ISRAEL JOURNAL OF MATHEMATICS, Vol. 73, No. 1, 1991

# APPLICATIONS OF DIMENSION SUBGROUPS TO THE POWER STRUCTURE OF $p$-GROUPS

BY

CARLO M. SCOPPOLA[a,†] AND ANER SHALEV[b,‡]

[a]*Dipartimento di Matematica, Universita degli Studi di Trento, 38050 Povo (Trento), Italy; and* [b]*Mathematical Institute, University of Oxford, 24-29 St. Giles, Oxford OX1 3LB, U.K.*

ABSTRACT

Dimension subgroups in characteristic $p$ are employed in the study of the power structure of finite $p$-groups. We show, e.g., that if $G$ is a $p$-group of class $c$ ($p$ odd) and $k = \lceil \log_p((c+1)/(p-1)) \rceil$, then, for all $i$, any product of $p^{i+k}$th powers in $G$ is a $p^i$th power. This sharpens a previous result of A. Mann. Examples are constructed in order to show that our constant $k$ is quite often the best possible, and in any case cannot be reduced by more than 1.

## 1. Introduction

Dimension subgroups over fields of characteristic $p$, introduced by R. Brauer, H. Zassenhaus and S. A. Jennings in the late thirties, were used by the last in the study of the Loewy-structure of modular $p$-group algebras $KG$ (also referred to as local group algebras) [J]. An explicit expression for the dimension subgroup $D_m = G \cap (1 + \Delta^m)$ (where $\Delta$ denotes the augmentation ideal) was subsequently derived by Lazard [L]. Passi and Sehgal [PS2] studied the Lie dimension subgroups $D_{(m)} = G \cap (1 + \Delta^{(m)})$, where $\_^{(m)}$ denotes Lie-powers. They were able to give a group-theoretic description somewhat analogous to that of Lazard. Since then, dimension subgroups have proved useful in various interesting and seemingly unrelated contexts: the isomorphism problem for local group algebras (e.g., Passi and Sehgal, 1972 [PS1]; Röhl, 1989 [R]), the class of nilpotent wreath products (Shield, 1977 [Shi]), unipotent representations of nilpotent groups (Wehrfritz, 1987 [W]), Frobenius-Wielandt complements (Scoppola [Sc]), numbers of generators of ideals

†Partially supported by MPI funds. This author is a member of GNSAGA-CNR.
‡Partially supported by a Rothschild Fellowship.
Received July 12, 1990

in local group algebras (Shalev [Sh1]), the Lie-structure of local group algebras and the structure of their unit groups (Shalev [Sh2]). The applicability of dimension subgroups to the study of transitive permutation modules for $p$-groups has recently been pointed out by Alperin [A]. Another context in which dimension subgroups (and the restricted Lie algebras they give rise to) play some role is the restricted Burnside problem, recently solved by Zelmanov.

Although dimension subgroups were primarily considered as a tool in the study of some ring-theoretic aspects of group algebras, it is now clear that they have some pure group-theoretic applications as well. In this paper we describe some of their applications to the power structure of $p$-groups. In fact, for some purposes we find it convenient to use a certain double-indexed series $\{D_{m,k}\}$, introduced in [Sh1], which includes ordinary dimension subgroups and Lie dimension subgroups as particular cases. For a general background on the power structure of $p$-groups, the reader is referred to [Hu, Chap. III], [M1], [M2].

In order to describe our main results we need some notation.

Throughout this paper, $G$ denotes a finite $p$-group, and $\{\gamma_j\}_{j\geq 1}$ stands for its lower central series. For $i \geq 0$ let $\mathfrak{U}_i = \langle x^{p^i} : x \in G\rangle$ – the subgroup generated by the $p^i$th powers. Define $\mathfrak{U}_{(i)}$ $(i \geq 0)$ inductively, by $\mathfrak{U}_{(0)} = G$, $\mathfrak{U}_{(i)} = \mathfrak{U}_1(\mathfrak{U}_{(i-1)})$ $(i \geq 1)$. Obviously,

$$\mathfrak{U}_{(i)} \supseteq \mathfrak{U}_i \supseteq \{x^{p^i} : x \in G\} \quad \text{(the set of } p^i\text{th powers)}$$

and both inclusions may be proper.

