given examples of p-groups in which the two series differ: Let G be the split extension of a cyclic group $\langle x \rangle$ of order p^{e+1} by a cyclic group $\langle y \rangle$ of order p^2, defined by $x^y = x^{1+p^{e-1}}$. Then, if $e > 1$, and $e > 2$ if $p = 2$, $G_{p+1,p^e} = 1$ while $i_{p+1}(e, G) \neq 1$.

For $e = p = 2$, we give the following example: Let H be a non-Abelian central extension of a cyclic group of order 4 by the product of two cyclic groups of order 4, in which $H' = Z(H)$ (for example, group 180 on the list of Hall and Senior [2]); then the central product G of H and a cyclic group of order 8 with the subgroup of order 4 amalgamated, satisfies

$$1 = G_{p+1,p^e} < i_{p+1}(e, G).$$

The principle behind these examples is the following:

LEMMA 1.7. *If $n \leqslant p$ and $x^{p^{e-1}}$ is in $i_n(\mathbf{Z}_{p^e}, G)$, then x^{p^e} is in $i_{n+p-1}(\mathbf{Z}_{p^e}, G)$.*

Proof. With $m = p^{e-1}$, $x^m - 1 = \binom{m}{i}(x-1)^i$; so, modulo $I^n = I^n(\mathbf{Z}_{p^e}, G)$,

$p^{e-1}(x-1)\gamma \equiv 0$ for some γ in $\mathbf{Z}_{p^e}G$ of augmentation equal to 1. But, modulo I^n, the subset $1 + I$ forms a group; so $p^{e-1}(x-1) \equiv 0$. Thus, $p^{e-1}(x-1)^p$ is in I^{n+p-1}, so that $x^{p^e} - 1$ is in I^{n+p-1}.

Although $i_n(\mathbf{Z}_{p^e}, G)$ can be strictly greater than G_{n,p^e} for a p-group G and for $n > p$, it is a result of Moran [7] that they coincide for $n \leqslant p$. His proof is as that of 3.15 of [12] but a proof may be given, via 1.9, which cites only the statement of 3.15:

THEOREM 1.8. *If $n \leqslant p$ and G is a p-group, $i_n(\mathbf{Z}_{p^e}, G) = G_{n,p^e}$.*

Proof. We may assume that $G_{n,p^e} = 1$, so that G has class less than n and exponent p^e. To show that $i_n(e, G) = 1$, it suffices to use 3.15, which shows that $i_n(Z, G) = G_n = 1$, in conjunction with the following lemma, a refinement of Lemma 1.1:

LEMMA 1.9. *If G has exponent p^e, $i_n(\mathbf{Z}, G) = i_n(\mathbf{Z}_{p^{e+r-1}}, G)$, where $n \leqslant 1 + r(p-1)$.*

Proof. Let $I = I(\mathbf{Z}, G)$ and $m = p^{e+r-1}$. As in proof of 1.1, it suffices to show that mI is in I^n. We induct on r that, in fact, mI is in $I^{1+r(p-1)}$; we assume $r \geqslant 1$. Since $\exp G = p^e$,

$$0 = x^m - 1 = \sum \binom{m}{i} (x-1)^i.$$

Collecting terms, we see that there are elements γ_i in I^{p^i}, $0 \leqslant i \leqslant r-1$, with γ_0 of augmentation equal to 1, for which $0 = \sum m/p^i(x-1)\gamma_i$ modulo $I^{1+r(p-1)}$, sum over $0 \leqslant i \leqslant r-1$. For $i > 0$, $m/p^i(x-1)$ is in $I^{1+(r-i)(p-1)}$ by induction on r so that $m/p^i(x-1)\gamma_i \equiv 0$. Thus, $m(x-1)\gamma_0 \equiv 0$; so $m(x-1) \equiv 0$ as in 1.7.

We remark that Passi [9] has shown that, for G cyclic of order p^e, the exponent of $I/I^{1+r(p-1)}$ is precisely p^{e+r-1}.

For $n \leqslant p$, the dimension subgroups have a further significance.

PROPOSITION 1.10. *If G is a p-group, $n \leqslant p$, $I = I(R, G)$, $i_n = i_n(R, G)$, then the exponent of G/i_n equals the exponent of I/I^n. Consequently, if $R = \mathbf{Z}$, the exponent of I/I^n equals the exponent of G/G_n.*

Proof. If G^{p^e} is in i_n for some e, the equivalence $x^{p^e} - 1 \equiv p^e(x-1)\gamma$ modulo I^n, γ of unit augmentation, shows that p^eI is in I^n. Conversely, since I/I^2 is isomorphic to $R \otimes G/G'$, there is some e for which p^eI is in I^n; the same equivalence shows that G^{p^e} is in i_n.

For arbitrary n, it is still a frequent occurrence that $i_n(e, G) = G_{n,p^e}$. The techniques of Section 2 of [12] provide enough examples in fact, to show

that every finite p-group is contained in a finite p-group for which the two series are identical.

