THE CONTROLLER SUBGROUP OF ONE-SIDED IDEALS IN COMPLETED GROUP RINGS

KONSTANTIN ARDAKOV

ABSTRACT. Let G be a compact p-adic analytic group and let I be a right ideal of the Iwasawa algebra kG. A closed subgroup H of G is said to control I if I can be generated as a right ideal by a subset of kH. We prove that the intersection of any collection of such subgroups again controls I. This has an application to the study of two-sided ideals in nilpotent Iwasawa algebras.

1. Introduction

1.1. **Controlling subgroups.** Let G be a group and let k be a field. A subgroup H of G is said to *control* a right ideal I of the group algebra $k[G]$ if I can be generated as a right ideal by a subset of the subalgebra $k[H]$ of $k[G]$, or equivalently, if $I = (I \cap k[H]) \cdot k[G]$. It is clear that if I is controlled by a proper subgroup H then I is completely determined by a right ideal in a smaller group algebra, namely $I \cap k[H]$. In the study of two-sided ideals in group rings, theorems that assert that under suitable conditions a two-sided ideal is controlled by a known small subgroup of the group are particularly desirable: a canonical example of such a result is Zalesskii's Theorem [11], which asserts that every faithful prime ideal of the group algebra of a finitely generated torsion-free nilpotent group is controlled by the centre of the group.

Let I be a right ideal of $k[G]$ and suppose that I is controlled by H; it can happen that $I \cap k[H]$ is controlled by an even smaller subgroup L of G, and then obviously I will also be controlled by L. Somewhat less obviously, Passman showed that if two different subgroups control I then so does their intersection. A simple argument [9, Lemma 8.1.1] based on an induction on the size of support of an element in the group ring then shows that for any right ideal I of $k[G]$ there is always a unique smallest subgroup of G that controls I; it is called the *controller subgroup* I^χ of I and can be defined simply as the intersection of all possible controlling subgroups. Using this notion, Roseblade [10] essentially classified the prime ideals of $k[G]$ when the group G in question is polycyclic-by-finite.

1.2. **Completed group rings.** Let G be a profinite group, let k be a field and let $k[[G]]$ be the completed group algebra of G with coefficients in k, defined as the inverse limit of the ordinary group rings $k[F]$ as F runs over all continuous finite homomorphic images of G. The purpose of this paper is to develop the notion of controller subgroups for profinite groups. Whenever H is a closed subgroup of G, the completed group algebra $k[[H]]$ is a closed subalgebra of $k[[G]]$ and we say that a closed right ideal I of $k[[G]]$ is *controlled by* H if it can be topologically generated by a subset of $k[[H]]$, or equivalently, if $I = \overline{(I \cap k[[H]]) \cdot k[[G]]}$. In this setting arguments by induction on the size of support are no longer available, and it is no longer clear in this generality that the intersection of two controlling subgroups (or of a descending chain of controlling subgroups) again controls. The naive definition of the controller subgroup as the intersection of all possible controlling subgroups does not immediately seem to lead to an adequate theory.

However, if we restrict our focus to *open* subgroups H then not all is lost. In this case $(I \cap k[[H]]) \cdot k[[G]]$ is automatically closed whenever I is closed, so the definition of "controlling subgroup" coincides with the classical one. In §2 we abstract several key features of Passman's proofs from [9] and show that the intersection of any two open controlling subgroups of an arbitrary ideal I of $k[[G]]$ again controls I, and in §2.7 we define the *controller subgroup* I^χ of I to be the intersection of all open controlling subgroups of I. We show that I^χ has the desirable property that every open subgroup U of G containing I^χ controls I, but were unable to answer the following seemingly basic

Question. *Let I be a closed right ideal of $k[[G]]$. Is I controlled by I^χ?*

1.3. **Iwasawa algebras.** Let p be a prime number and let G be a compact p-adic analytic group: a very special kind of profinite group. If R is a complete discrete valuation ring of characteristic zero with uniformizer p and k is any factor ring of R then the completed group algebra $k[[G]]$ is alternatively known as an *Iwasawa algebra* and is of interest in number theory. We will always denote Iwasawa algebras by $kG = k[[G]]$. Lazard proved in [6] that kG is complete with respect to a filtration whose associated graded ring is Noetherian; standard arguments from [7] then show that every right ideal in kG is finitely generated and closed. The main result of this paper is a positive answer to Question 1.2 for Iwasawa algebras.

Theorem A. *Let G be a compact p-adic analytic group, let I be a right ideal of kG and let H be a closed subgroup of G. Then $I = (I \cap kH)kG$ if and only if $H \supseteq I^\chi$. In particular, $I = (I \cap kI^\chi)kG$.*

The analogous result for left ideals also holds and can in fact be deduced from Theorem A. The proof of the less straightforward "if" direction consists of two main steps. First we show that after passing to a suitable open subgroup of G containing H, we may assume that the homogeneous space G/H is "uniform" in the sense that for some open normal uniform subgroup U of G, G/H is isomorphic as a U-space to U/V for some closed isolated subgroup $V = H \cap U$ of U. We then show that the factor module $kG/(I \cap kH)kG$ is isomorphic as a filtered k-module to the set of power series $(kH/(I \cap kH))[[x_1, \cdots x_e]]$ and run an induction argument which in our setting serves as a kind of substitute to Passman's induction argument appearing in the proof of [9, Lemma 8.1.1].

1.4. **An application to two-sided ideals.** Our motivation for proving Theorem A comes from our research into the structure of two-sided ideals in non-commutative Iwasawa algebras. The basic idea (see [3], [2] and [1]) is to use the adjoint action of G together with the right regular action of kG on itself to prove that under certain hypotheses a two-sided ideal of kG must be controlled by a proper open subgroup of G. In a forthcoming publication [4], we will sharpen this technique and use Theorem A to prove an exact analogue of Zalesskii's Theorem mentioned in §1.1 above for Iwasawa algebras: if k is a field of characteristic p and G is a nilpotent uniform pro-p group then every faithful prime ideal of kG is controlled by the centre of G. Recall that a prime ideal P of kG is said to be *faithful* if G embeds faithfully into the group of units of kG/P.

1.5. **Acknowledgements.** This work was supported by an Early Career Fellowship from the Leverhulme Trust. The author is very grateful to the Trust for providing him the opportunity to focus on his research without too many distractions. The author would also like to thank the organizers of the "New Trends in Noncommutative Algebra" conference for the invitation to speak and for providing excellent working conditions during which a large part of this paper was written. Finally, thanks are due to the referee for making a number of useful suggestions.

2. The controller subgroup for profinite groups

2.1. **Locally constant functions.** Let G be a profinite group and let k be a commutative ring. Recall that a function $f : G \to k$ is *locally constant* if for all $g \in G$ there is an open neighbourhood U of g such that f is constant on U.