It is well known that, for a regular $p$-group, these three notions coincide ([Ha]; see also [Hu, Chap. III, Sec. 10]). A similar phenomenon holds for powerful $p$-groups, as shown by Lubotzky and Mann in [LM]. In fact, it follows from [Ar, Theorem 2 & Corollary 2.1] that this remains true under the weaker condition $\gamma_a \leq \mathfrak{U}_1$ for some $a < p$. The following theorem generalizes this phenomenon.

THEOREM A. *Let $m = ap^{\alpha-1}$, where $a < p$ and $\alpha \geq 1$. Suppose $G$ is a $p$-group satisfying $D_m = D_{m+1}$. Then $\mathfrak{U}_{(i)} = \mathfrak{U}_i = \{x^{p^i} : x \in G\}$ for all $i \geq \alpha$.*

Note that, since $D_a = \gamma_a \cdot \mathfrak{U}_1$ for $a < p$, Arganbright's result is obtained from our theorem by substituting $\alpha = 1$.

COROLLARY A1 [Sh1, Theorem 2.2]. *Any group $G$ of order $p^n$ satisfies $\mathfrak{U}_{(i)} = \mathfrak{U}_i = \{x^{p^i} : x \in G\}$ for any integer $i \geq (n-1)/(p-1)$.*

Indeed, by a simple counting argument, we must have $D_m = D_{m+1}$ for some $m = ap^{\alpha-1}$, where $1 \leq a < p$ and $\alpha \leq \lceil (n-1)/(p-1) \rceil$.

In the following theorem, referring to problem 4 in [M1], the nilpotency class

of $G$ is taken into account. According to a result of A. Mann quoted in [M1, Sec. 1], if $G$ is of class $c$ and $k = [(c-1)/(p-1)]$, then any product of $p^{i+k}$th powers is a $p^i$th power, i.e. $\mathfrak{U}_{i+k} \subseteq \{x^{p^i} : x \in G\}$. Here we improve this by reducing $k$ to $\lceil \log_p((c+1)/(p-1)) \rceil$, and replacing $\mathfrak{U}_{i+k}$ by $\mathfrak{U}_{(i+k)}$.

However, we assume that $p$ is odd.

THEOREM B. *Let $G$ be a $p$-group of class $c$ ($p$ odd), and let $k$ be the minimal integer such that $c < (p-1)p^k$.*

*Then $\mathfrak{U}_{(i+k)} \subseteq \{x^{p^i} : x \in G\}$ for all $i > 0$.*

Finally, we claim that our constant $k$ is the best possible for most values of $c$, and in any case cannot be reduced by more than 1. The proof is based on the detailed description of the factors $D_m(F)/D_{m+1}(F)$, where $F$ is a (finitely generated) free group, given in [Sc].

THEOREM C. *For every positive integer $k$ there exists a $p$-group $G$ of class $c = p^{k+1}$, in which $\mathfrak{U}_{1+k} \not\subseteq \{x^p : x \in G\}$; in fact, if $F$ is the free group on two generators, then $G = F/D_{p^{k+1}+1}(F)$ would be as required.*

Some words on the structure of this paper:

In section 2 we discuss dimension subgroups, and set up the machinery required in the proofs of Theorems A and B; these results are then derived in section 3, while section 4 is devoted to the proof of Theorem C.

Let us now introduce some additional notations. Group commutators are denoted by [ , ], and long commutators are interpreted using the left-normed convention. We define $[x,y;n]$ inductively by $[x,y;0] = x$, $[x,y;n+1] = [[x,y;n],y]$ ($n \geq 0$). An $N_p$-series in a group $G$ is a descending series of normal subgroups $\{H_m\}_{m \geq 1}$, satisfying $[H_m, H_n] \leq H_{m+n}$ and $\mathfrak{U}_1(H_m) \leq H_{pm}$ for all $m, n$. It is well known (see, e.g., [P, Chap. 3]) that $\{D_m\}$ is an $N_p$-series. For a real number $x$, denote by $[x]$ ($\lceil x \rceil$) the maximal (minimal) integer which is not greater (smaller) than $x$.

## 2. Dimension subgroups; the series $\{D_{m,k}\}$

The detailed study of dimension subgroups in characteristic $p$ seems to require the definition of a somewhat more general notion (see [Sh1,Sh2]).