PROPOSITION 1.11. *$i_2(e, G) = G_{2,p^e}$ for all G.*

Proof. There is an obvious map from $\mathbf{Z}_{p^e}G$ to $G/G'G^{p^e}$ which induces an isomorphism from I/I^2 to $G/G'G^{p^e} = \mathbf{Z}_{p^e} \otimes G/G'$, where $I = I(\mathbf{Z}_{p^e}, G)$. Thus, $i_2(e, G) = G'G^{p^e} = G_{2,p^e}$.

The proofs of 2.3 and 2.4 of [12], slightly modified, give the following results.

THEOREM 1.12. *If G is an abelian-by-cyclic group of exponent p^e, $i_n(e, G) = G_{n,p^e}$ for all n.*

THEOREM 1.13. *If G splits over a normal abelian subgroup A of exponent p^e, then $i_n(e, G) = i_n(e, T)[A, (n-1)G]$, where T is a complement to A. If $i_n(e, T) = T_{n,p^e}$, $i_n(e, G) = G_{n,p^e}$.*

We show next that the series coincide for abelian groups; the examples given show that this is not the case for class 2 groups.

PROPOSITION 1.14. *If G is Abelian, $i_n(\mathbf{Z}_{p^e}, G) = G_{n,p^e}$ for all n and e. Thus, $i_n(e, G) = G$ for $n = 1$, and $= G^{p^{e+j}}$ for $p^j < n \leqslant p^{j+1}$.*

Proof. We may assume that G is cyclic of order p^a where $p^a \geqslant np^{e-1}$. Let $I = I(\mathbf{Z}_{p^e}, G)$; inducting on m, we see that, for $0 \leqslant m \leqslant p^{a-e+1}$, I^m is $\mathbf{Z}_{p^e}$-free on all $(x-1)^i$, $m \leqslant i < p^a$, where x is a generator of G. Since we may assume $n > p^{a-e}$, we obtain a contradiction to the uniqueness of expression of elements in $I^{p^{a-e}}$ by assuming that x^q is in i_n, where $q = p^{a-1}$; that is, $x^q - 1 = \sum \binom{q}{i}(x-1)^i$ and p^e does not divide $\binom{q}{i}$ for $i = p^{a-e}$.

The above proof shows the utility of bases for RG other than the standard one consisting of the group elements. In characteristic p, there is a basis, subsets of which form bases for the powers of the augmentation ideal. In general, such is not the case; instead, we try to obtain useful sets of generators of I^n. The method we give dates at least to Jennings [4]; its importance to research on problems involving powers of the augmentation ideal is enormous.

Let G be a finite (nilpotent) group with a Lazard series $\{H_n\}$ which eventually reaches 1. This series filters G via the function w defined on G as $w(x)$ equals the largest n for which x is in H_n. We may choose elements x_i in G, $1 \leqslant i \leqslant d$, such that, if $w_i = w(x_i)$, the Abelian group H_w/H_{w+1} has basis consisting of the cosets of all the x_i for which $w_i = w$; we may assume that $w_i \leqslant w_{i+1}$. Define q_i to be the order of the coset of x_i in H_w/H_{w+1}, where $w = w_i$.

Let A be the set of all lists $\alpha = (\alpha_1, \ldots, \alpha_d)$ of nonnegative integers, and B the subset of all α for which $\alpha_i < q_i$. Then each element of G may be written uniquely as $x^\alpha = \prod x_i^{\alpha_i}$ for an α in B.

To use the set A, we need a large dose of notation. $w(\alpha) = \sum \alpha_i w_i$; $n(\alpha) = \sum \alpha_i$; $(-1)^\alpha = (-1)^{n(\alpha)}$; $s(\alpha) =$ smallest i for which $\alpha_i > 0$; $l(\alpha) =$ largest i for which $\alpha_i > 0$; $\beta \leqslant \alpha$ if $\beta_i \leqslant \alpha_i$ for all i; $(\alpha + \beta)_i = \alpha_i + \beta_i$; if $\beta \leqslant \alpha$, we can define subtraction by $(\alpha - \beta)_i = \alpha_i - \beta_i$; $\binom{\alpha}{\beta} = \prod \binom{\alpha_i}{\beta_i}$, product over all i; δ_i is defined by $(\delta_i)_j = \delta_{ij}$ the Kronecker symbol.

The following statements are obvious but useful:

(1) If α is in B and $\alpha_i > 0$, then $w_i \geqslant w(x^\alpha)$,

(2) If $i < j$ and $[x_j, x_i] = x^\alpha$, α in B, then $s(\alpha) > j$.

We apply the set A to the group ring RG by defining $P(\alpha)$ to be the product $\prod (x_i - 1)^{\alpha_i}$ over all i. Let A_n be the R-submodule of RG generated by all $P(\alpha)$, α in A, with $w(\alpha) \geqslant n$; let B_n be the corresponding module with α confined to B. We shall prove that $A_n A_m$ is in A_{n+m}, and that, under certain conditions, even $B_n B_m$ is in B_{n+m}. These assertions will provide manageable generators for $I^n(R, G)$.

