IDENTIFICATIONS IN MODULAR GROUP ALGEBRAS

HAMID USEFI

ABSTRACT. Let G be a group, S a subgroup of G, and $\mathbb{F}$ a field of characteristic p. We denote the augmentation ideal of the group algebra $\mathbb{F}G$ by $\omega(G)$. The Zassenhaus-Jennings-Lazard series of G is defined by $D_n(G) = G \cap (1 + \omega^n(G))$. We give a constructive proof of a Theorem of Quillen stating that the graded algebra associated to $\mathbb{F}G$ is isomorphic as an algebra to the enveloping algebra of the restricted Lie algebra associated to the $D_n(G)$. We then extend a theorem of Jennings that provides a basis for the quotient $\omega^n(G)/\omega^{n+1}(G)$ in terms of a basis of the restricted Lie algebra associated to the $D_n(G)$. We shall use these theorems to prove the main results of this paper. For G a finite p-group and n a positive integer, we prove that $G \cap (1+\omega(G)\omega^n(S)) = D_{n+1}(S)$ and $G \cap (1 + \omega^2(G)\omega^n(S)) = D_{n+2}(S)D_{n+1}(S \cap D_2(G))$. The analogous results for integral group rings of free groups have been previously obtained by Gruenberg, Hurley, and Sehgal.

1. INTRODUCTION

The connection between the commutator subgroup of a group and Lie theory has been highly developed. Perhaps, the first and central example is the Magnus embedding [11] of a free group F into the power series ring completion of a free associative ring. In particular, Magnus confirmed the so called dimension subgroup conjecture for free groups by proving that $F \cap (1+\mathfrak{f}^n) = \gamma_n(F)$. Here, $\mathfrak{f}$ is the augmentation ideal of the integral group ring $\mathbb{Z}F$ and $\gamma_n(F)$ is the n^{th} term of the lower central series of F.

Closely related to the Magnus representation is the free differential calculus of Fox [3] originating in Knot theory. Let R be a normal subgroup of F and denote by $\mathfrak{r}$ the kernel of the natural homomorphism $\mathbb{Z}F \to \mathbb{Z}(F/R)$. The problem of identifying the subgroups $F \cap (1 + \mathfrak{r}\mathfrak{f}^n)$ which was posed by Fox was considered amongst the most important problems in combinatorial group theory, see [10]. A complete solution to this problem was given independently by Hurley [6] and Yunus [18].

The purpose of the present paper is to consider the analogue of Fox's problem for finite p-groups over a field $\mathbb{F}$ of characteristic p. We denote by $\mathbb{F}_p$ the field of p elements. Let G be a group. Recall that the augmentation ideal, $\omega(G)$, of the group algebra $\mathbb{F}G$ is the kernel of the algebra map $\epsilon : \mathbb{F}G \to \mathbb{F}$

2000 *Mathematics Subject Classification.* Primary 20C07, 16S34; Secondary 20C11.

The research is supported by a postdoctoral fellowship from the department of Mathematics at the University of British Columbia.

induced by $\sum_{g\in G}\alpha_g g \mapsto \sum_{g\in G}\alpha_g$. For every $n \geq 1$, the n^{th} dimension subgroup of G is defined by

$$D_n(G) = G \cap (1+\omega^n(G)) = \prod_{ip^j\geq n} \gamma_i(G)^{p^j}.$$

This series is also known as the Zassenhaus-Jennings-Lazard series of G. Since $D_i(G)/D_{i+1}(G)$ is an elementary abelian p-group, it may be viewed as a vector space over $\mathbb{F}_p$. It is known that the graded $\mathbb{F}_p$-vector space

$$\mathcal{L} := \bigoplus_{i\geq 1} D_i(G)/D_{i+1}(G),$$

is a restricted Lie algebra, see [13], for example. The corresponding construction for $\mathbb{F}G$ is to consider the graded algebra associated to the filtration of $\mathbb{F}G$ by the powers of $\omega(G)$:

$$\mathrm{gr}(\mathbb{F}G) := \bigoplus_{i\geq 0} \omega^i(G)/\omega^{i+1}(G).$$

The natural bridge between $\mathcal{L}$ and $\mathrm{gr}(\mathbb{F}G)$ is provided by a well-known theorem of Quillen [14] stating that $\mathrm{gr}(\mathbb{F}G)$ is isomorphic as an $\mathbb{F}$-algebra to the restricted enveloping algebra of $\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L}$. We give a new proof of Quillen's Theorem in a constructive way, see Theorem 3.2. Meanwhile, we are able to extend a theorem of Jennings that plays the role of the Poincaré-Birkhoff-Witt Theorem for enveloping algebras, see Theorem 3.1 and Corollary 3.3.

Let S be a subgroup of a group G and n a positive integer. It follows from the results of Section 4 that $G \cap (1+\omega(S)\omega^n(G)) \subseteq D_{n+1}(S)D_{n+2}(G)$, see Proposition 4.2. Our main results, though, are about finite p-groups. It is well-known that $\omega(G)$ is nilpotent if and only if G is a finite p-group, see [2] or [13]. This fact is one of the main reasons that we have to restrict ourselves to finite p-groups. Our results hold over any field of characteristic p. The following is our first main result:

Theorem A. *Let G be a finite p-group. For every subgroup S of G and every positive integer n, we have*

$$G \cap (1+\omega(G)\omega^n(S)) = D_{n+1}(S).$$

We shall prove Theorem A in Section 5. The analogue of Theorem A for free groups says that $F \cap (1+\mathfrak{r}^n) = \gamma_{n+1}(R)$, for every $n \geq 1$. This result was first proved by Gruenberg using induction on n, see Section 4.1 in [4]. The case $n = 1$ was independently proved by Magnus [11], Schumann [16], and Fox [3]. Our second main result is as follows:

Theorem B. *Let G be a finite p-group. For every subgroup S of G and every positive integer n, we have*

$$G \cap (1+\omega^2(G)\omega^n(S)) = D_{n+2}(S)D_{n+1}(S \cap D_2(G)).$$

The analogue of Theorem B for free groups is due to Hurley and Sehgal [7]. They prove that $F \cap (1 + \mathfrak{f}^2\mathfrak{r}^n) = \gamma_{n+2}(R)\gamma_{n+1}(R \cap \gamma_2(F))$, for every $n \geq 1$. We shall prove Theorem B in Section 6.