Definition. *Let $C^\infty = C^\infty(G, k)$ denote the set of all locally constant functions from G to k.*

C^∞ becomes a unital commutative k-algebra when equipped with pointwise multiplication of functions. Moreover it is a Hopf algebra over k, with comultiplication Δ, antipode S and counit ϵ given by the formulas

$$\Delta(f)(g,h) = f(gh), \quad S(f)(g) = f(g^{-1}) \quad \text{and} \quad \epsilon(f) = f(1)$$

for all $f \in C^\infty$ and all $g, h \in G$.

2.2. **Open subgroups.** The group G acts by left and right translations on C^∞ as follows:

$$(g \cdot f \cdot h)(x) = f(hxg) \quad \text{for all} \quad g, h, x \in G, f \in C^\infty.$$

For any open subgroup U of G (denoted $U \leqslant_o G$), let $k^{G/U}$ denote the set of functions from the (finite) set of left cosets G/U to k, and define

$$\pi_U^* : k^{G/U} \to C^\infty$$

by the formula $\pi_U^* f(g) = f(gU)$. This is clearly an injection, whose image is the set of left U-invariants in C^∞:

$$\pi_U^*(k^{G/U}) = \{f \in C^\infty : f(gU) = f(g) \quad \text{for all} \quad g \in G\} = {}^U C^\infty.$$

Similarly, $k^{U\backslash G}$ can be identified with $C^{\infty\ U}$.

Lemma. $C^\infty = \bigcup_{U \leqslant_o G} {}^U C^\infty = \bigcup_{U \leqslant_o G} C^{\infty\ U}$.

Proof. By symmetry, it is enough to prove the first equality. A locally constant function defines a finite partition of G by open subsets. But any open subset of G is a union of left cosets of an open subgroup of G, so by choosing a sufficiently small open subgroup U we can ensure that the sets in the partition are all unions of left cosets of U. It follows that f is constant on the left cosets of U and hence lies in ${}^U C^\infty$. □

2.3. **Lemma.** If U, V are open subgroups of G, then

$$C^{\infty\ U} \cdot C^{\infty\ V} \quad = \quad C^{\infty\ U\cap V}.$$

Proof. Let δ_{Ug} be the characteristic function of the clopen subset Ug of G. Clearly $\{\delta_{Ug} : g \in G\}$ forms a basis for $C^{\infty\ U}$. Let $W = U \cap V$. Now $Wg = Ug \cap Vg$ for any $g \in G$, so

$$\delta_{Wg}(x) = \delta_{Ug}(x)\delta_{Vg}(x) = (\delta_{Ug} \cdot \delta_{Vg})(x)$$

for all $x \in G$. Hence $\delta_{Wg} = \delta_{Ug} \cdot \delta_{Vg}$. □

2.4. **Module algebras.** Recall [8] that if H is a Hopf algebra over k, then a k-algebra A is a *left H-module algebra* if there exists an action

$$H \otimes A \to A, \quad h \otimes a \mapsto h \cdot a$$

such that

$$h \cdot (ab) = (h_1 \cdot a)(h_2 \cdot b), \quad (hk) \cdot a = h \cdot (k \cdot a) \quad \text{and} \quad 1 \cdot a = a$$

for all $h, k \in H$ and $a, b \in A$. Here we use the sumless Sweedler notation. There is a similar notion of *right* H-module algebra, and the two notions coincide in the case when H is commutative.

2.5. **G-graded algebras.** Recall that if G is a finite group, then the k-algebra A is a *G-graded algebra* if there exists a k-module decomposition $A = \bigoplus_{g\in G} A_g$ of A such that $A_g \cdot A_h \subseteq A_{gh}$ for all $g, h \in G$, and $1 \in A_1$. It is known [8, Example 4.1.7] that A is G-graded if and only if it is a k^G-module algebra.

Definition. *Let G be a profinite group and let A be a k-algebra. We say that A is* G-graded *if for each clopen subset U of G there exists a k-submodule A_U of A such that*

(i) $A = A_{U_1} \oplus A_{U_2} \oplus \cdots \oplus A_{U_n}$ *if $G = U_1 \cup \cdots \cup U_n$ is an open partition of G,*
(ii) $A_U \leqslant A_V$ *if $U \subseteq V$ are clopen subsets of G,*
(iii) $A_U \cdot A_V \subseteq A_{UV}$ *if U, V are clopen subsets of G,*
(iv) $1 \in A_U$ *whenever U is an open subgroup of G.*

Note that conditions (iii) and (iv) imply that A_U is a k-subalgebra of A, for any open subgroup U of G.

Proposition. *Let G be a profinite group, let $C^\infty = C^\infty(G, k)$ and let A be a k-algebra. Then A is a C^∞-module algebra if and only if A is G-graded.*

Proof. ($\Rightarrow$) For each clopen subset U of G, let $\delta_U \in C^\infty$ be its characteristic function, and define $A_U := \delta_U \cdot A$. Since $1 = \delta_{U_1} + \cdots + \delta_{U_n}$ is a decomposition of 1 into a sum of orthogonal idempotents whenever $G = U_1 \cup \ldots \cup U_n$ is an open partition of G, (i) holds. Part (ii) holds because $\delta_V \cdot \delta_U = \delta_U$ whenever $U \subseteq V$. Choose an open normal subgroup W of A such that U and V are unions of cosets of W. Now $k^{G/W}$ is isomorphic to ${}^W C^\infty$, so A is a $k^{G/W}$-module algebra and therefore A is G/W-graded by [8, Example 4.1.7]. Translating this into our notation shows that (iii) and (iv) hold.

($\Leftarrow$) Suppose A is G-graded. If $f \in C^\infty$, we can find an open normal subgroup W of G such that $f \in {}^W C^\infty$ by Lemma 2.2; then f is constant on the cosets of W and we have the decomposition

$$A = \bigoplus_{x\in G/W} A_x.$$

Define the action of f on A by the formula

$$f \cdot \sum_{x\in G/W} a_x = \sum_{x\in G/W} f(x) a_x.$$

This makes sense because f is constant on the cosets of W in G; note also that this definition does not depend on the choice of W. Thus the action of each $\delta_x \in {}^W C^\infty$ is the projection of A onto the A_x-component. Since A is G-graded, it is easily checked that this turns A into a C^∞-module algebra. $\square$

2.6. **Controlling open subgroups.**

Definition. *Let A be a C^∞-module algebra, let I be a right ideal of A, and let $U \leqslant_o G$. We say that U* controls I *if I is a $C^{\infty\ U}$-submodule of A:*

$$C^{\infty\ U} \cdot I \subseteq I.$$

Let $\mathcal{C}(I)$ denote the set of open subgroups of G that control I.

Lemma. *(a) U controls I if and only if $I = \bigoplus_{g \in U\backslash G}(I \cap A_{Ug})$.*
(b) $\mathcal{C}(I)$ is closed under finite intersections.
(c) If $U \in \mathcal{C}(I)$ and $U \leqslant V \leqslant_o G$ then $V \in \mathcal{C}(I)$.