Our first observation is an arithmetic identity valid in any ring, trivially proved by induction.

LEMMA 1.15. *Let y_i, $1 \leqslant i \leqslant n$, be elements of a ring with unit. Then $\prod y_i = \sum \prod (y_i - 1)$, where the sum is taken over all subsets of $\{1, \ldots, n\}$ and the product is over all elements of a given subset.*

This has the corollaries that

COROLLARY 1.16. $x^\alpha = \sum \binom{\alpha}{\beta} P(\beta)$; $P(\alpha) = \sum (-1)^{\alpha-\beta}\binom{\alpha}{\beta} x^\beta$; *thus, the set of $P(\alpha)$ for α in B forms an R-basis of RG.*

We now prove the main assertion

THEOREM 1.17. *$A_n A_m$ is contained in A_{n+m}.*

Proof. It suffices to show that $P(\alpha)\, P(\beta)$ is in $A_{w(\alpha)+w(\beta)}$. This we establish by inducting on $d - s(\beta)$, $n(\beta)$ and α in that order. We may assume that $\alpha > 0$ and that $i = s(\beta) < d$; in fact, by induction on $n(\beta)$, we may assume that $\beta = \delta_i$. Let $j = l(\alpha)$ so we may assume $i < j$.

Let $[x_j, x_i] = x = x^\gamma$, some $\gamma \in B$. Then $x - 1 = \sum \binom{\gamma}{\epsilon} P(\epsilon)$, sum over all ϵ, $0 < \epsilon \leqslant \gamma$, so that $w(\epsilon) \geqslant w_i + w_j$ by (1) and the fact that $\{H_n\}$ is a Lazard series, and $s(\epsilon) \geqslant s(\gamma) > i$ by (2).

$P(\alpha)P(\beta) = P(\alpha - \delta_j)(x_j - 1)(x_i - 1)$. We can interchange $(x_i - 1)$ and $(x_j - 1)$ by means of the standard five term identity:

$$(x_j - 1)(x_i - 1) = (x_i - 1)(x_j - 1) + (x_i - 1)(x - 1) + (x_j - 1)(x - 1) + (x_i - 1)(x_j - 1)(x - 1) + (x - 1).$$

We conclude by making the above substitution for $x - 1$ and using the induction hypothesis which asserts that $P(\alpha')P(\beta')$ is in $A_{w(\alpha')+w(\beta')}$ if either

$$s(\beta') > i, \tag{3}$$

or

$$s(\beta') = i \quad \text{and} \quad \alpha' < \alpha. \tag{4}$$

The full force of the Lazard series context is needed only to dispose of the term $P(\alpha - \delta_j)(x - 1)$.

As an example, we do one term, say $P(\alpha - \delta_j)(x_i - 1)(x - 1)$. It suffices to show that $P(\alpha - \delta_j)P(\delta_i + \epsilon)$ is in $A_{w(\alpha)+w(\beta)}$ for all ϵ, $0 < \epsilon \leqslant \gamma$. But $s(\delta_i + \epsilon) = i$ and $\alpha - \delta_j < \alpha$ so induction applies via (4), so that this term is in A_w,

$$w = w(\alpha - \delta_j) + w(\delta_i + \epsilon) \geqslant w(\alpha) - w_j + w_i + w(\epsilon) \geqslant w(\alpha) + 2w_i ;$$

but $w(\beta) = w_i$.

Since $A_0 = RG$, we see that A_n is an ideal of RG; since $A_1 = I(R, G)$ by 1.16, we see that I^n is contained in A_n, so that every element of I^n may be expressed as a sum of elements $P(\alpha)$, $w(\alpha) \geqslant n$. If H_n is contained in $i_n(R, G)$ for all n, A_n and I^n are equal for all n.

We shall make use of several refinements of 1.17 which we give without proof since the proofs are only elaborations of the above proof.

The first is relevant to the study of groups with a distinguished normal subgroup, which cannot readily be realized as a term in a Lazard series of an appropriate type; for example, an Abelian-by-cyclic group.

Let N be a normal subgroup of G and $\bar{G} = G/N$. Then $\{\bar{H}_n\}$ is a Lazard series in $\bar{G}$ and $\{H_n \cap N\}$ is a Lazard series in N; the filtration of the latter is just w restricted to N while, if $\bar{w}$ is the filtration of the former, there is an element x in each coset of N such that $w(x) = \bar{w}(\bar{x})$. We may choose elements x_i, $1 \leqslant i \leqslant d$, in G such that, in $\bar{G}$, the elements $\bar{x}_i$, $1 \leqslant i \leqslant d'$, form a set as above with $w_i = w(x_i) = w(\bar{x}_i)$ while, in N, the elements x_i, $d' < i \leqslant d$, form a set as above with $w_i = w(x_i)$.