I would like to thank the referee, Luzius Grunenfelder, and Dale Rolfsen for their valuable comments and discussions.

2. Preliminary results and definitions

2.1. **Restricted Lie algebras.** Throughout this paper, $\mathbb{F}$ denotes a field of characteristic p and $\mathbb{F}_p$ denotes the field of p elements. Unless otherwise stated all vector spaces are taken over $\mathbb{F}$. Let L be a Lie algebra over $\mathbb{F}$. The adjoint representation of L is given by $\mathrm{ad}x : L \to L$, $\mathrm{ad}x(y) = [y, x]$, where $x, y \in L$. Recall that L is called a restricted Lie algebra or Lie p-algebra [8], if it additionally affords a p-map $^{[p]} : L \to L$, satisfying

(1) $(\mathrm{ad}x)^p = \mathrm{ad}(x^{[p]})$, for every $x \in L$;
(2) $(\alpha x)^{[p]} = \alpha^p x^{[p]}$, for every $x \in L$ and $\alpha \in \mathbb{F}$; and,
(3) $(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x, y)$, for all $x, y \in L$, where $is_i(x, y)$ is the coefficient of λ^{i-1} in $\mathrm{ad}(\lambda x + y)^{p-1}(x)$.

Let L be a restricted Lie algebra. We denote the restricted enveloping algebra of L by $u(L)$. The augmentation ideal, $\omega(L)$, of $u(L)$ is the associative ideal of $u(L)$ generated by L. Let $\gamma_1(L) = L$. For every $n \geq 2$, we denote by $\gamma_n(L) = [\gamma_{n-1}(L), L]$ the n^{th} term of the lower central series of L. The n^{th} dimension subalgebra of L is

$$D_n(L) = L \cap \omega^n(L) = \sum_{ip^j \geq n} \gamma_i(L)^{[p]^j},$$

where $\gamma_i(L)^{[p]^j}$ is the restricted subalgebra of L generated by all $x^{[p]^j}$, $x \in \gamma_i(L)$, see [15]. The *height* of an element $x \in L$, $\nu(x)$, is defined to be the largest integer n in which $x \in D_n(L)$, if n exists and it is infinity otherwise.

Let X be an ordered basis of L over $\mathbb{F}$. The analogue of the Poincaré-Birkhoff-Witt (PBW) Theorem for restricted Lie algebras (see [8]) allows us to view L as a restricted Lie subalgebra of $u(L)$ in such a way that $u(L)$ has a basis consisting of PBW monomials, that is, monomials of the form

$$x_1^{a_1} \dots x_t^{a_t},$$

where $x_1 < \cdots < x_t$ in X, $0 \leq a_i \leq p-1$, and t is a non-negative integer. The *weight* of any such monomial is defined to be $\sum_{i=1}^{t} a_i \nu(x_i)$.

It is known that $[D_n(L), D_m(L)] = \gamma_{m+n}(L)$ and $D_n(L)^{[p]} \subseteq D_{np}(L)$, for every $m, n \geq 1$, see [15]. Furthermore, it is not hard to see that the Lie commutator and the $[p]$-map in L induce a restricted Lie algebra structure on the graded vector space

$$\mathrm{gr}(L) := \bigoplus_{i \geq 1} D_i(L)/D_{i+1}(L).$$

We need to fix some notations for the next lemma. Let n be a sufficiently large integer. Let $\bar{X}_n$ be a homogeneous basis for $\bigoplus_{i=1}^{n} D_i(L)/D_{i+1}(L)$ and X_n be a fixed set of representatives of $\bar{X}_n$. We can extend X_n to a basis X of L by choosing a basis for $D_{n+1}(L)$. Finally we order X in some way. With these notations we have:

Lemma 2.1. *Let L be a restricted Lie algebra with an ordered basis X as described above. For every positive integer m, $\omega^m(L)$ is spanned by all PBW monomials in X of weight at least m.*

Lemma 2.1 is a modification and correction of Theorem 2.1 in [15]. Note that the hypothesis of Theorem 2.1 in [15] does not hold for every restricted Lie algebra. However, Lemma 2.1 can be proved along the same lines as the proof of Theorem 2.1 in [15].

Note that for every positive integer i, the quotient $D_i(L)/D_{i+1}(L)$ embeds into $\omega^i(L)/\omega^{i+1}(L)$ via $x+D_{i+1}(L) \mapsto x+\omega^{i+1}(L)$, for every $x \in D_i(L)$. Thus $\mathrm{gr}(L)$ embeds into $\mathrm{gr}(\omega(L))$ and so there is an induced algebra map $\varphi : u(\mathrm{gr}(L)) \to \mathrm{gr}(u(L))$. Note that $L/D_2(L) \cong \omega(L)/w^2(L)$. Hence, φ is surjective. We claim that φ is injective. Let $\bar{w}$ be a non-zero element in $u(\mathrm{gr}(L))$ such that $\varphi(\bar{w}) = 0$. By the PBW Theorem, there exist linearly independent homogeneous elements $\bar{x}_1, \ldots, \bar{x}_t \in \mathrm{gr}(L)$ such that $\bar{w} = \sum \alpha \bar{x}_1^{a_1} \ldots \bar{x}_t^{a_t}$, where each α lies in $\mathbb{F}$ and all but finitely many of them are non-zero. Let x_i be a fixed representative of $\bar{x}_i$, for every $1 \leq i \leq t$. Since $\mathrm{gr}(u(L))$ is graded, without loss of generality, we assume that all PBW monomials in the expression of w have the same weight, namely n. Then $\varphi(\bar{w}) = 0$ simply means that $\varphi(\bar{w}) = \sum \alpha x_1^{a_1} \ldots x_t^{a_t} \in \omega^{n+1}(L)$. But this contradicts Lemma 2.1. We have established the following:

Theorem 2.2. *Let L be a restricted Lie algebra. The map $u(\mathrm{gr}(L)) \to \mathrm{gr}(u(L))$ induced by the embeddings $D_i(L)/D_{i+1}(L) \hookrightarrow \omega^i(L)/\omega^{i+1}(L)$ is an algebra isomorphism.*

2.2. **Dimension subgroups.** Let G be a group. For every $g, h \in G$, we denote by (g, h) the group commutator $g^{-1}h^{-1}gh$ and by $[g, h]$ the Lie commutator $gh - hg$ in $\mathbb{F}G$. Let H and K be subgroups of G. We denote by (H, K) the subgroup of G generated by all group commutators (h, k) and by H^p the group generated by all h^p, where $h \in H$ and $k \in K$. Dimension subgroups of G are defined by

$$D_n(G) = G \cap (1 + \omega^n(G)) = \prod_{ip^j \geq n} \gamma_i(G)^{p^j},$$

for every $n \geq 1$, see [13]. This series is also known as the Zassenhaus-Jennings-Lazard series of G. We shall write D_n for $D_n(G)$ if there is no confusion. It is well-known that the $\{D_n\}$ is an N_p-series of G, that is $(D_i, D_j) \subseteq D_{i+j}$, and $D_i^p \subseteq D_{ip}$, for every $i, j \geq 1$, see [13].

Let S be a subgroup of G and $g \in S$. The *height* of g in S is denoted by $\nu_S(g)$ and is defined to be the largest integer t such that $g \in D_t(S)$, if t

exists and to be infinity if it does not. We shall denote the height of g in G by $\nu(g)$.

Note that each quotient D_i/D_{i+1} is an elementary abelian p-group and so we can view D_i/D_{i+1} as a vector space over $\mathbb{F}_p$. A typical element of the quotient D_i/D_{i+1} is a left coset gD_{i+1}, where $g \in D_i$.

Consider the $\mathbb{F}_p$-vector space

$$\mathcal{L} := \bigoplus_{i\geq 1} D_i/D_{i+1}.$$

It is known that $\mathcal{L}$ inherits a restricted Lie algebra structure, see [13], for example. Indeed, the Lie bracket and the $^{[p]}$-map can be defined first on homogeneous elements of $\mathcal{L}$ and then they can be extended linearly:

$$[gD_{m+1}, hD_{n+1}] := (g,h)D_{m+n+1}, \qquad (gD_{m+1})^{[p]} := g^p D_{mp+1},$$

where $g \in D_m$ and $h \in D_n$. If R and S are subgroups of G, we denote by $\mathcal{R}$ and $\mathcal{S}$ the associated $\mathbb{F}_p$-restricted Lie algebras obtained from their dimension subgroups. There is, however, another restricted Lie algebra associated to a subgroup S of G. For every positive integer i, denote by C_i the subgroup $S \cap D_i$. Note that $(C_i, C_j) \subseteq C_{i+j}$, and $C_i^p \subseteq C_{ip}$, for every $i, j \geq 1$. It follows that the associated vector space $\mathfrak{S} = \bigoplus_{i\geq 1} C_i/C_{i+1}$ is a graded restricted Lie algebra over $\mathbb{F}_p$. Wall [17] has given a nice survey of these constructions.

The following lemma follows from the definitions.

Lemma 2.3. *The following statements hold.*

(1) $D_n(\mathcal{L}) = \bigoplus_{i\geq n} D_i/D_{i+1}$, *for every* $n \geq 1$.
(2) *The graded* $\mathbb{F}_p$*-restricted Lie algebras* $\mathrm{gr}(\mathcal{L})$ *and* $\mathcal{L}$ *are isomorphic.*
(3) *The graded* $\mathbb{F}$*-restricted Lie algebras* $\mathrm{gr}(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})$ *and* $\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L}$ *are isomorphic.*

Let $\bar{X}$ be an ordered linearly independent homogeneous subset of $\mathcal{L}$ over $\mathbb{F}_p$. Let X be a fixed set of representatives of $\bar{X}$. It follows that X is a linearly independent subset of $\mathbb{F}G$. Also, X inherits the ordering of $\bar{X}$. A *straight monomial* in X is of the form $(x_1 - 1)^{a_1} \dots (x_t - 1)^{a_t}$, where $x_1 \leq \cdots \leq x_t$ in X, $0 \leq a_k < p$, and t is a non-negative integer. The *weight* of any such monomial is defined to be $\sum_{k=1}^t a_k \nu(x_k)$ and its *degree* is $\sum_{k=1}^t a_k$.

We shall say X is ordered with respect to the dimension subgroups of G provided that $x_1 \leq x_2$ implies $\nu(x_1) \leq \nu(x_2)$, for every $x_1, x_2 \in X$. Note that, by Lemma 2.3, $\nu(x) = n$ in G if and only if $\nu(\bar{x}) = n$ in $\mathcal{L}$, for every $x \in X$. Note that for every $g, h \in G$ we have

$$gh - 1 = (g-1) + (h-1) + (g-1)(h-1). \tag{2.4}$$

Thus, if $x_1 \leq x_2 \in X$ then $x_1 x_2 - 1 = (x_1 - 1) + (x_2 - 1)$, modulo straight monomials of degree at least two.

