REFLEXIVE IDEALS IN IWASAWA ALGEBRAS

K. ARDAKOV, F. WEI AND J. J. ZHANG

Abstract. Let G be a torsionfree compact p-adic analytic group. We give sufficient conditions on p and G which ensure that the Iwasawa algebra Ω_G of G has no non-trivial two-sided reflexive ideals. Consequently, these conditions imply that every nonzero normal element in Ω_G is a unit. We show that these conditions hold in the case when G is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ and p is arbitrary. Using a previous result of the first author, we show that there are only two prime ideals in Ω_G when G is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$: the zero ideal and the unique maximal ideal. These statements partially answer some questions asked by the first author and Brown.

0. Introduction

0.1. **Motivation.** The Iwasawa theory for elliptic curves in arithmetic geometry provides the main motivation for the study of Iwasawa algebras Λ_G, for example when G is a certain subgroup of the p-adic analytic group $\mathrm{GL}_2(\mathbb{Z}_p)$ [CSS, Section 8]. Homological and ring-theoretic properties of these Iwasawa algebras are useful for understanding the structure of the Pontryagin dual of Selmer groups [OV, V3] and other modules over the Iwasawa algebras. Several recent papers [A, AB1, AB2, V1, V2] are devoted to ring-theoretic properties of the Iwasawa algebras. One central question in this research direction is whether there are any non-trivial prime ideals in $\Omega_G = \Lambda_G/p\Lambda_G$, when G is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, see [A, Question, p.197]. The aim of this paper is to answer this question and a few other related open questions.

An Iwasawa algebra over any uniform subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ is local and extremely noncommutative since the only nonzero prime ideal is the maximal ideal by one of our main results, Theorem C. These algebras give rise to a class of so-called just infinite-dimensional algebras. On the other hand, their associated graded rings are commutative polynomial rings and hence Iwasawa algebras share many good properties with commutative rings. This class of algebras is very interesting from the ring-theoretic point of view and deserves further investigation.

0.2. **Definitions.** Throughout we fix a prime integer p. Let $\mathbb{Z}_p$ be the ring of p-adic integers and let $\mathbb{F}_p$ be the field $\mathbb{Z}/(p)$. We refer to the book [DDMS] for the definition and basic properties of a p-adic analytic group and related material. Let G be a compact p-adic analytic group. The *Iwasawa algebra* of G (or the *completed group algebra* of G over $\mathbb{Z}_p$) is defined to be

$$\Lambda_G := \varprojlim \mathbb{Z}_p[G/N],$$

2000 *Mathematics Subject Classification.* 16L30, 16P40.

Key words and phrases. Iwasawa algebra, uniform pro-p group, reflexive ideal, normal element, microlocalisation.

where the inverse limit is taken over the open normal subgroups N of G [La, p.443], [DDMS, p.155]. A closely related algebra is $\Omega_G := \Lambda_G/p\Lambda_G$, whose alternative definition is

$$\Omega_G := \varprojlim \mathbb{F}_p[G/N].$$

For simplicity, the algebra Ω_G is also called the *Iwasawa algebra* of G (or the *completed group algebra* of G over $\mathbb{F}_p$). We refer to [AB1] for some basic properties of Λ_G and Ω_G and to the articles [CSS, CFKSV, V1, V2] for general readings about Iwasawa algebras and their modules.

In this paper, we deal entirely with Ω_G. For a treatment of the implications of our results for the Iwasawa algebra Λ_G, see [A2].

0.3. **Reflexive ideals.** Let A be any algebra and M be a left A-module. We call M *reflexive* if the canonical map

$$M \to \mathrm{Hom}_{A^{\mathrm{op}}}(\mathrm{Hom}_A(M, A), A)$$

is an isomorphism. A reflexive right A-module is defined similarly. We will call a two-sided ideal I of A *reflexive* if it is reflexive as a right and as a left A-module.

For the rest of the introduction we assume that G is torsionfree, in which case Ω_G is an Auslander regular domain. Here is our first main result.

Theorem A. *Let G be a torsionfree compact p-adic analytic group whose $\mathbb{Q}_p$-Lie algebra $\mathcal{L}(G)$ is split semisimple over $\mathbb{Q}_p$. Suppose that $p \geqslant 5$ and that $p \nmid n$ in the case when $\mathfrak{sl}_n(\mathbb{Q}_p)$ occurs as a direct summand of $\mathcal{L}(G)$. Then Ω_G has no non-trivial two-sided reflexive ideals.*

The proof of Theorem A is based on a result from [AWZ]. For a few small p, there are some extra difficulties to be dealt with; hence we exclude these primes from consideration. We believe that these restrictions on p are not really necessary.

0.4. **Normal elements.** Recall that an element w of a ring A is said to be *normal* if $wA = Aw$. The first author and Brown [AB1, Question K] asked whether under hypotheses on G similar to the ones in Theorem A any nonzero normal element of Ω_G must be a unit. Because every nonzero normal element $w \in \Omega_G$ gives rise to a nonzero reflexive two-sided ideal $w\Omega_G$, Theorem A implies

Theorem B. *Under the same hypotheses as in Theorem A, every nonzero normal element of Ω_G is a unit.*

Theorem B partially answers the open question [AB1, Question K].

0.5. **Iwasawa algebras over subgroups of $\mathrm{SL}_2(\mathbb{Z}_p)$.** Another open question [AB1, Question J] is, under hypotheses similar to those in Theorem A, whether there are any non-trivial prime ideals in Ω_G? This question is particularly interesting when G an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. Using [A, Theorem A] we can prove

Theorem C. *Let G be an open torsionfree subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. Then every prime ideal in Ω_G is either zero or maximal.*

The proof of Theorem C is independent of [AWZ].

0.6. **A key step in proof.** To prove the theorems above we have to overcome several technical difficulties which seem unrelated to the main theorems. The proof is divided into several steps and we only mention one key step: a control theorem for reflexive ideals.

Theorem (Theorem 5.3)**.** *Let (A, A_1) be a Frobenius pair satisfying the derivation hypothesis, such that* $\operatorname{gr} A$ *and* $\operatorname{gr} A_1$ *are UFDs. Let I be a reflexive two-sided ideal of A. Then $I \cap A_1$ is a reflexive two-sided ideal of A_1 and I is controlled by A_1:*

$$I = (I \cap A_1) \cdot A.$$

All undefined terms will be explained later. As an example we may take (A, A_1) to be (Ω_G, Ω_{G^p}). We will verify that the derivation hypothesis holds for certain groups G, and the main theorems then follow from the control theorem and induction. This control theorem is in fact the heart of the paper, on which all our main results are dependent. The control theorem should be useful for studying Iwasawa algebras over other classes of groups, such as the nilpotent or solvable groups.