Proof. (a) By Proposition 2.5, we have a direct sum decomposition

$$A = \bigoplus_{g \in U\backslash G} A_{Ug}.$$

The action of δ_{Ug} on A is precisely the projection onto the A_{Ug} component. Since $C^{\infty\ U}$ is spanned by these characteristic functions, U controls I if and only if I contains each component of each element of I in this decomposition. This is equivalent to the statement

$$I = \bigoplus_{g \in U\backslash G} (I \cap A_{Ug}).$$

Part (b) follows from Lemma 2.3, and part (c) is obvious. □

So $\mathcal{C}(I)$ is a *filter* of open subgroups on G.

2.7. **The controller subgroup.**

Definition. *Let A be a C^∞-module algebra and let I be a right ideal of A. The* controller subgroup *of I is*

$$I^\chi := \bigcap \mathcal{C}(I).$$

This is always a closed subgroup of G.

Proposition. *Every open subgroup containing I^χ controls I:*

$$\mathcal{C}(I) = \{U \leqslant_o G : I^\chi \leqslant U\}.$$

Proof. The inclusion $\subseteq$ is obvious, so suppose that $I^\chi \leqslant U \leqslant_o G$. Then

$$G - U \subseteq \bigcup_{V \in \mathcal{C}(I)} (G - V).$$

Since U is open, $G - U$ is closed and hence compact. Each $G - V$ is open since each V is closed, so we can find a finite set $V_1, \ldots, V_n \in \mathcal{C}(I)$ such that

$$G - U \subseteq \bigcup_{i=1}^{n} (G - V_i).$$

Alternatively put, $\cap_{i=1}^n V_i \leqslant U$. Hence U controls I by Lemma 2.6. □

2.8. **Strongly G-graded algebras.**

Definition. *Let G be a profinite group and let A be a G-graded algebra. We say that G is* strongly G-graded *if*

$$A_U \cdot A_V = A_{UV}$$

for all clopen subsets $U, V \subseteq G$.

This is again an obvious generalisation of the well-known notion in the case when G is finite. The following result explains our terminology.

Proposition. *Let A be a strongly G-graded algebra, let I be a right ideal of A and let U be an open subgroup of G. Then I is controlled by U if and only if $I = (I \cap A_U) \cdot A$.*

Proof. ($\Rightarrow$) Fix $g \in G$ and $x \in I \cap A_{Ug}$. Since $g^{-1}Ug$ is an open subgroup of G, $1 \in A_{g^{-1}Ug}$. Now $g^{-1}U \cdot Ug = g^{-1}Ug$ and A is strongly G-graded, so we can find a finite set of elements $a_i \in A_{g^{-1}U}$ and $b_i \in A_{Ug}$ such that $1 = \sum_i a_i b_i$. Now $xa_i \in A_{Ug} \cdot A_{g^{-1}U} \subseteq A_U$ and I is a right ideal, so $x = \sum_i (xa_i) b_i \in (I \cap A_U) \cdot A$. Hence

$$I \cap A_{Ug} \subseteq (I \cap A_U) \cdot A \quad \text{for all} \quad g \in G.$$

As I is controlled by U by assumption,

$$I = \bigoplus_{g \in U \backslash G} (I \cap A_{Ug}) \subseteq (I \cap A_U) \cdot A \subseteq I$$

by Lemma 2.6(a), and therefore $I = (I \cap A_U) \cdot A$.

($\Leftarrow$) Since A is G-graded, $A = \bigoplus_{g \in U \backslash G} A_{Ug}$. Hence

$$I = (I \cap A_U) \cdot A \subseteq \bigoplus_{g \in U \backslash G} (I \cap A_U) \cdot A_{Ug}.$$

But $A_U \cdot A_{Ug} \subseteq A_{Ug}$ and I is a right ideal, so $(I \cap A_U) \cdot A_{Ug} \subseteq I \cap A_{Ug}$ for all $g \in G$, and therefore

$$I \subseteq \bigoplus_{g \in U \backslash G} (I \cap A_U) \cdot A_{Ug} \subseteq \bigoplus_{g \in U \backslash G} (I \cap A_{Ug}).$$

The reverse inclusion is clear, so I is controlled by U — again by Lemma 2.6(a). $\square$

2.9. **Completed group rings.** Let $k[[G]]$ denote the *completed group ring* of G with coefficients in k:

$$k[[G]] := \varprojlim k[G/U]$$

where the inverse limit is taken over all the open normal subgroups U of G. The group G is always contained inside $k[[G]]$ as a subgroup of the group of units of $k[[G]]$.

Lemma. *$k[[G]]$ is a strongly G-graded k-algebra.*

Proof. Let $A = k[[G]]$, and let U be a clopen subset of G. If U is an open subgroup of G, the completed group ring $k[[U]]$ is naturally a subring of $k[[G]]$, so we define $A_U := k[[U]]$. In general, U is a union of cosets of an open normal subgroup W

$$U = Wg_1 \cup \cdots \cup Wg_n$$

and we define $A_U := \sum_{i=1}^n k[[W]] \cdot g_i$. Clearly this is independent of the choice of subgroup W, or coset representatives g_i. It is now straightforward to verify that all the axioms of Definition 2.5 are satisfied, so A becomes a G-graded algebra. The fact that

$$(k[[W]] \cdot g) \cdot (k[[W]] \cdot h) = k[[W]] \cdot gh$$

for any open normal subgroup W of G and any $g, h \in G$ implies that $k[[G]]$ is strongly G-graded. $\square$

We remark that when G is a uniform pro-p group and k is a field of characteristic p, one can show that each *microlocalisation* of the Iwasawa algebra $k[[G]]$ inherits the structure of a strongly G-graded k-algebra from $k[[G]]$. These microlocalisations therefore provide further non-trivial examples of strongly G-graded k-algebras, but we will not discuss them further in this paper.

3. Compact p-adic analytic groups

3.1. **Some group theory.** We refer the reader to [5, Chapter 4] for the definitions and elementary properties of uniform pro-p groups. Let U be a uniform pro-p group and let H be a closed subgroup. Let $U_i = U^{p^{i-1}}$ be the lower p-series of U. Define, for each $i \geqslant 1$,

$$H(i) := \{g \in U \mid g^{p^{i-1}} \in HU_{i+1}\}.$$

Lemma. *(a) $H(i)$ is a subgroup of U for all $i \geqslant 1$.*
(b) $H(i) \leqslant H(i+1)$ for all $i \geqslant 1$.

Proof. (a) Let $g, h \in H(i)$, so that $g^{p^{i-1}}, h^{p^{i-1}} \in HU_{i+1}$. By [5, Theorem 3.6(iv)],

$$(gh)^{p^{i-1}} \equiv g^{p^{i-1}} h^{p^{i-1}} \mod U_{i+1}.$$

So $(gh)^{p^{i-1}} \in HU_{i+1}$ and $gh \in H(i)$. Also $(g^{-1})^{p^{i-1}} = (g^{p^{i-1}})^{-1} \in HU_{i+1}$, and hence $g^{-1} \in H(i)$.