3. An extension of Jennings' Theorem

Note that D_i/D_{i+1} embeds into $\omega^i(G)/\omega^{i+1}(G)$ via the map $g \mapsto g-1$, for every $i \geq 1$. The induced map $\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L} \to \mathrm{gr}(\mathbb{F}G)$ is a restricted Lie algebra homomorphism and consequently there is an algebra map $\phi : u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L}) \to \mathrm{gr}(\mathbb{F}G)$. Note that $u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})$ and $\mathbb{F} \otimes_{\mathbb{F}_p} u(\mathcal{L})$ may be identified as $\mathbb{F}$-algebras. Since $\phi(\mathbb{F} \otimes_{\mathbb{F}_p} D_1/D_2) = \omega(G)/\omega^2(G)$ and $\mathrm{gr}(\mathbb{F}G)$ is generated by $\omega(G)/\omega^2(G)$, it follows that ϕ is surjective. The fact that ϕ is injective is a well-known theorem of Quillen [14] where his proof is based on the structure theorems of Milnor and Moore for Hopf algebras. Another alternative proof is given in [13] and Section 3.14 in [1]. Here, we give a new proof of Quillen's Theorem and then extend the following theorem of Jennings. For a proof of Jennings' Theorem see [9] or Theorem 2.6 in Chapter VIII of [5].

Theorem 3.1 (Jennings)**.** *Let $\bar{X}$ be a homogeneous basis of $\mathcal{L}$ over $\mathbb{F}_p$ and X a fixed set of representatives of $\bar{X}$. If X is ordered with respect to the dimension subgroups of G then the set of all straight monomials in X of weight n forms an $\mathbb{F}$-basis of $\omega^n(G)/\omega^{n+1}(G)$.*

Theorem 3.2 (Quillen)**.** *The map $\phi : u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L}) \to \mathrm{gr}(\mathbb{F}G)$ induced by the embeddings $D_i/D_{i+1} \hookrightarrow \omega^i(G)/\omega^{i+1}(G)$ is an $\mathbb{F}$-algebra isomorphism.*

Proof. Notice that $\phi(\omega(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})) = \bigoplus_{i\geq 1} \omega^i(G)/\omega^{i+1}(G)$. To see this, note that $\phi(\mathbb{F} \otimes_{\mathbb{F}_p} D_1/D_2) = \omega(G)/\omega^2(G)$. Thus, the image under ϕ of the associative ideal generated by D_1/D_2 in $u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})$ is the associative ideal generated by $\omega(G)/\omega^2(G)$ in $\mathrm{gr}(\mathbb{F}G)$. Consequently,

$$\phi(\omega^n(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})) = \bigoplus_{i\geq n} \omega^i(G)/\omega^{i+1}(G),$$

for every $n \geq 1$. Notice that, by Theorem 3.1 and Lemma 2.1, the induced map

$$\bar{\phi}_n : \omega^n(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})/\omega^{n+1}(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L}) \to \omega^n(G)/\omega^{n+1}(G)$$

is an isomorphism, for every $n \geq 1$. So, ϕ induces an isomorphism of $\mathbb{F}$-vector spaces:

$$\bar{\phi} : \mathrm{gr}(u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})) \to \mathrm{gr}(\mathbb{F}G).$$

Now consider the diagram:

$$\begin{array}{ccc} \mathrm{gr}(u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})) & \xrightarrow{\bar{\phi}} & \mathrm{gr}(\mathbb{F}G) \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \phi} \\ u(\mathrm{gr}(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L})) & \longleftarrow & u(\mathbb{F} \otimes_{\mathbb{F}_p} \mathcal{L}) \end{array}$$

The map φ is the isomorphism described in Theorem 2.2 and the map in the second row is the isomorphism induced from Lemma 2.3. We observe that the diagram is commutative. To do so, it is enough to take an ordered homogeneous basis $\bar{X}$ of $\mathcal{L}$ over $\mathbb{F}_p$ and verify the commutativity of the

diagram on every PBW monomial of $u(\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L})$. It follows that ϕ and $\bar{\phi}$ are algebra isomorphisms. □

Corollary 3.3. *Let $\bar{X}$ be an ordered homogeneous basis of $\mathcal{L}$ over $\mathbb{F}_p$. Let X be a fixed set of representatives of $\bar{X}$ and n a positive integer. Then the set of all straight monomials in X of weight n forms an $\mathbb{F}$-basis for $\omega^n(G)/\omega^{n+1}(G)$.*

Proof. We know that the set of all $1\otimes\bar{x}$ with $\bar{x}\in\bar{X}$ is an $\mathbb{F}$-basis for $\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L}$. So, by Lemmas 2.1 and 2.3, the PBW monomials $1\otimes\bar{x}_1^{a_1}\dots\bar{x}_t^{a_t}$ with $\sum_{k=1}^{t}a_k\nu(\bar{x}_k)=n$ form a basis for $\omega^n(\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L})/\omega^{n+1}(\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L})$. Note that

$$\bar{\phi}(1\otimes\bar{x}_1^{a_1}\dots\bar{x}_t^{a_t}+\omega^{n+1}(\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L}))=(x_1-1)^{a_1}\dots(x_t-1)^{a_t}+\omega^{n+1}(G).$$

The result then follows since $\omega^n(\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L})/\omega^{n+1}(\mathbb{F}\otimes_{\mathbb{F}_p}\mathcal{L})\cong\omega^n(G)/\omega^{n+1}(G)$. □

Note that we have shown that Theorem 3.2 and Corollary 3.3 are equivalent. It is well-known that $\omega(G)$ is nilpotent if and only if G is a finite p-group, see [2] or [13]. So we can deduce the following immediately from Corollary 3.3.