DEFINITION 2.1. For integers $m \geq 1$ and $k \geq 0$ put

$$D_{m,k} = \prod_{jp^i \geq m} \mathfrak{U}_i(\gamma_{j+k}).$$

Define non-negative integers $d_{m,k}$ by

$$p^{d_{m,k}} = (D_{m,k} : D_{m+1,k}).$$

Lazard's formula for the dimension subgroups $D_m$ is obtained by substituting $k = 0$ in the definition of $D_{m,k}$, i.e. $D_m = D_{m,0}$ $(m \geq 1)$, whereas Passi and Sehgal's expression for the Lie dimension subgroup may be formulated by $D_{(m+1)} = D_{m,1}$ $(m \geq 1)$. It is straightforward to verify (e.g., using [P1, Corollary 1.18, p. 42]) that, fixing $k$, $\{D_{m,k}\}_{(m \geq 1)}$ is an $N_p$-series. Moreover, this sequence can be shown to be the minimal $N_p$-series starting with $\gamma_{k+1}$, which is central in $G$.

The following technical notation will be needed in the sequel.

DEFINITION 2.2. (1) For integers $m \geq 1$ and $k, v \geq 0$ put

$$D_{m,k}^{\leq v} = \prod_{\substack{i \leq v \\ jp^i \geq m}} U_i(\gamma_{j+k}); \qquad D_{m,k}^{>v} = \prod_{\substack{i > v \\ jp^i \geq m}} U_i(\gamma_{j+k}).$$

(2) For a prime $p$ and a positive integer $m$, denote by $v_p(m)$ the maximal integer $v$ such that $p^v$ divides $m$; let $(m)_{p'}$ be the maximal divisor of $m$ which is prime to $p$, i.e. $(m)_{p'} = m/p^v$ where $v = v_p(m)$.

The following theorems summarize the basic properties of the series $D_{m,k}$.

THEOREM 2.3. (1) $D_{m,k+1} = [G, D_{m,k}]$ [Sh1, Proposition 1.2].
(2) $d_{m,k} = 0$ *implies* $d_{m,h} = 0$ *for every* $h > k$.

Note that part (2) follows immediately from (1). Indeed,

$$d_{m,k} = 0 \Rightarrow D_{m,k} = D_{m+1,k} \Rightarrow [G, D_{m,k}] = [G, D_{m+1,k}]$$

$$\Rightarrow D_{m,k+1} = D_{m+1,k+1} \Rightarrow d_{m,k+1} = 0,$$

which yields (2) by induction.

Let us now fix $k \geq 0$, and study the series $\{D_{m,k}\}_{m \geq 1}$ and the associated series $\{d_{m,k}\}_{m \geq 1}$.

As indicated in [Sh2], these series are subject to various constraints, similar to those derived in [Sh1, Sec. 1] for $k = 0$, and in [Sh2, Sec. 4] for $k = 1$. Some related results for the case $k = 0$ were obtained independently by Leedham-Green and Staszewski in [LS].

THEOREM 2.4. *Suppose* $\exp(\gamma_{k+1}) = p^e$, *and let* $m \geq 1$. *Then*
(1) *If* $p^{e-1}$ *divides* $m$, *then* $D_{m+1,k} = [G, D_{m,k}]$; *consequently,* $d_{m,k} = 0$ *implies* $D_{m,k} = 1$.

(2) *If $m$ is a power of $p$, then $D_{m+1,k} = [G, D_{m,k}] \cdot \mathfrak{U}_1(D_{m,k})$; consequently $d_{m,k} = 0$ implies $D_{m,k} = 1$.*

THEOREM 2.5. *Suppose $d_{m,k} = 0$ and let $n \geq m$. Then*

(1) $D_{n,k} = \mathfrak{U}_1(D_{\lceil n/p \rceil, k})$.

(2) $D_{n,k}^{\leq v} \leq [G, D_{n,k}]$, *where* $v = v_p(m)$.

(3) $D_{n,k} = D_{n,k}^{>v}$, *where* $v = v_p(m)$.

(4) $(n)_{p'} \geq (m)_{p'}$ *implies* $d_{n,k} = 0$.

(5) $d_{n,k} \leq d_{\lceil n/p \rceil, k}$.

We omit most proofs, as they are essentially identical to those given in [Sh1, Sh2] for $k = 0, 1$. However, as part (5) of Theorem 2.5 for $k = 0$ is evidently stronger than the parallel result given in [Sh1, Theorem 1.12], it requires a separate proof. The proof which we now give relies on [Sc].

First observe that, if $n$ is prime to $p$, then $(n)_{p'} = n \geq m \geq (m)_{p'}$. Hence, by part (4) we have $d_{n,k} = 0$, so (5) follows. Therefore we may assume $n = pr$, for some positive integer $r$.