Form the series K_n defined as H_nN if $n \leqslant k$, and as $N \cap H_{n-k+l}$ if $n \geqslant k$, where k is the smallest i for which H_i is in N and l is the largest i for which N is in H_i. Let v be the filtration associated with this series and let $v_i = v(x_i)$. Then K_v/K_{v+1} has basis consisting of the cosets of all the x_i for which $v_i = v$; define q_i as the order of the coset of x_i in K_v/K_{v+1}.

With these x_i, w_i and q_i, all the previous assertions go through, including (1) and (2), except that w_i is not necessarily $\leqslant w_{i+1}$ if $i = d'$. We conclude

THEOREM 1.18. *Let A_n be the R-module generated by all $P(\alpha)$, $w(\alpha) \geqslant n$, defined via x_i and w_i. Then $A_nA_m \leqslant A_{n+m}$.*

The next refinement, and its corollary, are intuitively clear but complicated to prove.

LEMMA 1.19. *With notation as that in* 1.17, *$P(\alpha)P(\beta)$ may be expressed as a sum $\sum r_\gamma P(\gamma)$, where r_γ is in R and $w(\gamma) \geqslant w(\alpha) + w(\beta)$ and where $r_\gamma = 0$ if there is an $i < s(\alpha)$ for which $\gamma_i > \beta_i$.*

COROLLARY 1.20. *If $\alpha_i < q_i$ for all i such that $w_i < w$, then $P(\alpha)$ may be expressed as a sum $\sum r_\gamma P(\gamma)$ where r_γ is in R and γ is in B and where $r_\gamma = 0$ if there is an i such that $w_i \leqslant w$ and $\gamma_i > \alpha_i$.*

The proof of the Corollary 1.20 proceeds by induction on such α, under dictionary ordering. The only new problem involved is that of reducing terms involving $(x_i - 1)^{a_i}$; this is tackled by expressing $x_i^{q_i} - 1$ as a sum of elements of B, just as with $[x_j, x_i] - 1$ in the proof of 1.17, and by appeal to the induction hypothesis, as in 1.17. This same problem arises in the last refinement we give, in which it is similarly dealt with, under a stronger induction hypothesis.

THEOREM 1.21. *Let R have characteristic p and assume the notation is as in* 1.17. *If there are x_i such that $w(x_i^{q_i}) \geqslant q_i w_i$, then B_nB_m is contained in B_{n+m}.*

This has the important corollary, due to Jennings (4), that

THEOREM 1.22. *If R has characteristic p and $H_n \leqslant i_n(R, G)$, then the set of $P(\alpha)$, α in B, with $w(\alpha) \geqslant n$, forms a basis for $I^n(R, G)$.*

The next corollary is due to Lazard (6) for $R = \mathbf{Z}_p$.

THEOREM 1.23. *Let R have characteristic p. Then $i_n(R, G) = G_{n,p}$ for all groups G.*

Proof. We may assume that G is a finite p-group. If G is a minimal counterexample, we may assume that $i_n(R, G) = G_{n,p}$ for $n < c$ and that $i_c > G_{c,p} = 1$. Choose x_i and w_i for the series $\{i_n\}$; these same x_i are also a suitable selection for the series $\{G_{n,p}\}$ with associated filtration w'. But $w_i = w_i'$ unless $w_i \geqslant c$, when $w_i > w_i'$. Let $m = 1 + (p - 1)\sum w_i'$.

By 1.22 for $\{G_{n,p}\}$, $I^m = 0$ but, by 1.22 for $\{i_n\}$, I^m contains $P(\alpha)$, where $\alpha_i = p - 1$ for all i. Since $P(\alpha)$ is not 0, this is a contradiction.

A proof of 1.23 may be read into Quillen's paper [10] by reference to 1.5 for $e = 1$.

The last part of this section is devoted to the calculation of $i_3(\mathbf{Z}_{p^e}, G)$ (note that 1.8 already shows this to be G_{3,p^e} for $p > 2$). For clarity, we present first a new proof that $i_3(\mathbf{Z}, G) = G_3$.

THEOREM 1.24. *Let G be a finite group. Then $i_3(\mathbf{Z}, G) = G_3$ and the embedding of G'/G_3 in I^2/I^3 splits, $I = I(\mathbf{Z}, G)$.*

Proof. It suffices to find an homomorphism from I^2/I^3 to G'/G_3 which sends the coset of $x - 1$ to the coset of x, for x in G'. For this, we may assume that $G_3 = 1$.

Choose x_i, w_i and q_i with respect to the series $\{G_n\}$ in G. The isomorphism of I/I^2 with G/G' shows that the set of all $P(\alpha)$, α in B and $w(\alpha) \geqslant 2$, together with all $q_i(x_i - 1)$, $w_i = 1$, is a basis for I^2. Thus, we may define a map from I^2 to the Abelian group G' by defining it on this basis. Define such a map by sending everything to 1 except $x_i - 1$, $w_i = 2$, which is sent to x_i, and $q_i(x_i - 1)$, $w_i = 1$, to $x_i^{q_i}$.