Corollary 3.4. *Let G be a finite p-group and $\bar{X}$ an ordered homogeneous basis of $\mathcal{L}$ over $\mathbb{F}_p$. If X is a set of representatives of $\bar{X}$ then the set of all straight monomials in X of weight at least n is an $\mathbb{F}$-basis for $\omega^n(G)$, for every $n\geq 1$.*

4. Some general results

In this section R is a subgroup of an arbitrary group S. We fix the following notations for the rest of this section. For every $i\geq 1$, consider the natural sequence of $\mathbb{F}_p$-vector spaces:

$$\frac{D_i(R)\cap D_{i+1}(S)}{D_{i+1}(R)}\xhookrightarrow{f_i}\frac{D_i(R)}{D_{i+1}(R)}\xrightarrow{g_i}\frac{D_i(R)}{D_i(R)\cap D_{i+1}(S)}\xhookrightarrow{h_i}\frac{D_i(S)}{D_{i+1}(S)}.$$

Note that the maps g_i are surjective. There is an induced natural sequence of graded $\mathbb{F}_p$-vector spaces as follows:

$$\begin{array}{ccccc}\mathcal{V}=\bigoplus_{i\geq 1}\frac{D_i(R)\cap D_{i+1}(S)}{D_{i+1}(R)} & \xhookrightarrow{f} & \mathcal{R}=\bigoplus_{i\geq 1}\frac{D_i(R)}{D_{i+1}(R)} & & \\ & & \downarrow g & & \\ & & \mathcal{W}=\bigoplus_{i\geq 1}\frac{D_i(R)}{D_i(R)\cap D_{i+1}(S)} & \xhookrightarrow{h} & \mathcal{S}=\bigoplus_{i\geq 1}\frac{D_i(S)}{D_{i+1}(S)}.\end{array}$$

Since g is surjective, we can choose a linearly independent homogeneous subset $\bar{X}\subseteq\mathcal{R}$ so that $g(\bar{X})$ is a homogeneous basis for $\mathcal{W}$ over $\mathbb{F}_p$. Let $\bar{Y}$ be an $\mathbb{F}_p$-homogeneous basis for $\mathcal{V}$. Clearly, $\bar{X}\cup\bar{Y}$ is a homogeneous basis of $\mathcal{R}$ over $\mathbb{F}_p$. Since h is injective, we can extend $g(\bar{X})$ to a basis $\bar{Z}$ of $\mathcal{S}$ over

$\mathbb{F}_p$. Let X, Y, Z be fixed sets of representatives of $\bar{X}, \bar{Y}, \bar{Z}$, respectively (we assume $X \subseteq Z$).

We order X with respect to $D_n(R)$. We then order $X \cup Y$ assuming that every $x \in X$ is less than every $y \in Y$. We also order Z so that every $x \in X$ is less than every $z \in Z \setminus X$. Note that the elements $z-1$ with $z \in Z$ form a linearly independent subset of $\omega(S)$ over $\mathbb{F}$. Let E_2 be the $\mathbb{F}$-vector space spanned by all straight monomials in Z of degree at least two.

Lemma 4.1. *Let S be a group and R a subgroup of S. Then for every positive integer n and non-negative integer k with $k \leq n-1$, we have*

$$\omega^{n-k}(R)\omega^k(S) \subseteq \omega^{n+1}(S) + E_2 + \omega^n(R).$$

Proof. We use induction on k; the case $k = 0$ being trivial. Let $w \in \omega^{n-k-1}(R)\omega^{k+1}(S)$. By Corollary 3.3 applied to both R and S, w is a sum of elements uv, where each u lies in $\omega^{n-k-1}(R)$ and, modulo $\omega^{n-k}(R)$, is a straight monomial in $X \cup Y$ and each v lies in $\omega^{k+1}(S)$ and, modulo $\omega^{k+2}(S)$, is a straight monomial in Z. Thus, without loss of generality, we assume that each u is a straight monomial in $X \cup Y$, each v is a straight monomial in Z, and

$$w = \sum uv \text{ modulo } \omega^{n+1}(S).$$

Note that if u involves a basis element $y-1$, $y \in Y$, then uv lies in $\omega^{n+1}(S)$. So, modulo $\omega^{n+1}(S)$, we can assume that each u is a straight monomial in X. Now suppose that $v = (z-1)v_1$, where $z \in Z$. We observe that if $z \notin X$ then uv is a straight monomial of degree at least 2. Thus, modulo E_2, each v is of the form $v = (z-1)v_1$ and $z \in X$. But $z \in X$ means that $z \in D_i(S)$ if and only if $z \in D_i(R)$, where i is a positive integer. So, modulo $\omega^{n+1}(S) + E_2$, we have

$$uv = (u(z-1))v_1 \in \omega^{n+i-k-1}(R)\omega^{k-i+1}(S).$$

It follows, by induction hypothesis applied to $k-i+1$, that uv lies in $\omega^{n+1}(S) + E_2 + \omega^n(R)$. Hence, $w \in \omega^{n+1}(S) + E_2 + \omega^n(R)$ and the proof is complete. □

Proposition 4.2. *Let S be a group and R a subgroup of S. Then for every positive integer n, we have*

$$S \cap (1 + \omega^{n+1}(S) + \omega(R)\omega^{n-1}(S)) \subseteq D_n(R)D_{n+1}(S).$$

Proof. Let $w \in S$ such that $w-1 \in \omega^{n+1}(S) + \omega(R)\omega^{n-1}(S)$. By the previous lemma, we have

$$w - 1 \in \omega^{n+1}(S) + E_2 + \omega^n(R).$$

Thus, modulo $\omega^{n+1}(S) + E_2$ and by Corollary 3.3, we can write $w-1$ as a linear combination of straight monomials $u \in \omega^n(R)$ in the basis $X \cup Y$. But if u involves a basis element $y-1$, $y \in Y$, then u lies in $\omega^{n+1}(S)$. So, modulo