(b) Let $g \in H(i)$, so that $g^{p^{i-1}} \in HU_{i+1}$. By [5, Theorem 3.6(iii)], we can write $g^{p^{i-1}} = hu^{p^i}$ for some $h \in H$ and $u \in U$. Now

$$g^{p^i} = (hu^{p^i})^p \equiv h^p u^{p^{i+1}} \mod (U, U_{i+1}).$$

But $(U, U_{i+1}) \subseteq U_{i+2}$ by definition of the lower p-series, so $g^{p^i} \in HU_{i+2}$ and hence $g \in H(i+1)$. $\square$

Since U/U_2 is a finite group, the ascending chain of subgroups

$$HU_2 = H(1) \leqslant H(2) \leqslant \cdots \leqslant U$$

must terminate:

$$H(\ell) = H(\ell+1) = \cdots$$

for some integer $\ell \geqslant 1$.

3.2. **Proposition.** Let H be a closed subgroup of a uniform pro-p group U. Then there exists an integer $\ell \geqslant 1$, depending only on H, such that $H \cap U_t$ is an isolated uniform subgroup of U_t for all $t \geqslant \ell$.

Proof. Choose ℓ as in §3.1. We first show that $H \cap U_t$ is isolated in U_t whenever $t \geqslant \ell$. Suppose for a contradiction that $g \in U_t \backslash H$ is such that $g^p \in H \cap U_t$.

Since H is a closed subgroup, and the U_i form a fundamental system of neighbourhoods of the identity in U,

$$H = \bigcap_{i=1}^{\infty} HU_i.$$

As $g \in U_t \backslash H$, we can find an integer $m \geqslant t$ such that $g \in HU_m \backslash HU_{m+1}$. Write $g = hz$ for some $h \in H$ and $z \in U_m$, and work modulo U_{m+2}. By [5, Theorem 3.6], the commutator (h, z) lies in U_{m+1}, and the image of U_{m+1} is central in U/U_{m+2} and is an elementary abelian p-group. By the Hall-Petrescu formula [5, Appendix A],

$$g^p = (hz)^p \equiv h^p z^p (h, z)^{\frac{p(p-1)}{2}} \mod U_{m+2}.$$

Now if $p = 2$, we know from [5, Theorem 3.6(i)] that $(h, z) \in U_{m+2}$. So $(h, z)^{\frac{p(p-1)}{2}} \in U_{m+2}$ regardless of whether p is odd or even. Hence

$$z^p \equiv h^{-p} g^p \mod U_{m+2};$$

but $h \in H$ and $g^p \in H$ by assumption so $z^p \in HU_{m+2}$.

Since $z \in U_m$, we may write $z = u^{p^{m-1}}$ for some $u \in U$ by [5, Theorem 3.6(iii)]. So $u^{p^m} = z^p \in HU_{m+2}$ and therefore $u \in H(m+1)$. But $m \geqslant t \geqslant \ell$, so $H(m+1) = H(m)$ and hence $u \in H(m)$. So $z = u^{p^{m-1}} \in HU_{m+1}$, and hence $g = hz \in HU_{m+1}$, a contradiction.

Hence $V_t = H \cap U_t$ is an isolated subgroup of the uniform pro-p group U_t. But now

$$(V_t, V_t) \leqslant (U_t, U_t) \cap V_t \leqslant U_t^p \cap V_t = V_t^p$$

and therefore V_t is a powerful pro-p group. Since V_t is torsion-free, being a subgroup of the torsion-free group U_t, V_t must also be uniform, by [5, Theorem 4.5]. □

3.3. **Extra-powerful groups.** Recall that a uniform group U is said to be *extra-powerful* if $(U,U) \leqslant U^{p^2}$. If U is uniform then $U_n = U^{p^{n-1}}$ is extra-powerful for all $n \geqslant 2$ by [5, Theorem 3.6]. Proposition 3.2 has the following

Corollary. *Let G be a compact p-adic analytic group, and let H be a closed subgroup of G. Then there exists an open normal uniform extra-powerful subgroup U of G such that $H \cap U$ is uniform and isolated in U.*

Proof. By [5, Corollary 8.34], we can find an open normal uniform subgroup W of G, and $H \cap W$ is a closed subgroup of W. By Proposition 3.2, there exists an integer ℓ such that $H \cap W_t = (H \cap W) \cap W_t$ is uniform and isolated in W_t for any $t \geqslant \ell$. Take $U = W_{\ell+1} = W_\ell^p$; it is still open and normal in G, but also extra-powerful. □

3.4. **Notation.** Let H be a closed subgroup of a compact p-adic analytic group G. Using Corollary 3.3, we fix an open normal uniform extra-powerful subgroup U of G such that $V := H \cap U$ is an isolated uniform subgroup of U.

Pick a finite set of coset representatives C for V in H; then

$$H = CV \quad \text{and} \quad HU = CU.$$

Because V is isolated in U, $gV^p \mapsto gU^p$ defines an embedding $V/V^p \hookrightarrow U/U^p$. Let $d := \dim U$ and $e := \dim U - \dim V$. Choose a basis $\{g_1V^p, \ldots, g_{d-e}V^p\}$ for V/V^p over $\mathbb{F}_p$ and extend it to a basis $\{g_1U^p, \ldots, g_dU^p\}$ for U/U^p, say. Since the Frattini subgroup of U is U^p by [5, Lemma 3.4], $\{g_1, \ldots, g_d\}$ is a minimal topological generating set for U such that $\{g_1, \ldots, g_{d-e}\}$ is a minimal topological generating set for V, by [5, Proposition 1.9(iii)].

Let R be a complete discrete valuation ring of characteristic 0 with uniformiser p and residue field $\overline{k}$ of characteristic p, and let k be any quotient of R. The ring k carries a canonical filtration v induced by the normalised discrete valuation on R.

Let $b_i = g_i - 1 \in kU$ and write

$$\mathbf{b}^\alpha := b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_d^{\alpha_d} \in kU \quad \text{for all} \quad \alpha \in \mathbb{N}^d.$$

We will also write

$$\begin{array}{lcllll} c_i & := & b_{d-e+i} & \text{for all} & i = 1, \ldots, e, & \\ \mathbf{c}^\gamma & := & c_1^{\gamma_1} \cdots c_e^{\gamma_e} \in kU & \text{for all} & \gamma \in \mathbb{N}^e, & \text{and} \\ |\alpha| & := & \alpha_1 + \cdots + \alpha_d & \text{for all} & \alpha \in \mathbb{N}^d. & \end{array}$$

Finally, define

$$A_\infty := kH, \quad \text{and} \quad A_n := kHU_n \quad \text{for each} \quad n \geqslant 1\,,$$

where $U_n = U^{p^{n-1}}$ is the lower p-series of U.