It suffices to show that I^3 is in the kernel K of this map since, if x is in G', $x = \prod x_i^{n_i}$, product over all i with $w_i = 2$, then

$$x - 1 \equiv \sum n_i(x_i - 1) \text{ modulo } I^3$$

so that $x - 1$ would be sent to $\prod x_i^{n_i} = x$.

I^3 is generated as Abelian group by all products of basis elements of I^2 with elements $x_i - 1$, $w_i = 1$. We show that each such product is in K.

Case 1. *$I(G)I(G')$ is in K.* Since $G' \leqslant Z(G)$, it suffices to show that $P(\alpha)$ is in K for all α in A with $w(\alpha) \geqslant 3$ and $\alpha_i < q_i$ except possibly $\alpha_j = q_j$ for some single j, $w_j = 2$. We need deal only with this exceptional case. But $0 = x_j^{q_j} - \sum \binom{q_j}{i}(x_j - 1)^i$; substituting this expression for $(x_j - 1)^{q_j}$, we see that $P(\alpha)$ is a sum of elements $P(\beta)$, β in B, all of which are in K, with one possible exception: if $P(\alpha) = (x_j - 1)^{q_j}$, $P(\alpha) \equiv q_j(x_j - 1)$ modulo K, but $q_j(x_j - 1)$ goes to $x_j^{q_j} = 1$.

This case eliminates all products $P(\alpha)(x_i - 1)$ where $w_{l(\alpha)} = 2$.

Case 2. *$P(\alpha)(x_i - 1)$ is in K if $w_{l(\alpha)} = 1$, $w(\alpha) \geqslant 2$.* We may assume that $\alpha_i = q_i - 1$ because, modulo $I(G)I(G')$, $P(\alpha)(x_i - 1) \equiv P(\alpha + \delta_i)$, and $\alpha + \delta_i$ is in B otherwise. Again substituting the expression for $(x_i - 1)^{q_i}$, we see that we are done, since $x_i^{q_i}$ is in G', unless $P(\alpha)$ is $(x_i - 1)^{q_i - 1}$, in which case $P(\alpha)(x_i - 1) = (x_i - 1)^{q_i}$ which is equivalent to $(x_i^{q_i} - 1) - q_i(x_i - 1)$ modulo K but $x_i^{q_i} - 1$ goes to $x_i^{q_i}$ and $-q_i(x_i - 1)$ goes to $x_i^{-q_i}$.

Case 3. $q_j(x_j - 1)(x_i - 1)$ *is in* K. We may assume $j > i$, the case $i = j$, $q_j = 2$ being covered by the technique used at the end of Case 2. But, modulo $I(G)I(G')$, $q_j(x_j - 1)(x_i - 1) \equiv q_j([x_j, x_i] - 1)$ modulo K, which goes to $[x_j, x_i]^{q_j} = [x_j^{q_j}, x_i] = 1$.

We have thus constructed an isomorphism of $I(G')\mathbf{Z}G + I^3/I^3$ with G'/G_3 and so an isomorphism of I^2/I^3 with $G'/G_3 \oplus K/I^3$. Since $I^3 \leqslant K \leqslant I^2$, K is an ideal and so G/G_3 is isomorphic to the group of units $1 + I/K$, which solves the integral group ring problem for class 2 groups. It is not difficult to find a basis for K, but it does not seem feasible to construct a map K/I^4 to G_3/G_4, etc., thereby solving both the dimension subgroup problem and the integral group ring problem simultaneously.

THEOREM 1.25. *For* G *arbitrary,* $i_3(\mathbf{Z}_{p^e}, G)$ *is* G_{3,p^e} *if* $p > 2$; *if* $p = 2$, *it is the subgroup generated by* G_{3,p^e} *and all* x^{p^e} *for which* $x^{p^{e-1}}$ *is in* $G_{2,p^e} = G'G^{p^e}$.

Proof. By 1.3 and 1.7, the subgroup on the right is contained in $i_3(e, G)$ so we may assume that the subgroup on the right is trivial. By standard reduction arguments, we may assume that G is a finite p-group.

Choose x_i, w_i and q_i with respect to the series $\{G_{n,p^e}\}$ in G. The isomorphism of I/I^2 with $G/G_{2,p^e}$ shows that the set of all $P(\alpha)$, α in B and $w(\alpha) \geqslant 2$, together with all $q_i(x_i - 1)$, $w_i = 1$, is a basis for I^2, $I = I(\mathbf{Z}_{p^e}, G)$.

For $p > 2$, define a map from I^2 to G_{2,p^e} by sending everything to 1 except $x_i - 1$ to x_i, when $w_i = 2$, and $q_i(x_i - 1)$ to $x_i^{q_i}$, when $w_i = 1$ and $q_i < p^e$. This is readily seen to define a map of Abelian groups and the proof concludes just as in 1.24.