$\omega^{n+1}(S) + E_2$, each u is a straight monomial in X. Also, if the degree of u is greater than one then $u \in E_2$. Hence,

$$w = \sum_{x \in X} \alpha_x (x-1) \text{ modulo } \omega^{n+1}(S) + E_2,$$

where each $\alpha_x \in \mathbb{F}$ and all but finitely many of them are non-zero. Notice that each x that appears in the equation above lies in $D_n(R)$. On the other hand, $w \in D_n(S)$. So, there exist distinct basis elements $z_1 < \cdots < z_t \in Z$ such that

$$\nu_S(z_1) = \cdots = \nu_S(z_t) = n$$

and

$$w = z_1^{b_1} \dots z_t^{b_t} D_{n+1}(S),$$

where $b_1, \dots, b_t \in \{0, \dots, p-1\}$. Hence, by Equation (2.4), we have

$$w - 1 = \sum_{k=1}^{t} b_k (z_k - 1) \text{ modulo } \omega^{n+1}(S) + E_2.$$

Thus,

$$\sum_{k=1}^{t} b_k (z_k - 1) = \sum_{x \in X} \alpha_x (x-1) \text{ modulo } \omega^{n+1}(S) + E_2.$$

So, there exists $u \in E_2$ such that $\sum_{k=1}^{t} b_k (z_k - 1) - \sum_{x \in X} \alpha_x (x-1) + u \in \omega^{n+1}(S)$. We now apply Corollary 3.3 to S. First note that, without loss of generality, we can assume that u is a linear combination of straight monomials of weight at most n. Next observe that, by Corollary 3.3, straight monomials of different degrees and weights less than $n+1$ are linearly independent modulo $\omega^{n+1}(S)$. We deduce that $u = 0$ and

$$\sum_{k=1}^{t} b_k (z_k - 1) - \sum_{x \in X} \alpha_x (x-1) = 0.$$

Since $Z - 1$ is an $\mathbb{F}$-linearly independent subset of $\omega(S)$, it follows that every z_k that appears in the equation above is equal to some $x \in X$ in the equation. However, any such x lies in $D_n(R)$. So each $z_k \in D_n(R)$. Thus, $w \in D_n(R) D_{n+1}(S)$, as required. □

5. Proof of Theorem A

Throughout G is a finite p-group and S is a subgroup of G. Recall from Section 2.2 that $C_i = S \cap D_i(G)$, for every $i \geq 1$, and $\mathfrak{S}$ denotes the graded restricted Lie algebra associated to the $\{C_i\}$ over $\mathbb{F}_p$. We fix a homogeneous basis $\bar{Y}$ of $\mathfrak{S}$ over $\mathbb{F}_p$ and let Y be a fixed set of representatives of $\bar{Y}$. Note that for every $i \geq 1$, C_i/C_{i+1} embeds into D_i/D_{i+1}. So, we can view $\mathfrak{S}$ as an $\mathbb{F}_p$-subalgebra of $\mathcal{L}$ and extend $\bar{Y}$ to an $\mathbb{F}_p$-basis $\bar{Y} \cup \bar{Z}$ of $\mathcal{L}$. We order Y with respect to the D_n. With these notations we have:

Lemma 5.1. *Let G be a finite p-group and S a subgroup of G. Then every element of $\omega(S)$ can be written as a linear combination of straight monomials in Y.*

Proof. First we show that every $s-1$, $s \in S$, is a linear combination of straight monomials in Y. Consider the consecutive quotients

$$C_1/C_2, C_2/C_3, \ldots, C_t/C_{t+1}, 1.$$

Note that there exists $y_1 < \cdots < y_t \in Y$ such that

$$s = \prod_{k=1}^{t} y_k^{a_k},$$

where $1 \leq a_k \leq p-1$, for every k. Thus, by Equation (2.4), $s-1 = \sum_{k=1}^{t} a_k(y_k-1)$ modulo straight monomials of degree at least two in Y. So the assertion is true for every $s-1$, $s \in S$. Hence, $Y-1$ generates $\omega(S)$. Let V_n be the $\mathbb{F}$-vector space spanned by all products $(y_{t_1}-1)\ldots(y_{t_n}-1)$, where $y_{t_1}, \ldots, y_{t_n} \in Y$. We prove the assertion for all elements in V_n, for every $n \geq 1$. Since $\omega(G)$ is nilpotent, there exists a positive integer m such that $V_{m+1} = 0$. Let u and v be monomials in Y such that $u(y_j-1)(y_i-1)v \in V_m$, where $y_i < y_j$. Note that

$$u(y_j-1)(y_i-1)v = u(y_i-1)(y_j-1)v + u[y_j-1, y_i-1]v.$$

But

$$(y_j, y_i) - 1 - [y_j, y_i] = (y_j^{-1}y_i^{-1} - 1)[y_j, y_i].$$

Hence,

$$u[y_j, y_i]v = u((y_j, y_i)-1)v \text{ modulo } V_{m+1}.$$

On the other hand, there exists $y_1 < \cdots < y_t \in Y$ such that $(y_j, y_i) = \prod_{k=1}^{t} y_k^{a_k}$, where $1 \leq a_k \leq p-1$, for every k. Hence

$$u((y_j, y_i)-1)v = u(\sum_{k=1}^{t} a_k(y_k-1))v \text{ modulo } V_{m+1}.$$

Thus, $u[y_j, y_i]v$ lies in $V_{m-1} + V_{m+1}$. So, modulo V_{m-1}, we can transform $u(y_j-1)(y_i-1)v$ into a straight monomial by finitely many transpositions. Hence, V_m is spanned by straight monomials in Y modulo V_{m-1}. Applying this process repeatedly, we deduce that each V_n is spanned by straight monomials in Y modulo V_1. The assertion then follows since, by definition, V_1 is spanned by Y. □