3.5. **Formal power series rings.** By the proof of [5, Theorem 7.20], kU can be identified with the set of non-commutative formal power series in the variables $b_1, \ldots, b_d$:

$$kU = \left\{ \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha : \lambda_\alpha \in k \right\}.$$

Since $HU = CU$ by construction and since C is finite, we can also write

$$A_1 = C \cdot kU = \left\{ \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha : \lambda_\alpha \in kC \right\}$$

where kC denotes the free k-module generated by the set C. Let us filter A_1 by powers of the augmentation ideal $\mathfrak{m} := \ker\left(A_1 \to \overline{k}[HU/U]\right)$, and extend the filtration v on k to kC by setting

$$v\left(\sum_{c \in C} \xi_c c\right) = \inf_{c \in C} v(\xi_c).$$

Then $\mathfrak{m} = Cw_U$ where w_U is the unique maximal ideal of kU and

$$\mathfrak{m}^n = Cw_U^n = \left\{ \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha \in A_1 : v(\lambda_\alpha) + |\alpha| \geqslant n \quad \text{for all} \quad \alpha \in \mathbb{N}^d \right\}.$$

Let $\deg : A_1 \to \mathbb{R} \cup \{\infty\}$ be the degree function associated with the $\mathfrak{m}$-adic filtration on A_1; by definition, $\deg(x) = n$ if $x \in \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$ for some n, and $\deg(x) = \infty$ otherwise. It follows from the above expression for $\mathfrak{m}^n$ that

$$\deg\left(\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha\right) = \inf_{\alpha \in \mathbb{N}^d} v(\lambda_\alpha) + |\alpha|.$$

Note that since U is extra-powerful by assumption, the associated graded ring $\operatorname{gr} kU$ of kU with respect to this filtration is commutative. We should also point out that because the function $\alpha \mapsto v(\lambda_\alpha) + |\alpha|$ takes values in $\mathbb{N} \cup \{\infty\}$, the infimum is always attained at some $\alpha \in \mathbb{N}^d$; the same goes for other similar formulas appearing below.

Lemma. *(a) Every element of A_1 can be written uniquely as a non-commutative formal power series in $c_1, \ldots, c_e$ with coefficients in A_∞:*

$$A_1 = \left\{ \sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^\gamma : r_\gamma \in A_\infty \quad \textit{for all} \quad \gamma \in \mathbb{N}^e \right\}.$$

(b) The degree function satisfies

$$\deg\left(\sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^\gamma\right) = \inf_{\gamma \in \mathbb{N}^e} \deg(r_\gamma) + |\gamma|.$$

Proof. (a) By an analysis similar to that applied to A_1 above, now applied to A_∞,

$$A_\infty = C \cdot kV = \left\{ \sum_{\beta \in \mathbb{N}^{d-e}} \lambda_\beta \mathbf{b}^\beta : \lambda_\beta \in kC \right\}.$$

For any $\alpha \in \mathbb{N}^d$, let $\beta \in \mathbb{N}^{d-e}$ and $\gamma \in \mathbb{N}^e$ denote its first $d-e$ and last e components, respectively. Abusing notation slightly, we may write $\alpha = (\beta, \gamma)$, so that $\mathbf{b}^\alpha = \mathbf{b}^\beta \mathbf{c}^\gamma$. Then each element $r = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha$ in A_1 can be written uniquely as

$$r = \sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^\gamma \quad \text{where} \quad r_\gamma = \sum_{\beta \in \mathbb{N}^{d-e}} \lambda_{(\beta,\gamma)} \mathbf{b}^\beta \in A_\infty.$$

We can now compute $\deg(r)$:

$$\begin{aligned} \deg\left(\textstyle\sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^\gamma\right) &= \inf_{\beta \in \mathbb{N}^{d-e}, \gamma \in \mathbb{N}^e} v(\lambda_{(\beta,\gamma)}) + |\beta| + |\gamma| \\ &= \inf_{\gamma \in \mathbb{N}^e} \left(\inf_{\beta \in \mathbb{N}^{d-e}} v(\lambda_{(\beta,\gamma)}) + |\beta|\right) + |\gamma| \\ &= \inf_{\gamma \in \mathbb{N}^e} \deg(r_\gamma) + |\gamma|. \end{aligned}$$

Part (b) follows. □

3.6. **The structure of an induced module.** Let J be a right ideal of A_∞ and let $M_\infty = A_\infty / J$. This cyclic A_∞-module carries the quotient filtration $\deg : M_\infty \to \mathbb{R} \cup \{\infty\}$, defined by

$$\deg(r + J) = \sup_{y \in J} \deg(r + y).$$

Let $x_1, \ldots, x_e$ be formal variables, and let

$$M_1 := M_\infty[[x_1, \ldots, x_e]] = \left\{ \sum_{\alpha \in \mathbb{N}^e} m_\alpha \mathbf{x}^\alpha : m_\alpha \in M_\infty \right\}$$

be the set of all formal power series in the x_i with coefficients in M_∞. We extend the filtration on M_∞ to M_1 by setting $\deg x_i = 1$. More precisely, define

$$\deg\left(\sum_{\alpha \in \mathbb{N}^e} m_\alpha \mathbf{x}^\alpha\right) = \inf_{\alpha \in \mathbb{N}^e} \deg(m_\alpha) + |\alpha|.$$

Proposition. *Define* $\psi : M_\infty[[x_1, \ldots, x_e]] \to A_1 / JA_1$ *by*

$$\psi\left(\sum_{\alpha \in \mathbb{N}^e} (r_\alpha + J)\mathbf{x}^\alpha\right) = \sum_{\alpha \in \mathbb{N}^e} r_\alpha \mathbf{c}^\alpha + JA_1.$$

Then ψ *is an isomorphism of filtered* k*-modules, if* A_1/JA_1 *is given the quotient filtration.*

Proof. Since A_∞ is Noetherian, we can find a finite generating set $\{z_1, \ldots, z_t\}$ for J. In view of Lemma 3.5, we see that JA_1 is exactly the set of formal power series in $c_1, \ldots, c_e$ with coefficients in J:

$$(1) \qquad JA_1 = \left\{ \sum_{i=1}^t z_i \sum_{\alpha \in \mathbb{N}^e} r_{i\alpha} \mathbf{c}^\alpha : r_{i\alpha} \in A_\infty \right\} = \left\{ \sum_{\alpha \in \mathbb{N}^e} y_\alpha \mathbf{c}^\alpha : y_\alpha \in J \right\}.$$

It follows that ψ is a well-defined bijection, and it remains to show that $\deg \psi(m) = \deg m$ for all $m = \sum_{\alpha \in \mathbb{N}^e} (r_\alpha + J)\mathbf{x}^\alpha \in M_\infty[[x_1, \ldots, x_e]]$.