0.7. **A field extension.** An algebra A over a field is called *just infinite-dimensional* if it is infinite-dimensional and every nonzero ideal in A is finite codimensional. This is analogous to the notion of just infinite groups, also known as the almost simple groups. Theorem C assures us of a large class of just infinite-dimensional algebras with good homological properties.

Several researchers are interested in just infinite-dimensional algebras over an algebraically closed field (or an infinite field in general) [BFP, FS]. For ring-theoretic considerations we introduce another algebra closely related to Ω_G. Let K be a field of characteristic p (in particular, K could be the algebraic closure of $\mathbb{F}_p$). Define

$$KG := K[[G]] := \varprojlim K[G/N],$$

where the inverse limit is taken over the open normal subgroups N of G. This algebra can be obtained by taking a completion of the algebra $\Omega_G \otimes_{\mathbb{F}_p} K$ with respect to the filtration $\{\mathfrak{m}^n \otimes_{\mathbb{F}_p} K \mid n \geqslant 0\}$ where $\mathfrak{m}$ is the Jacobson radical of Ω_G. Under the same hypotheses, Theorems A, B and C hold for KG.

1. Preliminaries

1.1. **Fractional ideals.** . Let R be a noetherian domain. It is well-known that R has a skewfield of fractions Q. Recall that a right R-submodule I of Q is said to be a *fractional right R-ideal* if I is nonzero and $I \subseteq uR$ for some nonzero $u \in Q$. When the ring R is understood, we simply say that I is a fractional right ideal. Fractional left R-ideals are defined similarly. If I is a fractional right ideal, then

$$I^{-1} := \{q \in Q : qI \subseteq R\}$$

is a fractional left ideal and there is a similar definition of I^{-1} for fractional left ideals I. Let $I^* := \operatorname{Hom}_R(I, R)$. This is a left R-module and there is a natural isomorphism $\eta_I : I^{-1} \to I^*$ that sends $q \in I^{-1}$ to the right R-module homomorphism induced by left multiplication by q.

1.2. **Reflexive right ideals.** Let I be a fractional right ideal and let $\overline{I} := (I^{-1})^{-1}$ be the *reflexive closure* of I. This is also a fractional right ideal which contains I. Recall that I is said to be *reflexive* if $I = \overline{I}$, or equivalently if the canonical map $I \to I^{**}$ is an isomorphism.

Proposition. *Let $R \hookrightarrow S$ be a ring extension such that R is noetherian and S is flat as a left and right R-module. Then there is a natural isomorphism*

$$\psi^i_M : S \otimes_R \operatorname{Ext}^i_R(M, R) \xrightarrow{\cong} \operatorname{Ext}^i_S(M \otimes_R S, S)$$

for all finitely generated right R-modules M and all $i \geqslant 0$. A similar statement holds for left R-modules. If in addition S is a noetherian domain, then
(a) $\overline{J \cdot S} = \overline{J} \cdot S$ for all right ideals J of R,
(b) if I is a reflexive right ideal of S, then $I \cap R$ is a reflexive right ideal of R.

Proof. Let M be a finitely generated right R-module and define

$$\psi_M : S \otimes_R \operatorname{Hom}_R(M, R) \to \operatorname{Hom}_S(M \otimes_R S, S)$$

by the rule $\psi_M(s \otimes f)(m \otimes t) = sf(m)t$ for all $s \in S, f \in \operatorname{Hom}_R(M, R), m \in M$ and $t \in R$. This gives a natural transformation

$$\psi : S \otimes_R \operatorname{Hom}_R(-, R) \to \operatorname{Hom}_S(- \otimes_R S, S)$$

such that ψ_{R^n} is an isomorphism for all $n \geqslant 0$. Now let $P_\bullet \to M \to 0$ be a projective resolution of M consisting of finitely generated free R-modules. Using the flatness assumptions on S, we see that

$$\begin{aligned} \operatorname{Ext}^i_S(M \otimes_R S, S) = H^i(\operatorname{Hom}_S(P_\bullet \otimes_R S, S)) &\cong H^i(S \otimes_R \operatorname{Hom}_R(P_\bullet, R)) = \\ = S \otimes_R H^i(\operatorname{Hom}_R(P_\bullet, R)) &= S \otimes_R \operatorname{Ext}^i_R(M, R), \end{aligned}$$

for all i, as required.

(a) The division ring of fractions Q of R embeds naturally into the division ring of fractions of S. Let I be a fractional right R-ideal, so that $I \subseteq uR$ for some $u \in Q\backslash 0$. Then $IS \subseteq uS$, so IS is a fractional right S-ideal. Now I^{-1} is a fractional left R-ideal and $I^{-1}I \subseteq R$, so

$$(SI^{-1})(IS) \subseteq SRS \subseteq S$$

and hence $SI^{-1} \subseteq (IS)^{-1}$. Consider the following diagram of left S-modules:

$$\begin{tikzcd} S \otimes_R I^{-1} \arrow[r, "\alpha"] \arrow[d, "1\otimes\eta_I"'] & SI^{-1} \arrow[r, "\iota"] & (IS)^{-1} \arrow[d, "\eta_{IS}"] \\ S \otimes_R I^* \arrow[r, "\psi_I"'] & (I \otimes_R S)^* & (IS)^*. \arrow[l, "\beta"] \end{tikzcd}$$

Here ι denotes the inclusion of SI^{-1} into $(IS)^{-1}$ and α and β are the obvious maps. A straightforward check shows that this diagram commutes. By the remarks made in §1.1 the maps η_I and η_{IS} are isomorphisms. Since S is a flat left R-module, α is an isomorphism and similarly β is an isomorphism. Now ψ_I is an isomorphism by the first part, so ι must also be an isomorphism. We deduce that $SI^{-1} = (IS)^{-1}$ for all fractional right R-ideals I. By symmetry, $I^{-1}S = (SI)^{-1}$ for all fractional left R-ideals I.

We may assume that J is nonzero, so that J is a fractional right ideal, and hence

$$\overline{J \cdot S} = ((JS)^{-1})^{-1} = (SJ^{-1})^{-1} = (J^{-1})^{-1}S = \overline{J} \cdot S$$

as required.