The idea is now to show that the map $x \mapsto x^p$ induces an epimorphism $\varphi$: $D_{r,k}/D_{r+1,k} \to D_{pr,k}/D_{pr+1,k}$. The fact that $\varphi$ is well-defined follows directly from P. Hall's collection formula and the fact that $\{D_{m,k}\}_{m \geq 1}$ is an $N_p$-series (see [Sh1, Theorem 1.12] for details). Furthermore, since $d_{m,k} = 0$, we get by 2.5(1) $D_{pr,k} = \mathfrak{U}_1(D_{r,k})$. Hence, if $\varphi$ is a homomorphism, it must be surjective. So we only have to show that $\varphi$ is a homomorphism.

Pick $x, y \in D_{r,k}$ and write

$$(xy)^p \equiv x^p y^p \bmod \mathfrak{U}_1(D'_{r,k}) \cdot \gamma_p(D_{r,k}).$$

It is sufficient to show that the right-hand terms are contained in $D_{pr+1,k}$. Clearly, $\mathfrak{U}_1(D'_{r,k}) \leq \mathfrak{U}_1(D_{2r,k}) \leq D_{2pr,k} \leq D_{pr+1,k}$, so we are left with the second term. So consider the commutator of $p$ typical factors in the definition of $D_{r,k}$, namely

$$[\mathfrak{U}_{i_1}(\gamma_{j_1+k}), \ldots, \mathfrak{U}_{i_p}(\gamma_{j_p+k})], \qquad \text{where } j_1 p^{i_1}, \ldots, j_p p^{i_p} \geq r.$$

We have to show that it lies in $D_{pr+1,k}$. Lemma 1.2 of [Sc] may be applied in order to express this commutator as a product of certain terms of the kind $\mathfrak{U}_i(\gamma_j)$. Note that, since $d_{m,k} = 0$, we get by 2.5(2) $\gamma_{pr+k} = D_{pr,k}^{\leq 0} \leq [G, D_{pr,k}] \leq D_{pr+1,k}$. Taking this into account, the result follows form [Sc, Lemma 1.2] by a straightforward calculation.

Theorem 2.5(3) provides us with shortened expressions for the groups $D_{n,k}$, provided some of the terms $d_{m,k}$ vanish. Perhaps the simplest phenomenon is

EXAMPLE 2.6. Let $m = ap^{\alpha-1}$, where $a < p$. Suppose $d_{m,k} = 0$, and let $n = ap^{i-1}$, where $i \geq \alpha$. Then, by Theorem 2.5(4), we have $d_{n,k} = 0$. Applying 2.5(3) we conclude that $D_{n,k} = D_{n,k}^{>(i-1)} = \mho_i(\gamma_{k+1})$.

Although the following result deals with ordinary dimension subgroups $D_m$, its proof is based on the properties of the more general series $D_{m,k}$. We denote $d_{m,0}$ by $d_m$. The value of $d_m$ in a subgroup $H$ of $G$ will be denoted by $d_m(H)$.

PROPOSITION 2.7. *Let $k > 1$ and let $H$ be a subgroup of $G$ satisfying*

(1) $H \geq \gamma_k$,

(2) $H' \leq \gamma_{k+1}$.

*Let $m$ be a positive integer with $(m)_{p'} < p$. Then $d_m(G) = 0$ implies $d_m(H) = 0$.*

PROOF. Write $m = ap^{i-1}$. If $a = 1$ then $D_m = 1$ by 2.4(2), and the result is clear. So assume $a \geq 2$. Note that $d_m = 0$ implies $d_{m,k} = 0$ for all $k \geq 0$, by 2.3(2). Example 2.6 now yields $D_{m,k} = \mho_i(\gamma_{k+1})$ for all $k$. Clearly condition (2) implies $\gamma_j(H) \leq \gamma_{j+k-1}$ for all $j \geq 2$. Substitution in Lazard's formula for $D_m(H)$ gives $D_m(H) \leq \mho_i(H)D_{m,k-1}$. But $D_{m,k-1} = \mho_i(\gamma_k) \leq \mho_i(H)$ by condition (1). Therefore $D_m(H) \leq \mho_i(H) \leq D_{p^i}(H) \leq D_{m+1}(H)$, so that $D_m(H) = D_{m+1}(H)$ and $d_m(H) = 0$, as required. ∎

COROLLARY 2.8. *Suppose $(m)_{p'} < p$ and $d_m = 0$. Let $H$ be a subgroup of $G$ satisfying either*

(1) $H = \langle \gamma_k, x \rangle$ *for some $k > 1$ and $x \in G$,*

*or*

(2) $\gamma_{2k-1} \leq H \leq \gamma_k$.