Let $y = \sum_{\alpha \in \mathbb{N}^e} y_\alpha \mathbf{c}^\alpha \in JA_1$ and let the infimum in the definition of $\deg m$ be attained at some $\beta \in \mathbb{N}^e$; thus $\deg m = \deg(r_\beta + J) + |\beta|$. Then using Lemma 3.5(b), we see that

$$\begin{aligned} \deg m &\geqslant \deg(r_\beta + y_\beta) + |\beta| \geqslant \inf_{\alpha \in \mathbb{N}^e} \deg(r_\alpha + y_\alpha) + |\alpha| = \\ &= \deg \textstyle\sum_{\alpha \in \mathbb{N}^e} (r_\alpha + y_\alpha)\mathbf{c}^\alpha = \deg \left(\sum_{\alpha \in \mathbb{N}^e} r_\alpha \mathbf{c}^\alpha + y\right) \end{aligned}$$

for all $y \in JA_1$. Therefore $\deg m \geqslant \deg \psi(m)$ by the definition of the quotient filtration on A_1/JA_1.

To show the reverse inequality, for each $\alpha \in \mathbb{N}^e$ let the supremum in the definition of $\deg(r_\alpha + J)$ be attained at some $y_\alpha \in J$ — this is possible even if $\deg(r_\alpha + J) = \infty$ because then $r_\alpha \in J$ (since the quotient filtration on A_1/J is separated) and we can take $y_\alpha = -r_\alpha$. Then $\sum_{\alpha \in \mathbb{N}^e} y_\alpha \mathbf{c}^\alpha \in JA_1$, so

$$\begin{aligned} \deg \psi(m) &\geqslant \deg \left(\textstyle\sum_{\alpha \in \mathbb{N}^e} r_\alpha \mathbf{c}^\alpha + \sum_{\alpha \in \mathbb{N}^e} y_\alpha \mathbf{c}^\alpha\right) \\ &= \inf_{\alpha \in \mathbb{N}^e} \deg(r_\alpha + y_\alpha) + |\alpha| = \inf_{\alpha \in \mathbb{N}^e} \deg(r_\alpha + J) + |\alpha| = \deg m, \end{aligned}$$

again using Lemma 3.5(b). Hence $\deg \psi(m) = \deg m$ for all $m \in M_\infty[[x_1, \ldots, x_e]]$ and therefore ψ is an isomorphism of filtered k-modules. □

3.7. Let us transport the action of A_1 on A_1/JA_1 to M_1 via the isomorphism ψ of Proposition 3.6. In other words, we turn M_1 into a right A_1-module by setting

$$m \cdot r = \psi^{-1}(\psi(m)r) \quad \text{for all} \quad m \in M_1, r \in A_1.$$

Because ψ is an isomorphism of filtered k-modules, it is actually an isomorphism of filtered A_1-modules.

Lemma. *For each $n \geqslant 1$, define $M_n := M_\infty[[x_1^{p^{n-1}}, \ldots, x_e^{p^{n-1}}]]$. Then*

$$\psi(M_n) = \frac{A_n + JA_1}{JA_1}.$$

Proof. By construction, $HU_n = \left\langle H, g_{d-e+1}^{p^{n-1}}, \ldots, g_d^{p^{n-1}} \right\rangle$. Hence

$$A_n = \left\{ \sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^{p^{n-1}\gamma} : r_\gamma \in A_\infty \quad \text{for all} \quad \gamma \in \mathbb{N}^e \right\},$$

so the image of A_n in A_1/JA_1 is

$$\left\{ \sum_{\gamma \in \mathbb{N}^e} r_\gamma \mathbf{c}^{p^{n-1}\gamma} + JA_1 : r_\gamma \in A_\infty \quad \text{for all} \quad \gamma \in \mathbb{N}^e \right\}.$$

But this is clearly just $\psi(M_n)$. □

3.8. Define $\mathbb{N}_p^e := \{\alpha \in \mathbb{N}^e : \alpha_i < p \text{ for all } i = 1, \ldots, e\}$. Part (b) of the next result will be crucial to the proof of our main theorem.

Proposition. *Fix $n \geqslant 1$.*

(a) For any $\beta \in \mathbb{N}_p^e$ and any $\gamma \in \mathbb{N}^e$,

$$\deg(\mathbf{c}^{p^{n-1}(\beta+p\gamma)} - \mathbf{c}^{p^n\gamma}\mathbf{c}^{p^{n-1}\beta}) > p^{n-1}|\beta + p\gamma|.$$

(b) Let $m_\beta \in M_{n+1}$ for all $\beta \in \mathbb{N}_p^e$. Then

$$\deg\left(\sum_{\beta\in\mathbb{N}_p^e} m_\beta \cdot \mathbf{c}^{p^{n-1}\beta}\right) = \inf_{\beta\in\mathbb{N}_p^e} \deg(m_\beta) + p^{n-1}|\beta|\,.$$

(c) Every element of M_n can be written uniquely in this form:

$$M_n = \bigoplus_{\beta\in\mathbb{N}_p^e} M_{n+1} \cdot \mathbf{c}^{p^{n-1}\beta}.$$

Proof. (a) This follows from the fact that $\operatorname{gr} kU$ is commutative.

(b) Write $m_\beta = \sum_{\gamma\in\mathbb{N}^e} m_{\beta\gamma}\mathbf{x}^{p^n\gamma}$ for some $m_{\beta\gamma} \in M_\infty$, and define

$$m' := \sum_{\beta\in\mathbb{N}_p^e}\sum_{\gamma\in\mathbb{N}^e} m_{\beta\gamma}\mathbf{x}^{p^{n-1}(\beta+p\gamma)} = \sum_{\beta\in\mathbb{N}_p^e}\sum_{\gamma\in\mathbb{N}^e} m_{\beta\gamma} \cdot \mathbf{c}^{p^{n-1}(\beta+p\gamma)}.$$

As β runs over $\mathbb{N}_p^e$ and γ runs over $\mathbb{N}^e$, $\beta + p\gamma$ runs over $\mathbb{N}^e$. So

$$\deg(m') = \inf_{\beta\in\mathbb{N}_p^e}\inf_{\gamma\in\mathbb{N}^e} \deg(m_{\beta\gamma}) + p^{n-1}|\beta + p\gamma|$$

by the definition of the degree function on M_1. On the other hand, $\deg(m_\beta) = \inf_{\gamma\in\mathbb{N}^e} \deg(m_{\beta\gamma}) + p^n|\gamma|$ for all $\beta \in \mathbb{N}_p^e$, so

$$\deg(m') = \inf_{\beta\in\mathbb{N}_p^e} \deg(m_\beta) + p^{n-1}|\beta|\,.$$

Now consider the difference between m' and the element we started off with, namely $m := \sum_{\beta\in\mathbb{N}_p^e} m_\beta \cdot \mathbf{c}^{p^{n-1}\beta}$:

$$m' - m = \sum_{\beta\in\mathbb{N}_p^e}\sum_{\gamma\in\mathbb{N}^e} m_{\beta\gamma} \cdot (\mathbf{c}^{p^{n-1}(\beta+p\gamma)} - \mathbf{c}^{p^n\gamma}\mathbf{c}^{p^{n-1}\beta}).$$