(b) Again, we may assume that $I \cap R$ is a nonzero, so that $I \cap R$ is a fractional right ideal. Clearly $I \cap R \subseteq \overline{I \cap R}$. Using part (a) we have

$$\overline{I \cap R} \subseteq \overline{(I \cap R) \cdot S} \subseteq \overline{I} = I,$$

but $\overline{I \cap R} \subseteq \overline{R} = R$ and hence $\overline{I \cap R} \subseteq I \cap R$. The result follows. $\square$

1.3. **Pseudo-null modules.** Let R be an arbitrary ring and M be an R-module. We denote $\mathrm{Ext}^j_R(M,R)$ by $E^j(M)$. Recall [CSS, Lemma 2.1 and Definition 2.5] that an R-module M is said to be *pseudo-null* if $E^0(N) = E^1(N) = 0$ for any submodule N of M. Part (b) of the Proposition below shows that this extends the notion of pseudo-zero modules in the sense of [BCA, Chapter VII, §4.4, Definition 2].

Lemma. *Let $0 \to X \to Y \to Z \to 0$ be an exact sequence of R-modules. Then Y is pseudo-null if and only if X and Z are pseudo-null.*

Proof. This appears in [CSS, §2] and follows easily from the long exact sequence of cohomology. $\square$

The following alternative characterisation of pseudo-null modules over noetherian domains is well-known, but we include a proof for the convenience of the reader.

Proposition. *Let R be a noetherian domain and let M be a finitely generated R-module.*
(a) M is pseudo-null if and only if $\mathrm{ann}(x)^{-1} = R$ for all $x \in M$.
(b) If R is commutative then M is pseudo-null if and only if $\mathrm{Ann}_R(M)^{-1} = R$.

Proof. (a) Suppose M is pseudo-null and let $x \in M$. The short exact sequence $0 \to \mathrm{ann}(x) \to R \to xR \to 0$ induces the long exact sequence

$$0 \to E^0(xR) \to E^0(R) \to E^0(\mathrm{ann}(x)) \to E^1(xR) \to 0$$

and $E^0(xR) = E^1(xR) = 0$ since M is pseudo-null. Hence $\mathrm{ann}(x)^{-1} = R^{-1} = R$ by the remarks made in §1.1.

Conversely, suppose that $\mathrm{ann}(x)^{-1} = R$ for all $x \in M$. It will be enough to show that $E^0(M) = E^1(M) = 0$. Let $N = yR$ be a quotient of a cyclic submodule xR of M. Then $\mathrm{ann}(x) \subseteq \mathrm{ann}(y)$, so $R \subseteq \mathrm{ann}(y)^{-1} \subseteq \mathrm{ann}(x)^{-1} = R$. Hence $\mathrm{ann}(y)^{-1} = R$ and the above long exact sequence shows that $E^0(N) = E^1(N) = 0$.

Because M is finitely generated, M is an extension of finitely many modules $M_1, \ldots, M_k$ such that each M_i is isomorphic to a quotient of a cyclic submodule of M. The result now follows from a long exact sequence.

(b) Suppose that $\mathrm{Ann}_R(M)^{-1} = R$. Since $\mathrm{Ann}_R(M) \subseteq \mathrm{ann}(x)$ for all $x \in M$, part (a) implies that M must be pseudo-null.

Conversely, suppose that M is pseudo-null and let $x_1, \ldots, x_k$ be a generating set for M. Since M is pseudo-null, $\mathrm{ann}(x_i)^{-1} = R$ for all i. Since R is commutative, $\mathrm{Ann}_R(M)$ contains the product $\mathrm{ann}(x_1) \cdots \mathrm{ann}(x_k)$ and it follows easily that $\mathrm{Ann}_R(M)^{-1} = R$. $\square$

1.4. **Unique factorisation domains.**

Lemma. *Let R be a commutative noetherian unique factorisation domain (UFD) and I be a nonzero ideal of R. Then $\overline{I} = xR$ for some $x \in R$ and xR/I is pseudo-null. Moreover, if R is a graded ring and I is a graded ideal, then x is homogeneous.*

Proof. By [BCA, Chapter VII, §4.2, Example 2 and §3.1, Definition 1], every reflexive ideal of R is necessarily principal. Hence $\overline{I} = xR$ for some $x \in R$.

Now let $J = \mathrm{Ann}_R(xR/I) = x^{-1}I$ and suppose that $q \in J^{-1}$. Then $qJ = qx^{-1}I \subseteq R$ and so $qx^{-1} \in I^{-1} = \overline{I}^{-1} = x^{-1}R$. Therefore $q \in R$ and $J^{-1} = R$. Hence xR/I is pseudo-null by Proposition 1.3 (b).

Suppose finally that R and I are graded. Then we can find a nonzero homogeneous element $y \in I$. Since $I \subseteq xR$ we see that x is a factor of y. Because R is a domain, homogeneous elements can only have homogeneous factors, so x is necessarily homogeneous. □

1.5. **Filtered rings.** A *filtered ring* is a ring R with a filtration $FR = \{F_nR : n \in \mathbb{Z}\}$ consisting of additive subgroups of R such that $R = \bigcup_{n\in\mathbb{Z}} F_nR$, $1 \in F_0R$, $F_nR \subseteq F_{n+1}R$ and $F_nRF_mR \subseteq F_{n+m}R$ for all $n, m \in \mathbb{Z}$. Our filtrations will always be *separated*, meaning that $\bigcap_{n\in\mathbb{Z}} F_nR = 0$. If x is a nonzero element of R, there exists a unique $n \in \mathbb{Z}$, which is called the *degree* of x and written $n = \deg x$, such that $x \in F_nR - F_{n-1}R$.

The abelian group $\mathrm{gr}\, R := \oplus_{n\in\mathbb{Z}} F_nR/F_{n-1}R$ becomes a graded ring with multiplication induced by that of R and is called the *associated graded ring* of R with respect to FR. The *principal symbol* of a nonzero element x of R of degree n is

$$\mathrm{gr}\, x := x + F_{n-1}R \in F_nR/F_{n-1}R \subseteq \mathrm{gr}\, R.$$

If $\mathrm{gr}\, R$ is a domain then $\mathrm{gr}(xy) = \mathrm{gr}(x)\,\mathrm{gr}(y)$ for any nonzero $x, y \in R$.