For $p = 2$, define a map, as above, on all the basis elements of I^2 except that, if $q_i = 2^e$ and $w_i = 1$, we define the map only on $2^{e-1}(x_i - 1)^2$ which is sent to $x_i^{2^e}$. We again conclude as in 1.24, the only change being that, if $q_i = 2^e$,

$$(x_i - 1)^{2^e} \equiv (x_i^{2^e} - 1) - \binom{2^e}{2}(x_i - 1)^2 \equiv (x_i^{2^e} - 1) + 2^{e-1}(x_i - 1)^2$$

which goes to $x_i^{2^e}x_i^{2^e} = 1$ since $G^{2^{e+1}} = 1$.

2. ARBITRARY COEFFICIENTS

The dimension subgroups $i_n(R, G)$ can be calculated in terms of the subgroups $i_n(\mathbf{Z}_{p^e}, G)$. If r, the characteristic of R, is 0, this can be done only if we assume that the dimension subgroup conjecture is valid, that is, $i_n(\mathbf{Z}, G) = G_n$. Conversely, the expression given will imply the conjecture by a suitable choice of R and G. The main result of this section is

THEOREM 2.1. *If r is not 0, then $i_n(R, G) = i_n(\mathbf{Z}_r, G)$; furthermore, if r_p is the largest power of p dividing r, then $i_n(\mathbf{Z}_r, G)$ is the intersection of all $i_n(\mathbf{Z}_{r_p}, G)$.*

If r equals 0, then under the assumption that $i_n(\mathbf{Z}, G) = G_n$, $i_n(R, G)$ is the product of all

$$i_n(\mathbf{Z}_{e(p)}, G) \cap T_p(G \bmod G_n),$$

taken over the set $\sigma(R)$ of primes p for which $p^e R = p^{e+1}R$ for some e, and $e(p) = e_R(p)$ is the smallest p^e for which this is so; if N is normal in G, $T_p(G \bmod N)$ is the p-torsion subgroup of $G \bmod N$, that is, the subgroup of G generated by all elements of G, some p-th power of which is in N.

We examine first the behaviour of $i_n(R, G)$ as a functor of R. Any ring homomorphism R to S induces an inclusion $i_n(R, G) \leqslant i_n(S, G)$. Under direct or tensor products, the behaviour is more erratic but we can make the following observation which proves the second assertion of 2.1 in the case that r is not 0.

LEMMA 2.2. *Let R_i be rings, i ranging over a finite index set. Then $I^n(\prod R_i, G)$ is the sum of all $I^n(R_i, G)$; $i_n(\prod R_i, G)$ is the intersection of all $i_n(R_i, G)$.*

Proof. Let $R = \prod R_i$. The first part is clear as is the assertion that the intersection of $i_n(R_i, G)$ is in $i_n(R, G)$ since: if $x - 1$ is in $I^n(R_i, G)$ for all i, $1_i(x - 1)$ is in $I^n(R, G)$, 1_i the unit of R_i. But 1, the unit of R, is the sum of all 1_i.

The opposite inclusion follows from the existence of the projections R to R_i, which are ring homomorphisms.

For direct products over an infinite index set, this lemma is generally false although it still holds for G finite. Similarly, $i_n(R \otimes S, G) = i_n(R, G)\, i_n(S, G)$ for G finite but not more generally, although this is true if both R and S have nonzero characteristic.

The following is not difficult; a clever category theoretic proof is given in Quillen [10].

LEMMA 2.3. *Let S be a subring of R. The usual isomorphism of RG with $SG \otimes_S R$ induces an isomorphism of*

$$RG/I^n(R, G) \qquad \text{with} \qquad (SG/I^n(S, G)) \otimes_S R$$

which is natural in G.

From this we can conclude that $i_n(R, G)$ equals $i_n(S, G)$, whenever we can establish assertions like: if M is a right S-module and $m \otimes 1 = 0$ in $M \otimes_S R$, then $m = 0$. Such arguments give the following results.

COROLLARY 2.4. *If r is not* 0, $i_n(R, G) = i_n(\mathbf{Z}_r, G)$.

COROLLARY 2.5. *If* $\mathbf{Q}$ *is in* R, $i_n(R, G) = i_n(\mathbf{Q}, G)$.

COROLLARY 2.6. *If R is the ring of algebraic integers of an algebraic number field, then* $i_n(R, G) = i_n(\mathbf{Z}, G)$.

This completes the proof of 2.1 for $r \neq 0$. For $r = 0$, the proof proceeds through several steps involving conditions on $\sigma(R)$. Let $\pi(R)$ be the subset of $\sigma(R)$ consisting of all p with $e(p) = 1$, that is, all p for which p^{-1} is in R.

Case 1. *All primes are in* $\pi(R)$. In this case, $\mathbf{Q}$ is in R; so, by 2.5, it suffices to calculate $i_n(\mathbf{Q}, G)$. Since $\mathbf{Z}_1$ is the zero ring, $i_n(\mathbf{Z}_1, G) = G$, so that 2.1 asserts that $i_n(\mathbf{Q}, G)$ is $T(G \bmod G_n)$, the torsion subgroup of $G \bmod G_n$. But this is a result of Jennings and Hall [5, 3] whose proof, as given in [3, p. 51], uses the technique of 1.17.