Since M_1 is a filtered A_1-module with respect to deg, part (a) implies that

$$\begin{aligned}\deg(m'-m) &\geqslant \inf_{\beta\in\mathbb{N}_p^e}\inf_{\gamma\in\mathbb{N}^e}\deg(m_{\beta\gamma}) + \deg(\mathbf{c}^{p^{n-1}(\beta+p\gamma)} - \mathbf{c}^{p^{n-1}\beta}\mathbf{c}^{p^n\gamma}) \\ &> \inf_{\beta\in\mathbb{N}_p^e}\inf_{\gamma\in\mathbb{N}^e}\deg(m_{\beta\gamma}) + p^{n-1}|\beta+p\gamma| = \deg(m').\end{aligned}$$

Therefore $\deg(m) = \deg(m') = \inf_{\beta\in\mathbb{N}_p^e} \deg(m_\beta) + p^{n-1}|\beta|$ as claimed.

(c) Let $m = \sum_{\alpha\in\mathbb{N}^e} m_\alpha\mathbf{x}^{p^{n-1}\alpha} \in M_n$. Define, for each $\beta \in \mathbb{N}_p^e$,

$$m_\beta := \sum_{\gamma\in\mathbb{N}^e} m_{\beta+p\gamma}\mathbf{x}^{p^n\gamma} \in M_{n+1}.$$

An argument similar to the one given in the proof of (b) above shows that

$$\deg\left(m - \sum_{\beta\in\mathbb{N}^e} m_\beta \cdot \mathbf{c}^{p^{n-1}\beta}\right) > \deg(m).$$

So m can be approximated arbitarily closely by elements of $\sum_{\beta\in\mathbb{N}_p^e} M_{n+1}\cdot\mathbf{c}^{p^{n-1}\beta}$. The quotient filtration on $(A_{n+1}+JA_1)/JA_1$ is complete, so M_{n+1} is complete with respect to the degree filtration by Lemma 3.7. Hence

$$M_n = \sum_{\beta\in\mathbb{N}_p^e} M_{n+1}\cdot\mathbf{c}^{p^{n-1}\beta}.$$

Finally the sum is direct by part (b) and the fact that the degree filtration on M_{n+1} is separated. □

Corollary. $A_n = \bigoplus_{\beta\in\mathbb{N}_p^e} A_{n+1}\mathbf{c}^{p^{n-1}\beta}$.

Proof. Take $J = 0$ in part (c) of the Proposition. □

3.9. We will need the following rather general Lemma in the proof of our main result.

Lemma. *Let G be a profinite group, let A be a strongly G-graded algebra and let U be an open subgroup of G.*
(a) For any right ideal J of A_U, $(JA)\cap A_U = J$.
(b) If I is a right ideal of A and U controls I, then $(I\cap A_U)^\chi = I^\chi$.

Proof. We will use Propositions 2.7 and 2.8 without further mention in this proof.
(a) This follows from the fact that $A = \bigoplus_{g\in U\backslash G} A_{Ug}$.
(b) Suppose that $V\in\mathcal{C}(I)$. Then $U\cap V\in\mathcal{C}(I)$ by Lemma 2.6(b):

$$I = (I\cap A_{U\cap V})A.$$

Since $A_{U\cap V}\subseteq A_U$, part (a) implies that

$$I\cap A_U = ((I\cap A_{U\cap V})A_U)A\cap A_U = ((I\cap A_U)\cap A_{U\cap V})A_U,$$

so $U\cap V\in\mathcal{C}(I\cap A_U)$. Hence $(I\cap A_U)^\chi \leqslant U\cap V$ for all $V\in\mathcal{C}(I)$ and therefore

$$(I\cap A_U)^\chi \leqslant U\cap I^\chi = I^\chi$$

because U controls I by assumption.

On the other hand, let $V\in\mathcal{C}(I\cap A_U)$; then $I\cap A_U = (I\cap A_V)A_U$ and

$$I = (I\cap A_U)A = (I\cap A_V)A\,.$$

So $V\in\mathcal{C}(I)$ and therefore $I^\chi\leqslant V$ for all $V\in\mathcal{C}(I\cap A_U)$. Hence

$$I^\chi \leqslant (I\cap A_U)^\chi$$

and the result follows. □

3.10. We return to the hypotheses and notation introduced in §3.6 — §3.8, and recall that every element $m \in M_n$ can be uniquely written in the form

$$m = \sum_{\beta \in \mathbb{N}_p^e} m_\beta \cdot \mathbf{c}^{p^{n-1}\beta}$$

for some $m_\beta \in M_{n+1}$ by Proposition 3.8(c).

Lemma. *Let I_1 be a right ideal of $A_1 = kHU$ which is controlled by HU_n for all $n \geqslant 1$. Let $J = I_1 \cap A_\infty$ and let $W = \psi^{-1}(I_1/JA_1)$, an A_1-submodule of M_1. Then*
(a) $W \cap M_n = (W \cap M_{n+1}) \cdot A_n$ for all $n \geqslant 1$, and
(b) if $m = \sum_{\beta \in \mathbb{N}_p^e} m_\beta \cdot \mathbf{c}^{p^{n-1}\beta} \in W \cap M_n$ then $m_\beta \in W \cap M_{n+1}$ for all $\beta \in \mathbb{N}_p^e$.

Proof. (a) By the modular law, $I_1 \cap (A_{n+1} + JA_1) = (I_1 \cap A_{n+1}) + JA_1$. Therefore

$$\psi(W \cap M_{n+1}) = \frac{(I_1 \cap A_{n+1}) + JA_1}{JA_1}$$

and hence

$$\psi\left((W \cap M_{n+1}) \cdot A_n\right) = \frac{(I_1 \cap A_{n+1})A_n + JA_1}{JA_1} \quad .$$

But $(I_1 \cap A_{n+1})A_n = (I_1 \cap A_{n+1})A_1 \cap A_n$ by Lemma 3.9(a), and

$$(I_1 \cap A_{n+1})A_1 \cap A_n = I_1 \cap A_n$$

since I_1 is controlled by HU_{n+1} by assumption, so

$$\psi\left((W \cap M_{n+1}) \cdot A_n\right) = \frac{(I_1 \cap A_n) + JA_1}{JA_1} = \psi(W \cap M_n)\,.$$

Since ψ is an isomorphism by Proposition 3.6, part (a) follows.