*Then $d_m(H) = 0$.*

Since, assuming $p > 2$, $d_2(H) = 0$ is equivalent to $H$ being powerful, this result generalizes [LM, Corollary 1.2(b)], stating that, for odd $p$, if $G$ is powerful, and for some $k > 1$ we have $\gamma_{k+1} \leq H \leq \gamma_k$, then $H$ is powerful.

## 3. Proof of Theorems A and B

The following phenomenon, which is well known for regular $p$-groups, is proved here in a different context.

LEMMA 3.1. *Let $m = ap^{\alpha-1}$ where $a < p$, and suppose $d_m = 0$. Then*

$$[G, \mho_i(\gamma_k)] = \mho_i(\gamma_{k+1}) \qquad \text{for all } i \geq \alpha \text{ and } k \geq 1.$$

PROOF. Consider first the case $i = \alpha$. Since $d_m = 0$, we must have $d_{m,k} = 0$ for all $k \geq 0$ (by Theorem 2.3(2)). Example 2.6 shows now that $D_{m,k} = \mho_i(\gamma_{k+1})$ for

all $k$. Applying Theorem 2.3(1) we conclude that $[G,\mathfrak{U}_i(\gamma_k)] = [G,D_{m,k-1}] = D_{m,k} = \mathfrak{U}_i(\gamma_{k+1})$.

The general case is now proved by replacing $m$ with $n = ap^{i-1}$, and observing that $d_n = 0$ (by Theorem 2.5(4)). ∎

This lemma extends similar results proved in [LM] for powerful $p$-groups.

We can now prove Theorem A.

So assume $m = ap^{\alpha-1}$, $a < p$, and $d_m = 0$. First observe that, since $\{D_m\}$ is an $N_p$-series starting with $G$, it follows that $\mathfrak{U}_{(i)} \leq D_{p^i}$ for every $i \geq 0$. Hence it is sufficient to verify that, for $i \geq \alpha$, every element of $D_{p^i}$ is a $p^i$th power. Replacing $m$ by $n = mp^{i-\alpha}$ if necessary, we may assume $\alpha = i$. The proof is by induction on $|G|$.

Obviously, we may assume that $G$ is non-cyclic.

By Theorem 2.5(3) we have $D_{p^i} = D_{p^i}^{\geq(i-1)} = \mathfrak{U}_i$. So it remains to be shown that every element in $\mathfrak{U}_i$ is of the form $x^{p^i}$ for some $x$. By P. Hall's collection formula

$$(xy)^{p^i} \equiv x^{p^i}y^{p^i} \bmod \mathfrak{U}_i(G') \prod_{r=1}^{i} \mathfrak{U}_{i-r}(\gamma_{p^r}). \tag{1}$$

Observe that

$$\prod_{r=1}^{i} \mathfrak{U}_{i-r}(\gamma_{p^r}) = D_{p^i}^{\leq(i-1)}. \tag{2}$$

Apply Theorem 2.5(2) to conclude that

$$D_{p^i}^{\leq(i-1)} \leq [G,D_{p^i}] = [G,\mathfrak{U}_i]. \tag{3}$$

But by Lemma 3.1 (with $k = 1$) we have

$$[G,\mathfrak{U}_i] = \mathfrak{U}_i(G'). \tag{4}$$

Combining (1)–(4) we obtain

$$(xy)^{p^i} \equiv x^{p^i}y^{p^i} \bmod \mathfrak{U}_i(G'). \tag{5}$$

It follows that, for every $g$ in $\mathfrak{U}_i$, there exists $x$ in $G$ such that

$$g \in x^{p^i}\cdot\mathfrak{U}_i(G') \leq \mathfrak{U}_i(H) \leq D_{p^i}(H), \qquad \text{where } H = \langle G',x\rangle. \tag{6}$$

Now, $H$ is a proper subgroup of $G$. Moreover, it clearly satisfies condition (1) of Corollary 2.8. Hence the property $d_m = 0$ is inherited by $H$ from $G$, i.e. $d_m(H) = 0$. By induction hypothesis for $H$, every element of $D_{p^i}(H)$ is a $p^i$th power. In particular, $g = h^{p^i}$ for some $h \in H$.

This terminates the proof of Theorem A.