The *Rees ring* of R (with respect to the filtration FR) is the following subring of the Laurent polynomial ring $R[t, t^{-1}]$:

$$\widetilde{R} := \bigoplus_{n\in\mathbb{Z}} t^n F_nR.$$

The Rees ring comes equipped with two natural surjective ring homomorphisms $\pi_1 : \widetilde{R} \to R$ and $\pi_2 : \widetilde{R} \to \mathrm{gr}\, R$ which send the indeterminate t to one and zero, respectively. The map π_1 is sometimes called *dehomogenisation.*

2. Frobenius Pairs

2.1. **The classical Frobenius map.** Let K be a field of characteristic p and let B be a commutative K-algebra. Then the Frobenius map $x \mapsto x^p$ is a ring endomorphism of B and gives an isomorphism of B onto its image

$$B^{[p]} := \{b^p : b \in B\}$$

in B provided B is reduced. We remark at this point that any derivation $d : B \to B$ is $B^{[p]}$-linear:

$$d(a^pb) = a^pd(b) + pa^{p-1}d(b) = a^pd(b)$$

for all $a, b \in B$.

2.2. **Frobenius pairs.** Let t be a positive integer. Whenever $\{y_1, \ldots, y_t\}$ is a t-tuple of elements of B and $\alpha = (\alpha_1, \ldots, \alpha_t)$ is a t-tuple of nonnegative integers, we define

$$\mathbf{y}^\alpha = y_1^{\alpha_1} \cdots y_t^{\alpha_t}.$$

Let $[p-1]$ denote the set $\{0, 1, \ldots, p-1\}$ and let $[p-1]^t$ be the product of t copies of $[p-1]$.

Definition. *Let A be a complete filtered K-algebra and let A_1 be a subalgebra of A. We always view A_1 as a filtered subalgebra of A, equipped with the subspace filtration $F_nA_1 := F_nA \cap A_1$. We say that (A, A_1) is a* Frobenius pair *if the following axioms are satisfied:*

(*i*) *A_1 is closed in A,*
(*ii*) *$\mathrm{gr}\, A$ is a commutative noetherian domain, and we write $B = \mathrm{gr}\, A$,*
(*iii*) *the image B_1 of $\mathrm{gr}\, A_1$ in B satisfies $B^{[p]} \subseteq B_1$, and*
(*iv*) *there exist homogeneous elements $y_1, \ldots, y_t \in B$ such that*

$$B = \bigoplus_{\alpha \in [p-1]^t} B_1 \mathbf{y}^\alpha.$$

Remark. It is easy to see that A_1 is closed in A if and only if the subspace filtration $\{F_nA_1\}_{n\in\mathbb{Z}}$ on A_1 is complete.

The canonical example to keep in mind is given by Iwasawa algebras of uniform pro-p groups G. We will show in §6.6 that (KG, KG^p) is always a Frobenius pair.

We will now deduce some consequences of the axioms.

2.3. **The structure of A as an A_1-module.** Let (A, A_1) be a Frobenius pair. We can view A as an A_1-bimodule. Let us choose elements $u_1, \ldots, u_t \in A$ such that $\mathrm{gr}\, u_i = y_i$ for all i and set $\mathbf{u}^\alpha := u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ for all $\alpha \in \mathbb{N}^t$.

Lemma. *The A is a free left and right A_1-module with basis $\{\mathbf{u}^\alpha : \alpha \in [p-1]^t\}$:*

$$A = \bigoplus_{\alpha \in [p-1]^t} A_1 \cdot \mathbf{u}^\alpha = \bigoplus_{\alpha \in [p-1]^t} \mathbf{u}^\alpha \cdot A_1.$$

Proof. By symmetry it is sufficient to prove the statement about left modules, say. Suppose for a contradiction that $\sum_{\alpha\in T} a_\alpha \mathbf{u}^\alpha = 0$, where $\{a_\alpha \in A_1 : \alpha \in T\}$ is some collection of nonzero elements and $T \subseteq [p-1]^t$ is a nonempty indexing set. Let n denote the maximum of the degrees of the $a_\alpha \mathbf{u}^\alpha$ and let S denote the subset of T consisting of those indices α where this maximum is attained. Then

$$\left(\sum_{\alpha\in T} a_\alpha \mathbf{u}^\alpha\right) + F_{n-1}A = \sum_{\alpha \in S} \mathrm{gr}\, a_\alpha \cdot \mathbf{y}^\alpha = 0,$$

which is contradictory to Definition 2.2(iv). Thus the sum $M := \sum_{\alpha\in[p-1]^t} A_1 \cdot \mathbf{u}^\alpha$ is direct.

Now M is a filtered A_1-submodule of A and $\mathrm{gr}\, M$ coincides with $\mathrm{gr}\, A$. Since A_1 is complete, M is equal to A and the result follows. $\square$

2.4. **Derivations.** Let $B_1 \subseteq B$ be commutative rings of characteristic p, such that $B^{[p]} \subseteq B_1$ and

$$B = \bigoplus_{\alpha\in[p-1]^t} B_1 \mathbf{y}^\alpha$$

for some elements $y_1, \ldots, y_t$ of B.

Fix $j = 1, \ldots, t$ and let ϵ_j denote the t-tuple of integers having a 1 in the j-th position and zeros elsewhere. We define a B_1-linear map $\partial_j : B \to B$ by setting

$$\partial_j \left(\sum_{\alpha\in[p-1]^t} u_\alpha \mathbf{y}^\alpha\right) := \sum_{\substack{\alpha\in[p-1]^t \\ \alpha_j>0}} \alpha_j u_\alpha \mathbf{y}^{\alpha-\epsilon_j}.$$

Let $\mathcal{D} := \mathrm{Der}_{B_1}(B)$ denote the set of all B_1-linear derivations of B. We now collect some very useful results about $\mathcal{D}$ and its natural action on B. In particular, we can give a complete characterisation of the $\mathcal{D}$-stable ideals of B.

Proposition. *(a) The map ∂_j is a B_1-linear derivation of B for each j.*
(b) $\mathcal{D} = \bigoplus_{j=1}^t B\partial_j$.
(c) For any $x \in B$, $\mathcal{D}(x) = 0$ if and only if $x \in B_1$.
(d) An ideal $I \subseteq B$ is $\mathcal{D}$-stable if and only if it is controlled by B_1:

$$I = (I \cap B_1)B.$$

Proof. (a) Because the y_i's generate B as a B_1-algebra and ∂_j is B_1-linear by definition, to show that ∂_j is a derivation it is sufficient to check that

$$\partial_j(\mathbf{y}^\alpha \cdot y_i) = \partial_j(\mathbf{y}^\alpha)y_i + \mathbf{y}^\alpha \cdot \partial_j(y_i)$$

for all $\alpha \in [p-1]^t$ and all $i = 1, \ldots, t$. This can be easily verified, using the fact that $y_k^p \in B_1$ for all $k = 1, \ldots, t$.