Let π be a set of primes and $T_\pi(G \bmod N)$ the π-torsion subgroup of $G \bmod N$.

LEMMA 2.7. *Let* $\mathbf{Z}(\pi^{-1})$ *be the subring of* $\mathbf{Q}$ *generated by all* p^{-1} *with* p *in* π. *Then* $i_n(\mathbf{Z}(\pi^{-1}), G) = T_\pi(G \bmod i_n(\mathbf{Z}, G))$.

Proof. Let $R = \mathbf{Z}(\pi^{-1})$. If x is in $i_n(R, G)$, there is a π-number q for which $q(x - 1)$ is in $I^n(\mathbf{Z}, G)$ and so $x^{q^n} - 1$ is in $I^n(\mathbf{Z}, G)$.

For the opposite inclusion, it suffices to show that, if p is in π and x^p is in $i_n(R, G)$, x is in $i_n(R, G)$. Choose m maximal such that x is in $i_m(R, G)$. If $m < n$, $x^p - 1 = \sum \binom{p}{i}(x - 1)^i$ is in I^{m+1}, $I = I(R, G)$, so $p(x - 1)$ is in I^{m+1}. But p^{-1} is in R; so $x - 1$ is in I^{m+1} which is a contradiction.

This lemma shows that the assertion that $i_n(\mathbf{Q}, G)$ equals $T(G \bmod G_n)$ is equivalent to the assertion that $i_n(\mathbf{Z}, G)/G_n$ is periodic. Hall's proof applies equally well to either formulation. We state the second form separately as a measure of the extent to which the dimension subgroup conjecture could fail.

THEOREM 2.8. $i_n(\mathbf{Z}, G)/G_n$ *is periodic.*

Case 2. $\sigma(R) = \pi(R)$. In this case, 2.1 asserts that

$$i_n(R, G) = T_\pi(G \bmod G_n),$$

where $\pi = \pi(R)$. We may assume by case 1 that π', the set of primes not in π, is nonempty. It is in this case that we must assume that $i_n(\mathbf{Z}, G) = G_n$.

The proof of 2.7 shows that $T_\pi(G \bmod G_n)$ is in $i_n(R, G)$; thus, we may assume that $T_\pi(G \bmod G_n) = 1$. (If $i_n(\mathbf{Z}, G) \neq G_n$, we could not assume $T_\pi(G \bmod i_n(\mathbf{Z}, G)) = 1$). Furthermore, we may assume that G is finitely generated.

The result is obvious for finite p-groups, p in π', so that the following result concludes this case.

LEMMA 2.9. *A finitely generated, nilpotent π-torsion free group G is residually a finite π'-group, that is, the intersection of all normal subgroups N of index a power of some prime p in π' is trivial.*

This result may be proved in the same manner as a theorem of Gruenberg which asserts that: A finitely generated, nilpotent torsion free group is residually a finite p-group, for any fixed prime p [8, p. 80].

This case is equivalent to the dimension subgroup conjecture, for: Let G be a minimal counterexample to the conjecture so that G is a finite p-group; let $R = \mathbf{Z}(q^{-1})$, where q is a prime different from p. Then this case shows $i_n(R, G) = G_n$ but $i_n(R, G) \geqslant i_n(\mathbf{Z}, G) \geqslant G_n$.

The remaining cases mainly involve only arithmetic in the ring R. Let $\tau(R)$ be the set of integers t for which $tR = t^2R$; thus, $\sigma(R)$ is in $\tau(R)$. We need several simple observations about this set.

LEMMA 2.10. *If t is in $\tau(R)$ and J is the annihilator of t in R, R is the direct sum of tR and J. Thus, as rings, R is the direct product of R/tR and R/J.*

Proof. Let $t = t^2\alpha$. Then $1 = t\alpha + (1 - t\alpha)$ and $1 - t\alpha$ is in J.

LEMMA 2.11. *Let t be in $\tau(R)$. If p is a prime dividing t, then p is in $\sigma(R)$ and $e(p)$ divides t. Thus, $tR = sR$, where s is the product of all $e(p)$ for which p divides t.*

If σ and τ are finite subsets of $\sigma(R) - \pi(R)$, and s and t are the products of all $e(p)$ for p in σ and τ, respectively, then

$$\sigma = \tau \quad \text{if and only if} \quad sR = tR.$$

Proof. The first paragraph is established by straightforward calculations. For the second, if $sR = tR$, we may assume that σ is contained in τ since, if p is in σ, $sR = e(p)sR = e(p)tR$. Thus, $t = su$, where s and u are relatively prime so that there are integers a and b for which $as + bu = 1$; but there is α in R for which $s = su\alpha$ whence $1 = (as\alpha + b)u$. If p is in τ and not in σ, p divides the unit u, so that p is in $\pi(R)$, which is a contradiction.