We now formulate Lemma 1.5 of [Sc], in the particular case required here. Observe that, since $\{D_m\}$ is an $N_p$-series, we clearly have $\gamma_s(D_m) \leq D_{sm}$. It turns out that, in certain circumstances, much more can be said.

LEMMA 3.2 [Sc, Lemma 1.5]. *Let $m, s$ be positive integers with $s \geq 2$. Put $n = p(\lceil m/p \rceil + (s-1)m)$. Then $\gamma_s(D_m) \leq \gamma_{sm} D_n$.*

Since $1 + p(s-1) \geq s+1$ for $s \geq 2$, we obtain

COROLLARY 3.3. *If $s \geq 2$ and $\gamma_{sm} = 1$, then $\gamma_s(D_m) \leq D_{(s+1)m}$.*

Let us now prove Theorem B.

The condition on the class of $G$ ensures that $\gamma_m = 1$ for $m = (p-1)p^k$. Since $m+1$ is prime to $p$ and $\gamma_{m+1} = 1$, it follows immediately from Lazard's formula that $D_{m+1} = D_{m+2}$, i.e. $d_{m+1} = 0$. Applying Theorem 2.5(1) we conclude that

$$D_{p^{k+1}} = \mho_1(D_{p^k}). \tag{7}$$

By Corollary 3.3 with $m = p^k$ and $s = p-1$ we obtain

$$\gamma_{p-1}(D_{p^k}) \leq D_{p^{k+1}} \tag{8}$$

(recall that $p$ is odd). Combining (7) and (8) we get

$$\gamma_{p-1}(D_{p^k}) \leq \mho_1(D_{p^k}). \tag{9}$$

Set $H = D_{p^k}$. Then (9) implies $d_{p-1}(H) = 0$. Therefore Theorem A may be applied, to conclude that

$$\mho_{(i)}(H) = \{h^{p^i} : h \in H\} \tag{10}$$

for all $i > 0$. As we have already noted, $\mho_{(k)}(G) \leq D_{p^k} = H$. Hence

$$\mho_{(i+k)}(G) \leq \mho_{(i)}(H). \tag{11}$$

The desired conclusion follows now from (10) and (11).

## 4. Proof of Theorem C

The proof of Theorem C rests on the study of the power-commutator structure of free groups, with respect to their modular dimension subgroups $D_m$.

The following standard result, holding in arbitrary groups $G$, reflects the fact that $\oplus D_m/D_{m+1}$ has the structure of a restricted Lie algebra over $F_p$, induced by the commutator and the $p$th power operations in $G$ (see [Z] and [L] for details).

LEMMA 4.1. *Let $u \in D_m$, $v_i \in D_{n_i}$ for $0 \le i \le s$. Then*

$$[u, v_0^{p^k}, v_1, \ldots, v_s] \equiv [[u, v_0; p^k], v_1, \ldots, v_s] \pmod{D_{n+1}},$$

*where $n = m + n_0 p^k + \sum_{i=1}^{s} n_i$.*

Throughout the rest of this section, we will assume our reader is familiar with P. Hall's commutator collecting process, and with M. Hall's theory of basic commutators, as presented, for instance, in [H] or in [Sc].

From now on let $F$ denote the free group on two generators $x, y$. Set $D_m = D_m(F)$ and $\gamma_n = \gamma_n(F)$ $(m, n \ge 1)$.

LEMMA 4.2 [Sc, Lemma 2.3]. *Let $k$ be the exponent of the commutator $[y, x, y; p-2]$ in P. Hall's expansion of the product $(xy)^p$. Then $k \equiv -1 \pmod{p}$.*

We also need the following fairly standard result (which may be established, e.g., using the method of [MW]).

LEMMA 4.3. *The images in $\gamma_{m+n}/\gamma_{m+n+1}$ of the basic commutators in $x, y$ of partial weights $m, n$, respectively, form a basis for the free abelian group generated by the images of all the commutators of partial weights $m, n$ in $\gamma_{m+n}/\gamma_{m+n+1}$.*

We now turn to the main part of our analysis.

LEMMA 4.4 [Sc, Lemma 1.10]. *Let $u \in D_m \backslash D_{m+1}$. Then $u^{p^k} \in D_{p^k m} \backslash D_{p^k m+1}$.*

The following description of a basis for $D_{pm}/D_{pm+1}$ in terms of a basis for $D_m/D_{m+1}$ is extremely useful for our purpose.