(b) If $b_j \in B$ are such that $\sum_{j=1}^t b_j\partial_j = 0$, then $b_i = (\sum_{j=1}^t b_j\partial_j)(y_i) = 0$ for all i, so the sum above is direct. Finally, if $f \in \mathcal{D}$, then it is easy to see that f and $\sum_{j=1}^t f(y_j)\partial_j$ agree on every element of B with the form $u \cdot \mathbf{y}^\alpha$ for $u \in B_1$, so $f = \sum_{j=1}^t f(y_j)\partial_j$ and the result follows.

(c) Suppose $x \notin B_1$ and write $x = \sum_{\alpha\in[p-1]^t} x_\alpha \mathbf{y}^\alpha$. Then $x_\alpha \neq 0$ for some $\alpha \neq 0$ and so $\alpha_j \neq 0$ for some j. Hence $\partial_j(x) \neq 0$. The converse is trivial.

(d) ($\Leftarrow$) Let $J = I \cap B_1$. For any $f \in \mathcal{D}$ we have

$$f(I) = f(JB) = Jf(B) \subseteq JB = I$$

so I is $\mathcal{D}$-stable.

($\Rightarrow$) Let I be a $\mathcal{D}$-stable ideal and let $J = I \cap B_1$. Note that the extension $B_1/J \subseteq B/JB$ satisfies the same conditions as $B_1 \subseteq B$, and the image of I in B/JB is stable under every B_1/J-linear derivation of B/JB by part (b). Without loss of generality we may therefore assume that $I \cap B_1 = 0$, and it will be enough to show that $I = 0$.

Suppose for a contradiction that $I \neq 0$. If $u = \sum_{\alpha\in[p-1]^t} u_\alpha \mathbf{y}^\alpha \in B$ is a nonzero element, define

$$m(u) := \max\{\alpha_1 + \cdots + \alpha_t : u_\alpha \neq 0\}$$

and choose $u \in I\backslash 0$ such that $m(u)$ is minimal. If $\partial_j(u) \neq 0$ for some j then $m(\partial_j(u)) < m(u)$ and $\partial_j(u) \in I\backslash 0$ contradicting the minimality of $m(u)$. Hence $\partial_j(u) = 0$ for all j and therefore $u \in B_1$ by parts (b) and (c). But then $I \cap B_1 \neq 0$, a contradiction. Hence $I = 0$ as required. $\square$

3. A control theorem for normal elements

3.1. **Main result.** The purpose of this section is to prove the following

Theorem. *Let (A, A_1) be a Frobenius pair satisfying the derivation hypothesis, suppose that B_1 is a UFD and let $w \in A$ be a normal element. Then the two-sided ideal wA of A is controlled by A_1:*

$$wA = (wA \cap A_1) \cdot A.$$

The derivation hypothesis is explained below in §3.5 and the proof is given in §3.6.

3.2. **Inducing derivations on** $\operatorname{gr} A$**.** Let A be a filtered ring with associated graded ring B and let $a \in A$. Suppose that there is an integer $n \geqslant 0$ such that

$$[a, F_k A] \subseteq F_{k-n} A$$

for all $k \in \mathbb{Z}$. This induces linear maps

$$\begin{array}{rccc} \{a, -\}_n : & \frac{F_k A}{F_{k-1} A} & \to & \frac{F_{k-n} A}{F_{k-n-1} A} \\ & b + F_{k-1} A & \mapsto & [a, b] + F_{k-n-1} A \end{array}$$

for each $k \in \mathbb{Z}$ which piece together to give a graded derivation

$$\{a, -\}_n : B \to B.$$

The idea of inducing derivations of $\operatorname{gr} A$ in this way was first suggested to the first author by Chris Brookes and later independently by Ken Brown.

Definition. *A* source of derivations *for a Frobenius pair* (A, A_1) *is a subset* $\mathbf{a} = \{a_0, a_1, a_2, \ldots\}$ *of* A *such that there exist functions* $\theta, \theta_1 : \mathbf{a} \to \mathbb{N}$ *satisfying the following conditions:*

(i) $[a_r, F_k A] \subseteq F_{k-\theta(a_r)} A$ *for all* $r \geqslant 0$ *and all* $k \in \mathbb{Z}$
(ii) $[a_r, F_k A_1] \subseteq F_{k-\theta_1(a_r)} A$ *for all* $r \geqslant 0$ *and all* $k \in \mathbb{Z}$,
(iii) $\theta_1(a_r) - \theta(a_r) \to \infty$ *as* $r \to \infty$.

Let $\mathcal{S}(A, A_1)$ *denote the set of all sources of derivations for* (A, A_1).

The reason behind this definition will hopefully become clear after Proposition 3.4 below. By (i), any source of derivations $\mathbf{a}$ generates a sequence of graded derivations $\{a_r, -\}_{\theta(a_r)}$ of $B = \operatorname{gr} A$. These derivations are B_1-linear for sufficiently large r by parts (ii, iii).

The subset $\{0\}$ is clearly an example of a source of derivations. Somewhat less trivially, we will show in Corollary 6.7 that if G is a uniform pro-p group and $g \in G$, then $\{g, g^p, g^{p^2}, \ldots\}$ is a source of derivations for the the Frobenius pair (KG, KG^p).

3.3. **The delta function.** Let (A, A_1) be a Frobenius pair and n be an integer. Each filtered part $F_n A_1$ is closed in A_1 by definition of the filtration topology, and A_1 is closed in A by assumption. Hence $F_n A_1$ is closed in A, which can be expressed as follows:

$$F_n A_1 = \bigcap_{k \geqslant 0} \left(F_n A_1 + F_{n-k} A \right).$$

We can now define a key invariant of elements of A.

Definition. *For any* $w \in A$*, let* $n = \deg w$*. Define*

$$\delta(w) = \begin{cases} \max\{k : w \in F_n A_1 + F_{n-k} A\} & \text{if} \quad w \notin A_1 \\ \infty & \text{if} \quad w \in A_1. \end{cases}$$

Clearly $\delta(w) \geqslant 0$. Note that if $w \in F_n A \backslash A_1$, then $w \notin F_n A_1 + F_{n-k} A$ for some $k \geqslant 0$ by the above remarks, so the definition makes sense and $\delta(w)$ is finite. The number $\delta(w)$ measures how closely the element w can be approximated by elements of A_1. It should be remarked that $\delta(w) > 0$ if and only if $\operatorname{gr} w \in B_1$, since both conditions are equivalent to $w \in F_n A_1 + F_{n-1} A$.