Proposition 5.2. *Let G be a finite p-group and S a subgroup of G. Then, $\omega(S) \cap \omega(G)\omega^n(S) = \omega^{n+1}(S)$, for every positive integer n.*

Proof. Obviously, $\omega^{n+1}(S) \subseteq \omega(S) \cap \omega(G)\omega^n(S)$. So we need to prove the reverse inclusion. Let $\bar{Y}$ be a homogeneous basis of $\mathfrak{S}$ and extend $\bar{Y}$ to a basis $\bar{Y} \cup \bar{Z}$ of $\mathcal{L}$ over $\mathbb{F}_p$. Let Y and Z be fixed sets of representatives of $\bar{Y}$ and $\bar{Z}$, respectively. We order Y with respect to the D_n and assume that

every $y \in Y$ is greater than every $z \in Z$. Let w be a non-zero element in $\omega(S) \cap \omega(G)\omega^n(S)$. Then w is a sum of elements uv, where each u is a straight monomial in $\omega(G)$ and each v lies in $\omega^n(S)$ and is a sum of straight monomials in Y only, by Lemma 5.1. But if u starts with a $y-1$, $y \in Y$, then $uv \in \omega^{n+1}(S)$. Thus, we can assume that

$$w = \sum_{z \in Z} (z-1)v \text{ modulo } \omega^{n+1}(S)$$

where each v is a straight monomial in Y. Since $w \in \omega(S)$, it can be written in terms of the straight monomials in Y only, by Lemma 5.1. It follows from the independence of straight monomials that $\sum_{z \in Z}(z-1)v = 0$. Thus, $w \in \omega^{n+1}(S)$, as required. □

Corollary 5.3. *Let G be a finite p-group and S a subgroup of G. The following statements hold for every integer $n \geq 1$.*

(1) $\omega(S) \cap \omega^n(S)\omega(G) = \omega^{n+1}(S)$.
(2) $\omega(S) \cap \omega^n(S)\mathbb{F}(G) = \omega^n(S)$.

Proof. Part (1) can be established using similar arguments as in Proposition 5.2 by choosing a different ordering on $\bar{Y} \cup \bar{Z}$. To prove (2), we note that $\omega^n(S) \subseteq \omega(S) \cap \omega^n(S)\mathbb{F}(G)$. Now let $w \in \omega(S) \cap \omega^n(S)\mathbb{F}(G)$. Then $w = u + v$ where $u \in \omega^n(S)$ and $v \in \omega^n(S)\omega(G)$. Thus, $v = w - u \in \omega(S) \cap \omega^n(S)\omega(G) = \omega^{n+1}(S)$, by part (1). Hence $w \in \omega^n(S)$ and (2) follows. □

We need a well-known technical lemma, see Lemma 1.4.12 in [12] for example.

Lemma 5.4. *Let H be an arbitrary group, K an arbitrary commutative ring with unity, and KH the corresponding group ring. Let $h_1, \ldots, h_t$ and u be elements of H. Suppose that $u-1$ belongs to the left (or right) ideal of KH generated by $(h_1 - 1), \ldots, (h_t - 1)$. Then u belongs to the subgroup of H generated by $h_1, \ldots, h_t$.*

Theorem A now follows: first note that $G \cap (1+\omega(G)\omega(S)) \subseteq S$, by Lemmas 5.4 and 5.1. Hence,

$$D_{n+1}(S) \subseteq S \cap (1 + \omega(G)\omega^n(S)) = G \cap (1 + \omega(G)\omega^n(S)).$$

Conversely, if $g \in S \cap (1 + \omega(G)\omega^n(S))$ then $g - 1 \in \omega(S) \cap \omega(G)\omega^n(S) = \omega^{n+1}(S)$, by Proposition 5.2. Hence, $g \in D_{n+1}(S)$.

Remark 5.5. *Note that $G \cap (1 + \omega(S)\omega(G)) \subseteq S$, by Lemmas 5.1 and 5.4. We deduce that $D_{n+1}(S) = G \cap (1 + \omega^n(S)\omega(G))$, by Corollary 5.3.*

6. Proof of Theorem B

Proposition 6.1. *Let G be a finite p-group and S a subgroup of G. Then for every positive integer n, we have*

$$\omega(S) \cap \omega^2(G)\omega^n(S) = \omega^{n+2}(S) + \omega(S \cap D_2(G))\omega^n(S).$$

Proof. Let $R = S \cap D_2(G)$. Clearly, $\omega^{n+2}(S)$ and $\omega(R)\omega^n(S)$ are both contained in $\omega^2(G)\omega^n(S)$. Now we prove the reverse inclusion. To do so, let $w \in \omega(S) \cap \omega^2(G)\omega^n(S)$. Let $\bar{Y}_1$ be a basis of S/R and extend it to a basis $\bar{Y}$ of $\mathfrak{S}$ over $\mathbb{F}_p$. Since $\mathfrak{S}$ embeds into $\mathcal{L}$, we can extend $\bar{Y}$ to an $\mathbb{F}_p$-basis $\bar{Y} \cup \bar{Z}$ of $\mathcal{L}$. Let Y_1, Y, Z where $Y_1 \subseteq Y$, be some fixed sets of representatives of $\bar{Y}_1, \bar{Y}, \bar{Z}$, respectively. We order Y with respect to the D_n and assume that every $z \in Z$ is smaller than every $y \in Y$. Since $w \in \omega^2(G)\omega^n(S)$, w is a sum of elements uv, where each u is a straight monomial of weight at least two, by Corollary 3.4, and each v lies in $\omega^n(S)$ and is a linear combination of straight monomials in Y only, by Lemma 5.1. Note that if u starts with a $y-1$, $y \in Y_1$, then uv lies in $\omega^{n+2}(S)$ since u has weight at least two. Also, if u starts with a $y-1$, $y \in Y \setminus Y_1$, then uv lies in $\omega(R)\omega^n(S)$. So,