(b) Since $W \cap M_n = (W \cap M_{n+1}) \cdot A_n$ by part (a), we can find $w_1, \ldots, w_s \in W \cap M_{n+1}$ and $r_1, \ldots, r_s \in A_n$ such that

$$m = \sum_{i=1}^s w_i \cdot r_i\,.$$

By Corollary 3.8 we can write $r_i = \sum_{\beta \in \mathbb{N}_p^e} r_{i\beta}\mathbf{c}^{p^{n-1}\beta}$ for some $r_{i\beta} \in A_{n+1}$. Now

$$m = \sum_{i=1}^s w_i \cdot \sum_{\beta \in \mathbb{N}_p^e} r_{i\beta}\mathbf{c}^{p^{n-1}\beta} = \sum_{\beta \in \mathbb{N}_p^e}\left(\sum_{i=1}^s w_i \cdot r_{i\beta}\right) \cdot \mathbf{c}^{p^{n-1}\beta}$$

and hence $m_\beta = \sum_{i=1}^s w_i \cdot r_{i\beta} \in W \cap M_{n+1}$ for all $\beta \in \mathbb{N}_p^e$ by Proposition 3.8(c). □

3.11. Proof of Theorem A. ($\Rightarrow$) Let U be an open subgroup containing H and let $f \in C^{\infty\, U}$. Then the action of f on kG defined in Proposition 2.5 is a left kU-module endomorphism of kG, so $f.I = f.((I \cap kH)kG) \subseteq (I \cap kH)f(kG) \subseteq I$. So U controls I by Definition 2.6 and therefore $I^\chi \subseteq U$ for any open subgroup containing H. Since H is closed, it has to contain I^χ by [5, Proposition 1.2(iii)].

($\Leftarrow$) By Corollary 3.3 we can find an open normal uniform subgroup U of G such that $V = H \cap U$ is uniform and isolated in U. Because $I^\chi \leqslant H \leqslant HU$ by assumption, I is controlled by HU by Proposition 2.7, and it will be enough to show that $I_1 = I \cap kHU$ is controlled by H.

Recall the notation of §3.4. Note that $I_1^\chi = I^\chi \leqslant H$ by Lemma 3.9(b), so I_1 is controlled by HU_n for all $n \geqslant 1$ by Proposition 2.7. Let $J = I_1 \cap A_\infty$ and $W = \psi^{-1}(I_1/JA_1)$, an A_1-submodule of M_1. Because ψ is an isomorphism by Proposition 3.6, it will be enough to show that $W = 0$.

Suppose $W \neq 0$ for a contradiction. Pick $0 \neq w_1 \in W$. We will inductively construct a sequence of elements $w_1, w_2, w_3, \dots$ such that:

- $w_n \in W \cap M_n$, for all $n \geqslant 1$,
- $\deg(w_{n+1}) \leqslant \deg w_n$, for all $n \geqslant 1$,
- $\deg(w_{n+1} - w_n) \geqslant p^{n-1}$ for all *sufficiently large* n.

Assume $w_n \in W \cap M_n$ has been constructed. By Proposition 3.8(c) we can write

$$w_n = \sum_{\beta \in \mathbb{N}_p^e} m_\beta^{(n)} \cdot \mathbf{c}^{p^{n-1}\beta}$$

for some unique $m_\beta^{(n)} \in M_{n+1}$. By Proposition 3.8(b), we know that

$$\deg(w_n) = \inf_{\beta \in \mathbb{N}_p^e} \deg(m_\beta^{(n)}) + p^{n-1}|\beta|;$$

let this minimum be attained at $\beta = \beta_n$ and define $w_{n+1} := m_{\beta_n}^{(n)}$. Thus

$$\deg(w_{n+1}) = \deg(w_n) - p^{n-1}|\beta_n| \tag{2}$$

and $w_{n+1} \in W \cap M_{n+1}$ by Lemma 3.10(b). Thus the first two conditions are satisfied. Summing equation (2) from $n = 1$ to $n = r$ shows that

$$\deg(w_{r+1}) = \deg(w_1) - \sum_{n=1}^{r} p^{n-1}|\beta_n|\,.$$

Since $\deg(w_{r+1})$ is always non-negative by construction, this forces β_n to be 0 for all sufficiently large n. But then

$$w_{n+1} - w_n = \sum_{0 \neq \beta \in \mathbb{N}_p^e} m_\beta^{(n)} \cdot \mathbf{c}^{p^{n-1}\beta}$$

has degree at least p^{n-1} by Proposition 3.8(b), so our third condition also holds.

Since $\deg(w_{n+1} - w_n) \to \infty$ as $n \to \infty$ and M_1 is complete, the limit

$$w := \lim_{n \to \infty} w_n$$

exists and is non-zero because $\deg(w_n) \leqslant \deg(w_1) < \infty$ for all $n \geqslant 1$. Fix $r \geqslant 1$; then $w_n \in M_n \subseteq M_r$ for all $n \geqslant r$. As M_r is a closed subset of M_1, we deduce that $w \in M_r$ for all $r \geqslant 1$, and therefore

$$0 \neq w \in \bigcap_{r=1}^{\infty} M_\infty[[x_1^{p^{r-1}}, \dots, x_e^{p^{r-1}}]] = M_\infty.$$

Now I_1/JA_1 is a closed submodule of A_1/JA_1 and ψ is a homeomorphism, so W is a closed submodule of M_1 and therefore $w = \lim_{n\to\infty} w_n \in W$. This shows that $W \cap M_\infty \neq 0$, which is absurd because

$$\psi(W \cap M_\infty) = \frac{I_1}{JA_1} \cap \frac{A_\infty + JA_1}{JA_1} = \frac{(I_1 \cap A_\infty) + JA_1}{JA_1} = 0$$

by the modular law and the fact that $I_1 \cap A_\infty = J$. □

References

[1] K. Ardakov and S. J. Wadsley. Γ-invariant ideals in Iwasawa algebras. *J. Pure Appl. Algebra*, 213(9):1852–1864, 2009.

[2] K. Ardakov, F. Wei, and J. J. Zhang. Non-existence of reflexive ideals in Iwasawa algebras of Chevalley type. *J. Algebra*, 320(1):259–275, 2008.

[3] K. Ardakov, F. Wei, and J. J. Zhang. Reflexive ideals in Iwasawa algebras. *Adv. Math.*, 218(3):865–901, 2008.

[4] Konstantin Ardakov. Prime ideals in nilpotent Iwasawa algebras. *in preparation*.

[5] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[6] Michel Lazard. Groupes analytiques p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (26):389–603, 1965.

[7] H. Li and F. Van Oystaeyen. *Zariskian filtrations*. Kluwer Academic Publishers, 1996.

[8] Susan Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1993.

[9] Donald S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co. Inc., Melbourne, FL, 1985. Reprint of the 1977 original.

[10] J. E. Roseblade. Prime ideals in group rings of polycyclic groups. *Proc. London Math. Soc. (3)*, 36(3):385–447, 1978.

[11] A. E. Zalesskiĭ. On subgroups of rings without divisors of zero. *Dokl. Akad. Nauk BSSR*, 10:728–731, 1966.

University of Nottingham,
School of Mathematical Sciences,
University Park,
Nottingham NG7 2RD

E-mail address:
konstantin.ardakov@nottingham.ac.uk