Now suppose that $w \in A\backslash A_1$. By the definition of δ, we can find elements $x \in F_n A_1$ and $y \in F_{n-\delta} A$ such that $w = x + y$; if $\delta = 0$ we take x to be zero. Note that $y \notin F_{n-\delta-1}A$ by the maximality of δ and hence

$$Y_w := \operatorname{gr} y = y + F_{n-\delta-1}A.$$

In view of our assumption on x, we have $Y_w = \operatorname{gr} w$ when $\delta = 0$.

3.4. **a-closures.** If w is an element of a right ideal I of A, then the symbol of w, $\operatorname{gr} w$ always lies in the associated graded ideal $\operatorname{gr} I$ of B. Naturally there are many elements w having the same symbol, so some information is lost when one passes to the symbol of w. It turns out that if the ideal I is two-sided, there is a way to save some of this information.

Definition. *Let* $\mathbf{a}$ *be a source of derivations for a Frobenius pair* (A, A_1) *and* I *be a graded ideal of* B*. We say that the homogeneous element* Y *of* B *lies in the* $\mathbf{a}$-closure *of* I *if* $\{a_r, Y\}_{\theta(a_r)}$ *lies in* I *for all* $r \gg 0$*.*

Proposition. *Let* (A, A_1) *be a Frobenius pair,* I *be a two-sided ideal of* A *and* $w \in I\backslash A_1$*. Then* Y_w *lies in the* $\mathbf{a}$*-closure of* $\operatorname{gr} I$ *for any source of derivations* $\mathbf{a}$*.*

Proof. Let us write $w = x + y$ as in the previous subsection. Since $\mathbf{a}$ is a source of derivations, we can find an integer $r_0 \geqslant 1$ such that $\theta_1(a_r) - \theta(a_r) > \delta$ for all $r \geqslant r_0$. Therefore

$$\begin{aligned} [a_r, x] &\in F_{n-\theta_1(a_r)}A \subseteq F_{n-\delta-\theta(a_r)-1}A \quad \text{and} \\ [a_r, y] &\in F_{n-\delta-\theta(a_r)}A, \end{aligned}$$

for all $r \geqslant r_0$. Hence

$$\begin{aligned} [a_r, w] &\in F_{n-\delta-\theta(a_r)}A, \quad \text{and} \\ [a_r, w] &\equiv [a_r, y] \mod F_{n-\delta-\theta(a_r)-1}A \end{aligned}$$

for all $r \geqslant r_0$. We can rewrite the above as follows:

$$[a_r, w] + F_{n-\delta-\theta(a_r)-1}A = [a_r, y] + F_{n-\delta-\theta(a_r)-1}A = \{a_r, Y_w\}_{\theta(a_r)}$$

for $r \geqslant r_0$. Since $w \in I$ and I is a two-sided ideal, this element must always lie in the ideal $\operatorname{gr} I$ of B, and hence Y_w lies in the $\mathbf{a}$-closure of $\operatorname{gr} I$ as required. $\square$

Each source of derivations $\mathbf{a}$ gives rise to a sequence of derivations $\{a_r, -\}_{\theta(a_r)}$ of B, and some or all of these could well be zero. To ensure that we get an interesting supply of derivations of B, we now introduce a condition which holds for Iwasawa algebras of only rather special uniform pro-p groups.

3.5. **Derivation hypothesis.** Recall that $\mathcal{D}$ denotes the set of all B_1-linear derivations of B and $\mathcal{S}(A, A_1)$ denotes the set of all sources of derivations for (A, A_1). Our derivation hypothesis is really concerned with the action of the derivations induced by $\mathcal{S}(A, A_1)$ on the graded ring B.

Definition. *Let* (A, A_1) *be a Frobenius pair and* $X \in B$ *be an arbitrary homogeneous element. We say that* (A, A_1) *satisfies the* derivation hypothesis *if whenever a homogeneous element* $Y \in B$ *lies in the* $\mathbf{a}$*-closure of* XB *for all* $\mathbf{a} \in \mathcal{S}(A, A_1)$*, we must have* $\mathcal{D}(Y) \subseteq XB$*.*

Assuming the derivation hypothesis, it is possible to "clean" a normal element by multiplying it by a unit. The following Proposition forms the inductive step in the proof of Theorem 3.1.

Proposition. *Let (A, A_1) be a Frobenius pair satisfying the derivation hypothesis and let $w \in A \backslash A_1$ be a normal element. Then there exists a unit $u \in A$ such that $\delta(wu) > \delta(w)$. Moreover, if $\delta(w) > 0$ then $u = 1 - c$ for some $c \in F_{-\delta(w)}A$.*

Proof. Write $w = x+y$ as in §3.3, let $X = \operatorname{gr} w$ and $Y = Y_w = \operatorname{gr} y$. By Proposition 3.4, Y lies in the $\mathbf{a}$-closure of $\operatorname{gr} wA = XB$ for all $\mathbf{a} \in \mathcal{S}(A, A_1)$ and hence $\mathcal{D}(Y) \subseteq XB$ because (A, A_1) satisfies the derivation hypothesis.

Suppose first that $\delta := \delta(w) = 0$, so that $Y = X$. Then the ideal XB of B is $\mathcal{D}$-stable and is hence controlled by B_1 by Proposition 2.4(d):

$$XB = (XB \cap B_1) \cdot B.$$

Because B is a free B_1-module, $XB \cap B_1$ is a reflexive ideal of B_1 by Proposition 1.2(b). Since B_1 is a UFD by assumption, $XB \cap B_1 = X_1 B_1$ for some homogeneous element $X_1 \in B_1$ by Lemma 1.4.

Hence $XB = X_1 B$ and we can therefore find a homogeneous unit $U \in B$ such that $X_1 = XU$. Choose $u, v \in A$ such that $\operatorname{gr} u = U$ and $\operatorname{gr} v = U^{-1}$; then $uv \equiv 1 \mod F_{-1}A$. But A is complete so $1 + F_{-1}A$ consists of units in A and hence u is a unit. Since $\operatorname{gr}(wu) = XU = X_1 \in B_1$, it follows that $\delta(wu) > 0 = \delta(w)$ as required.