LEMMA 4.5 [Sc, Lemma 1.11]. *A set of representatives of a basis of $D_{pm}/D_{pm+1}$ is given by the union of the set of the basic commutators of weight $pm$ with the set of the $p$th powers of the representatives of a basis of $D_m/D_{m+1}$.*

COROLLARY 4.6. *The map $x \mapsto x^p$ induces an isomorphism $\mu_m : D_m/D_{m+1} \to D_{pm}/\gamma_{pm} D_{pm+1}$.*

PROOF. It is well known (see, e.g., [Sh1], or the proof of Theorem 2.5 above) that $x \mapsto x^p$ induces a well-defined map from $D_m/D_{m+1}$ to $D_{pm}/D_{pm+1}$, so $\mu_m$ is the composition of this map with the canonical projection $D_{pm}/D_{pm+1} \to D_{pm}/\gamma_{pm} D_{pm+1}$. Using P. Hall's collection formula for $(xy)^p$ and Corollary 3.2 (with $s = p$), we see that $\mu_m$ is actually a homomorphism. Now, since the images in $D_{pm}/D_{pm+1}$ of the basic commutators of weight $pm$ generate $\gamma_{pm} D_{pm+1}/D_{pm+1}$, it follows from Lemma 4.5 above that $\mu_m$ maps any basis of $D_m/D_{m+1}$ to a basis of $D_{pm}/\gamma_{pm} D_{pm+1}$. Hence $\mu_m$ is an isomorphism. ∎

It is noteworthy that results 4.4–4.6 hold in fact for arbitrary free groups.

We now turn to the proof of Theorem C.

Let $F$ be as before, and let $G = F/D_{p^{k+1}+1}$.

$G$ is clearly a finite $p$-group of class $p^{k+1}$. We will identify elements of $F$ (e.g., $x,y$) with their images in $G$. This will not cause confusion, since we are not going to work in $F$ any more.

Consider the element $z = x^{p^{k+1}}y^{p^{k+1}} \in U_{k+1}(G) \leq D_{p^{k+1}}(G)$. We claim that $z$ is not a $p$th power.

By way of contradiction, assume that $z = w^p$ for some $w \in G$.

Then $w^p \in D_{p^{k+1}}(G) \setminus D_{p^{k+1}+1}(G)$, so Lemma 4.4 (applied for $F$) easily implies $w \in D_{p^k}(G) \setminus D_{p^k+1}(G)$.

Define $\bar{G} = G/\gamma_{p^{k+1}}(G) = F/\gamma_{p^{k+1}}D_{p^{k+1}+1}$, and use the $^-$-notation consistently.

Set $m = p^k$, and let $\mu = \mu_m$ be the isomorphism from $D_m/D_{m+1}$ to $D_{pm}/\gamma_{pm}D_{pm+1}$ defined in Corollary 4.6. Then $\mu$ may be identified, in a natural way, with the map from $D_{p^k}(\bar{G})/D_{p^k+1}(\bar{G})$ to $D_{p^{k+1}}(\bar{G})$, induced by taking $p$th powers.

Since $\mu$ is a homomorphism, we clearly have

$$\mu(\bar{x}^{p^k}\bar{y}^{p^k}D_{p^k+1}(\bar{G})) = \bar{x}^{p^{k+1}}\bar{y}^{p^{k+1}} = \bar{z} = \mu(\bar{w}D_{p^k+1}(\bar{G}))$$

and by the injectivity of $\mu$, $\bar{w} \equiv \bar{x}^{p^k}\bar{y}^{p^k} (\mathrm{mod}\, D_{p^k+1}(\bar{G}))$, which implies $w \equiv x^{p^k}y^{p^k} (\mathrm{mod}\, D_{p^k+1}(G))$. Since the value of $w^p$ depends only on the image of $w$ in $D_{p^k}(G)/D_{p^k+1}(G)$, this allows us to assume that $w = x^{p^k}y^{p^k}$.

Let us now apply P. Hall's collection process in order to compute $w^p$.

Write $w^p = x^{p^{k+1}}y^{p^{k+1}}P$, where $P$ is a product of basic commutators of weight $p$ in $x^{p^k}, y^{p^k}$ (all the other factors are easily seen to be trivial). Among these there is only one basic commutator of weight 1 in $x^{p^k}$, namely $[y^{p^k}, x^{p^k}, y^{p^k}; p-2]$, and, by Lemma 4.2, it appears in this expansion with exponent $-1$.