Case 3. $\sigma(R) - \pi(R)$ *is finite.* Let s be the product of all $e(p)$, p in $\sigma(R)$ but not in $\pi(R)$. Then, in this case, 2.1 asserts that $i_n(R, G)$ is the intersection of $i_n(\mathbf{Z}_s, G)$ and $T_{\sigma(R)}(G \bmod G_n)$ because of the following.

It is clear that $i_n(\mathbf{Z}_s, G)$ is the intersection of all $i_n(\mathbf{Z}_{e(p)}, G)$, p in $\sigma(R)$; also, $T_{\sigma(R)}(G \bmod G_n)$ is the product of all $T_p(G \bmod G_n)$, p in $\sigma(R)$. But $T_p(G \bmod G_n)$ is in $i_n(\mathbf{Z}_{e(q)}, G)$, whenever p and q are unequal; so the following lemma suffices.

LEMMA 2.12. *Let A_i and B_i be normal subgroups of G, i ranging over an arbitrary set of indices. If B_i is in A_j whenever i and j are unequal, then*

$$\bigcap A_i \cap \prod B_i = \prod (A_i \cap B_i).$$

Proof. It suffices to prove the case of a finite index set but this may be done by induction.

Using 2.10, we see that $i_n(R, G)$ is the intersection of $i_n(R/sR, G)$ and $i_n(R/J, G)$. We conclude, by showing that R/sR has characteristic s, by appealing to 2.4, by showing that R/J has characteristic 0 and

$$\sigma(R/J) = \pi(R/J) = \sigma(R),$$

and by appealing to Case 2.

If t is the characteristic of R/sR, t divides s because $s(R/sR) = 0$; so sR is in tR; but, by definition, tR is in sR so $tR = sR$. Thus, t is in $\tau(R)$. By the first part of 2.11, s divides t.

If an integer u is in J, $su = 0$ in R; since R has characteristic 0, $u = 0$ and R/J has characteristic 0. If $p^e(R/J) = p^{e+1}(R/J)$, then sp^e is in $\tau(R)$; so 2.11 shows p to be in $\sigma(R)$; thus, $\sigma(R/J)$ is in $\sigma(R)$. But the proof of 2.10 shows that s is a unit in R/J, so that $\sigma(R)$ is in $\pi(R/J)$.

Case 4. $\sigma(R)$ *is arbitrary.* $i_n(R, G)$ is the union of all $i_n(S, G)$, over all finitely generated subrings S of R. But, if p is in $\sigma(S)$, p is in $\sigma(R)$ and $e_R(p)$ divides $e_S(p)$ so that $i_n(\mathbf{Z}_{e_S(p)}, G)$ is in $i_n(\mathbf{Z}_{e_R(p)}, G)$. Hence, it suffices to assume that R is finitely generated. But this reduces to Case 3 by the following lemma.

LEMMA 2.13. *If $\sigma(R) - \pi(R)$ is infinite, R is not finitely generated.*

Proof. Enumerate the primes in $\sigma(R) - \pi(R)$ and let t_m be the product of $e(p_i)$, $1 \leqslant i \leqslant m$, and let J_m be the annihilator of t_m. By the second part of 2.11, $t_m R \neq t_{m+1} R$ so that, by 2.10, J_{m+1} is strictly larger than J_m. Hence, R is not Noetherian.

REFERENCES

1. R. DARK, "On Nilpotent Products of Groups of Prime Order," Thesis, Cambridge University, Cambridge, 1968.
2. M. HALL AND J. K. SENIOR, "The Groups of Order $2^n (n \leqslant 6)$," Macmillan, New York, 1964.
3. P. HALL, "Nilpotent Groups," Canad. Math. Congress, Univ. of Alberta, 1957; Queen Mary College Math. Notes, London, 1970.
4. 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.

5. S. A. JENNINGS, The group ring of a class of infinite nilpotent groups, *Canad. J. Math.* **7** (1955), 169–187.
6. M. LAZARD, Sur les groupes nilpotents et les anneaux de Lie, *Ann. École Norm. Sup.* **71** (1954), 101–190.
7. S. MORAN, Dimension subgroups modulo n, *Proc. Camb. Phil. Soc.* **68** (1970), 579–582.
8. H. NEUMANN, "Varieties of Groups," Springer, Berlin, 1968.
9. I. B. S. PASSI, Polynomial maps on groups, *J. Algebra* **9** (1968), 121–151.
10. D. G. QUILLEN, On the associated graded ring of a group ring, *J. Algebra* **10** (1968), 411–418.
11. R. SANDLING, "The Modular Group Rings of p-Groups," Thesis, University of Chicago, Chicago, Ill., 1969.
12. R. SANDLING, The dimension subgroup problem *J. Algebra* **21** (1972), 216–231.
13. H. ZASSENHAUS, Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen, *Abh. math. Sem. Hamburg* **13** (1940), 200–207.