Now suppose that $\delta > 0$; then X must lie in B_1. Applying Proposition 2.4(c) to the image of Y in B/XB yields that

$$Y \in XB + B_1.$$

Since X and Y are homogeneous, we can find homogeneous elements $C \in B$ and $Z \in B_1$ such that

$$Y = XC + Z;$$

moreover $\deg Y = \deg XC$ if $XC \neq 0$ and $\deg Y = \deg Z$ if $Z \neq 0$.

Suppose for a contradiction that $C = 0$. Then $Y = Z \in B_1$. Hence we can find $x' \in F_{n-\delta} A_1$ such that

$$x' \equiv y \mod F_{n-\delta-1}A.$$

Thus $w - (x + x') \in F_{n-\delta-1}A$, which is contradictory to the maximality of δ. So $C \neq 0$ and hence $\deg C = \deg Y - \deg X = -\delta$. Note that $\deg C < 0$.

We can find $c \in A$ such that $\operatorname{gr} c = C$. Then

$$w(1 - c) = (x + y)(1 - c) \equiv x + y - xc \mod F_{n-\delta-1}A$$

since $\deg(yc) < n - \delta$. But

$$y - xc + F_{n-\delta-1}A = Y - XC = Z \in B_1,$$

so we can find $z \in A_1$ such that $y - xc \equiv z \mod F_{n-\delta-1}A$ and hence

$$w(1 - c) - (x + z) \in F_{n-\delta-1}A.$$

Since $\deg Z = \deg Y$ if $Z \neq 0$, $z \in F_{n-\delta}A$ and hence $x + z \in F_n A_1$. This implies that $\delta(w(1 - c)) > \delta = \delta(w)$.

Finally, since $c \in F_{-\delta(w)}A \subseteq F_{-1}A$ and A is complete, $u := 1 - c$ is a unit in A and $\delta(wu) > \delta(w)$ by construction. □

3.6. **Proof of Theorem 3.1.**

Proof. It will be enough to construct a unit $u \in A$ such that $wu \in A_1$.

If w already happens to lie in A_1 then we can take $u = 1$, so assume that $w \notin A_1$. By Proposition 3.5 there exists a unit $u_0 \in A$ such that $\delta(wu_0) > 0$.

Let $w_0 := wu_0$. Using Proposition 3.5 we can inductively construct a sequence of normal elements $w_1, w_2, \ldots$ of A and a sequence of elements $c_1, c_2, \ldots$ of A, such that for all $i \geqslant 0$,

- $c_{i+1} \in F_{-\delta(w_i)}A$,
- $w_{i+1} = w_i(1 - c_{i+1})$,
- $\delta(w_{i+1}) > \delta(w_i)$ if $w_i \notin A_1$.

Here we interpret $F_{-\infty}A$ as the zero subspace of A. With this convention, the sequence c_i converges to zero as $i \to \infty$ by construction, so the limit

$$u := \lim_{i\to\infty} u_0(1 - c_1)\cdots(1 - c_i)$$

exists in A by the completeness of A. Note that u is unit because we can write down an inverse having the same form as u, and that $wu = \lim_{i\to\infty} w_i$.

We will now show that wu lies in A_1. Since A_1 is closed in A, it will be sufficient to show that $wu \in A_1 + F_kA$ for all $k \in \mathbb{Z}$. Let $n = \deg w_0$ and note that $\deg w_i = n$ for all $i \geqslant 0$ by construction. Since $w_i \to wu$ and $\delta(w_i) \to \infty$ as $i \to \infty$, we see that for $i \gg 0$, $wu - w_i \in F_kA$ and $w_i \in F_nA_1 + F_kA$. Hence $wu \in F_nA_1 + F_kA \subseteq A_1 + F_kA$, as required. □

4. Microlocalisation

4.1. **Notation.** We briefly recall some basic facts about the theory of algebraic microlocalisation, following [Li] and [AVV]. Our notation will be slightly non-standard. Throughout §4 we will make the following assumptions:

- R is a filtered ring whose Rees ring $\widetilde{R}$ is noetherian,
- T is a right Ore subset of $\operatorname{gr} R$ consisting of homogeneous regular elements.

Since R and $\operatorname{gr} R$ are homomorphic images of $\widetilde{R}$ by §1.5, these rings must also be noetherian. We should remark at this point that if the filtration on R is complete and $\operatorname{gr} R$ is noetherian, then the filtration on R is *zariskian*: see [LV, Chapter II, §2.1, Definition 1 and §2.2, Proposition 1]. In particular $\widetilde{R}$ is necessarily noetherian.

4.2. **Lifting Ore sets.** Let $\widetilde{T}$ denote the homogeneous inverse image of T in $\widetilde{R}$:

$$\widetilde{T} := \{r \in \widetilde{R} : r \text{ is homogeneous and } \pi_2(r) \in T\}.$$

It can be shown that $\widetilde{T}$ is a right Ore set in $\widetilde{R}$ [Li, Corollary 2.2], so we may form the Ore localisation $\widetilde{R}_{\widetilde{T}}$. This is still a $\mathbb{Z}$-graded ring.

Let $S := \pi_1(\widetilde{T}) \subseteq R$. This is a right Ore set in R and in fact

$$S = \{r \in R : \operatorname{gr} r \in T\}.$$

Note that S consists of regular elements in R, since every element of T is assumed to be regular. It follows that R embeds into the Ore localisation R_S.

The surjection $\pi_1 : \widetilde{R} \twoheadrightarrow R$ extends to surjection $\pi_1 : \widetilde{R}_{\widetilde{T}} \twoheadrightarrow R_S$. The grading on $\widetilde{R}_{\widetilde{T}}$ induces a filtration on R_S, as in [Li, Proposition 2.3(1)]:

$$F_nR_S := \pi_1((\widetilde{R}_{\widetilde{T}})_n).$$

Here $(\widetilde{R}_{\widetilde{T}})_n$ denotes the n^{th}-graded part of $\widetilde{R}_{\widetilde{T}}$.

Lemma. *The filtration on R_S is given explicitly by the formula*

$$F_nR_S = \{rs^{-1} : r \in R, s \in S \quad \textit{and} \quad \deg r - \deg s \leqslant n\}$$

for all integers n. This filtration is zariskian.

Proof. Before we begin the proof, let us observe that if $x \in R$ is nonzero and $y \in S$ then $(\operatorname{gr} x)(\operatorname{gr} y) \neq 0$ (because $\operatorname{gr} x \neq 0$ and $\operatorname{gr} y \in T$ is regular) and hence $\deg(xy) = \deg x + \deg y$.