Apply Lemma 4.1 to conclude that, in $G$,

$$[y^{p^k}, x^{p^k}, y^{p^k}; p-2] = [[y,x;p^k], y; p^{k+1}-1].$$

All the other factors appearing in $P$ may be written (using 4.1) as commutators of total weight $p^{k+1}$ in $x$ and $y$, whose partial weight in $x$ is at least $2p^k$.

Therefore, by Lemma 4.3,

$$w^p = x^{p^{k+1}}y^{p^{k+1}}[[y,x;p^k], y; p^{k+1}-1]^{-1}Q \tag{12}$$

where $Q$ is a product of basic commutators of total weight $p^{k+1}$ in $x$ and $y$, whose partial weight in $x$ is at least $2p^k$.

Equation (12) expresses $w^p$ (regarded as an element of $D_{p^{k+1}}/D_{p^{k+1}+1} \cong$

$D_{p^{k+1}}(G)$) in terms of a basis of the type given in Lemma 4.5. This expression is unique, so, in particular, $w^p \neq x^{p^{k+1}} y^{p^{k+1}}$.

This contradiction concludes the proof of Theorem C.

REMARK. While this paper was written, R. Dark pointed out to the authors that the example $G$ of Theorem C can be obtained as a subgroup of the group of units in the truncated free algebra on two noncommutative variables (see [HB, p. 265, Exercise 3]). While Dark's approach yields a shorter proof for Theorem C, our method seems to give a somewhat deeper insight into the power-commutator structure of $G$.

## ACKNOWLEDGEMENT

The second author would like to thank the Dipartimento di Matematica at Trento for its kind hospitality while part of this work was carried out.

## REFERENCES

[A] J. L. Alperin, *Loewy structure of permutation modules for p-groups*, Quart. J. Math. Oxford (2) **39** (1988), 129–133.

[Ar] D. E. Arganbright, *The power-commutator structure of finite p-groups*, Pac. J. Math. **29** (1969), 11–17.

[H] M. Hall, *The Theory of Groups*, 2nd Edition, New York, 1976.

[Ha] P. Hall, *A contribution to the theory of groups of prime power order*, Proc. London Math. Soc. **36** (1933), 29–95.

[Hu] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[HB] B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin, 1982.

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

[L] M. Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. École Norm. Sup. **71** (1954), 101–190.

[LM] A. Lubotzki and A. Mann, *Powerful p-groups I*, J. Algebra **105** (1987), 484–505.

[LS] C. R. Leedham-Green and R. Staszewski, *On the Loewy and Jennings series of a finite p-group*, preprint.

[M1] A. Mann, *The power structure of p-groups I*, J. Algebra **42** (1976), 121–135.

[M2] A. Mann, *On the power structure of some p-groups*, in *Group Theory-Bressanone 1989*, Palermo, 1990, pp. 227–235.

[MW] H. Meier-Wunderli, *Note on a basis of P. Hall for the higher commutators in free groups*, Comm. Math. Helv. **26** (1952), 1–5.

[P] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley Interscience, New York, 1978.

[P1] I. B. S. Passi, *Group Rings and Their Augmentation Ideals*, Lecture Notes in Math. Vol. 715, Springer-Verlag, Berlin, 1979.

[PS1] I. B. S. Passi and S. K. Sehgal, *Isomorphism of modular group algebras*, Math. Z. **129** (1972), 65–73.

[PS2] I. B. S. Passi and S. K. Sehgal, *Lie dimension subgroups*, Comm. Algebra **3** (1975), 59–73.

[R] F. Röhl, *Remarks on unit groups of completed modular group algebras and the isomorphism problem*, preprint.

[Sc] C. M. Scoppola, *Groups of prime power order as Frobenius-Wielandt complements*, Trans. Am. Math. Soc., to appear.

[Sh1] A. Shalev, *Dimension subgroups, nilpotency indices, and the number of generators of ideals in p-group algebras*, J. Algebra **129** (1990), 412-438.

[Sh2] A. Shalev, *Lie dimension subgroups, Lie nilpotency indices, and the exponent of the group of normalized units*, J. London Math. Soc., to appear.

[Shi] D. Shield, *The class of a nilpotent wreath product*, Bull. Aust. Math. Soc. **17** (1977), 53-89.

[W] B. A. F. Wehrfritz, *Unipotent representations of nilpotent groups*, Bull. London Math. Soc. **19** (1987), 320-324.

[Z] H. Zassenhaus, *Ein Verfahren, jeder endlichen p-Gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen*, Abh. Math. Sem. Univ. Hamburg **13** (1939), 200-207.