$$w = \sum uv \text{ modulo } \omega^{n+2}(S) + \omega(R)\omega^n(S)$$

where each u starts with a $z-1$, $z \in Z$. But $w \in \omega(S)$ and so w can be written as a linear combination of straight monomials in Y only, by Lemma 5.1. Hence, by the independence of straight monomials,

$$\sum uv = 0,$$

and thus $w \in \omega^{n+2}(S) + \omega(R)\omega^n(S)$, as required. □

Theorem B is the equality of (1) and (2) in the following theorem.

Theorem 6.2. *Let G be a finite p-group and S a subgroup of G. For every positive integer n, the following subgroups of G coincide.*

(1) $D_{n+2}(S)D_{n+1}(S \cap D_2(G))$,
(2) $G \cap (1 + \omega^2(G)\omega^n(S))$,
(3) $G \cap (1 + \omega^{n+2}(S) + \omega(S \cap D_2(G))\omega^n(S))$.

Proof. Let $R = S \cap D_2(G)$. We first show that

$$D_{n+2}(S)D_{n+1}(R) \subseteq 1 + \omega^2(G)\omega^n(S).$$

We note that, using Equation (2.4), it is enough to show that both $D_{n+2}(S)$ and $D_{n+1}(R)$ are contained in $1 + \omega^2(G)\omega^n(S)$. Clearly, $D_{n+2}(S) \subseteq 1 + \omega^{n+2}(S) \subseteq 1 + \omega^2(G)\omega^n(S)$. Also,

$$D_{n+1}(R) \subseteq 1 + \omega^{n+1}(R) \subseteq 1 + \omega(R)\omega^n(S) \subseteq 1 + \omega^2(G)\omega^n(S).$$

So (1)⊆(2) has been shown and now we show that (2)⊆(3). Let $w \in G \cap (1 + \omega^2(G)\omega^n(S))$. We have

$$w \in G \cap (1 + \omega(G)\omega^n(S)) = D_{n+1}(S),$$

by Theorem A. Thus, by Proposition 6.1, we have

$$w - 1 \in \omega(S) \cap \omega^2(G)\omega^n(S) = \omega^{n+2}(S) + \omega(R)\omega^n(S).$$

Finally, we show that (3)⊆(1). By Proposition 4.2, we have

$$G \cap (1 + \omega^{n+2}(S) + \omega(R)\omega^n(S)) \subseteq D_{n+1}(R)D_{n+2}(S).$$

Note that $D_{n+1}(R)D_{n+2}(S) = D_{n+2}(S)D_{n+1}(R)$, since $R \subseteq S$. The proof is complete. □

References

[1] D.J. Benson, *Representations and cohomology I: Basic representation theory of finite groups and associative algebras*, (Cambridge University Press, 30, Cambridge, 1991).
[2] I.G. Connell, On the group ring, *Canad. J. Math.* **15** (1963), 650–685.
[3] R.H. Fox, Free differential calculus I, *Ann. of Math.* **57** (1953), 547–560.
[4] K.W. Gruenberg, *Cohomological topics in group theory*, (Lecture Notes in Mathematics, 143, Springer, Berlin, 1970).
[5] B. Huppert, N. Blackburn, *Finite groups II*, (Springer-Verlag, 242, Berlin-New York, 1982).
[6] T.C. Hurley, Identifications in a free group, *J. Pure and Applied Algebra* **48** (1987), 249–261.
[7] T.C. Hurley, S.K. Sehgal, Groups related to Fox subgroups, *Comm. Algebra* **28** (2000), no. 2, 1051–1059.
[8] N. Jacobson, *Lie Algebras* (Interscience, New York, 1962).
[9] S.A. Jennings, The group ring of a class of infinite nilpotent groups, *Canad. J. Math.* **7** (1955), 169–187.
[10] R. Lyndon, Problems in combinatorial group theory, in Combinatorial group theory and topology (Alta, Utah, 1984), *Ann. of Math. Stud.* **111** (1987), 3–33 (Princeton Univ. Press).
[11] W. Magnus, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, *Math. Ann.* **111** (1935), no. 1, 259–280.
[12] A.A. Mikhalev, V. Shpilrain, J.-T. Yu, *Combinatorial Methods. Free Groups, Polynomials, Free Algebras*, (CMS Books in Mathematics, Springer, New York, 2004).
[13] I.B.S. Passi, *Group rings and their augmentation ideals*, (Lecture Notes in Mathematics, 715, Springer, Berlin, 1979).
[14] D.G. Quillen, On the associated graded ring of a group ring, *J. Algebra* **10** (1968), 411–418.
[15] D.M. Riley, A. Shalev, Restricted Lie algebras and their envelopes, *Canad. J. Math.* **47** (1995), 146–164.
[16] H.G. Schumann, *ü*ber Moduln und Gruppenbilder, *Math. Ann.* **114** (1937), no. 1, 385–413.
[17] G. E. Wall, Lie methods in group theory, in "Topics in Algebra", (M. F. Newman, Ed.), (Lecture Note in Mathematics, 697, Springer, Berlin, 1978).
[18] I.A. Yunus, A problem of Fox, *Dokl. Akad. Nauk SSSR* **278** (1984), no. 1, 53–56.

Department of Mathematics, University of British Columbia, # 121, 1984 Mathematics Road, Vancouver, BC, Canada, V6T 1Z2

E-mail address: usefi@math.ubc.ca