Let $L_n = \{rs^{-1} : r \in R, s \in S \text{ and } \deg r - \deg s \leqslant n\}$. Decoding the definition of F_nR_S, we see that F_nR_S is in fact the additive subgroup of R_S generated by L_n. It will therefore be sufficient to show that L_n is closed under addition.

So let $r_1s_1^{-1}$ and $r_2s_2^{-1}$ be elements of L_n for some $r_i \in R$ and $s_i \in S$. We can find $u_1 \in S$ and $u_2 \in R$ such that $s_1u_1 = s_2u_2 = s$ say; then $r_1s_1^{-1} + r_2s_2^{-1} = (r_1u_1+r_2u_2)s^{-1}$. Since $s_1, s_2 \in S$, we have $\deg s = \deg s_1 + \deg u_1 = \deg s_2 + \deg u_2$ by the first paragraph. Now

$$\begin{aligned} \deg(r_1u_1 + r_2u_2) - \deg s &\leqslant \max\{\deg r_1 + \deg u_1, \deg r_2 + \deg u_2\} - \deg s = \\ &= \max\{\deg r_1 - \deg s_1, \deg r_2 - \deg s_2\} \leqslant n \end{aligned}$$

so $(r_1u_1 + r_2u_2)s^{-1} \in L_n$, as required.

The last assertion follows from [Li, Proposition 2.8]. □

4.3. **Microlocalisation of rings.**

Definition. *The* microlocalisation *of R at T is the completion $Q_T(R)$ of R_S with respect to the filtration on R_S described in §4.2.*

We record some useful properties enjoyed by microlocalisation.

Proposition. *(a) $Q_T(R)$ is a complete filtered ring,*
(b) $F_nQ_T(R)$ is the closure of F_nR_S in $Q_T(R)$,
(c) R embeds into $Q_T(R)$,
(d) $Q_T(R)$ is a flat right R-module,
(e) there are natural isomorphisms

$$\operatorname{gr} Q_T(R) \cong \operatorname{gr}(R_S) \cong (\operatorname{gr} R)_T.$$

Proof. Parts (a) and (b) are clear from the definition. We have seen in §4.2 that R embeds into R_S, and the filtration on R_S is separated by Lemma 4.2 and [LV, Chapter II, §2.1, Theorem 2]. Hence R_S embeds into $Q_T(R)$ and part (c) follows. Parts (d) and (e) follow from [AVV, Corollary 3.20(1) and Proposition 3.10]. □

4.4. **Microlocalisation of modules.** Let M be a finitely generated right R-module. We define the *microlocalisation* of M at T to be

$$Q_T(M) := M \otimes_R Q_T(R).$$

This is naturally a right $Q_T(R)$-module. Recall that a filtration on M is said to be *good* if the associated Rees module is finitely generated over $\widetilde{R}$.

Lemma. *Let M be a finitely generated R-module equipped with some good filtration, and N be a submodule of M. Then*
(a) $\operatorname{gr} Q_T(M) \cong (\operatorname{gr} M)_T$,
(b) the Ore localisation M_S is a dense R_S-submodule of $Q_T(M)$,

(c) $Q_T(N)$ *can be identified with a* $Q_T(R)$*-submodule of* $Q_T(M)$*,*
(d) the tensor filtration on $Q_T(N)$ *coincides with the subspace filtration induced from* $Q_T(M)$*,*
(e) if L *is another submodule of* M*, then* $Q_T(N) \cap Q_T(L) = Q_T(N \cap L)$*.*

Proof. We should remark that the filtration on $Q_T(M) = M \otimes_R Q_T(R)$ is the *tensor filtration* in the sense of [LV, Chapter I, §6]. Part (a) follows from [AVV, Proposition 3.10 and Corollary 3.20(2)] and part (b) follows from [Li, Corollary 2.5(3)], whereas parts (c) and (d) follow from [AVV, Corollary 3.16(3)].

Finally, $Q_T(R)$ is a flat R-module by Proposition 4.3(d), so the microlocalisation functor $M \mapsto M \otimes_R Q_T(R)$ preserves pullbacks, and in particular, intersections. Part (e) follows. □

4.5. **Constructing normal elements.** Let I be a right ideal of R. Using Lemma 4.4(c), we can and will identify $Q_T(I)$ with a right ideal of $Q_T(R)$. By Lemma 4.4(d) this identification respects filtrations, and by Lemma 4.4(a) the associated graded ideal $\operatorname{gr} Q_T(I)$ is just the localised right ideal $(\operatorname{gr} I)_T$ of $\operatorname{gr} Q_T(R) = (\operatorname{gr} R)_T$.

Proposition. *Let* I *be a two-sided of* R *and suppose that there exists a central regular homogeneous element* $X \in \operatorname{gr} R$ *such that the localised ideal* $(\operatorname{gr} I)_T$ *of* $(\operatorname{gr} R)_T$ *is generated by* X*:*

$$(\operatorname{gr} I)_T = X \cdot (\operatorname{gr} R)_T.$$

Then there exists a normal *element* $w \in Q_T(R)$ *such that* $Q_T(I) = w \cdot Q_T(R)$*.*

Proof. Choose any $w \in Q_T(I)$ such that $\operatorname{gr} w = X$. Then the right ideal $w \cdot Q_T(R)$ is contained in $Q_T(I)$ and their graded ideals are equal by assumption. Because the filtration on $Q_T(R)$ is complete, it follows that $Q_T(I) = w \cdot Q_T(R)$.

The Ore localisation I_S is a *two-sided* ideal of R_S because R is noetherian [MR, Proposition 2.1.16]. By Lemma 4.4(b), $Q_T(I)$ is the closure of I_S inside $Q_T(R)$ and is hence a two-sided ideal of $Q_T(R)$.

Since $X = \operatorname{gr} w$ is central and regular in $(\operatorname{gr} R)_T$, and the filtration on $Q_T(R)$ is complete, the fact that w is a normal element in R will follow from the following rather general lemma. □

Lemma. *Let* R *be a complete filtered ring and* $w \in R$*. Suppose that* wR *is a two-sided ideal of* R *and that* $\operatorname{gr} w$ *is a central regular element of* $\operatorname{gr} R$*. Then* w *is a regular normal element in* R*.*

Proof. Because $\operatorname{gr} w$ is a regular element of $\operatorname{gr} R$, w must be a regular element of R. Since $Rw \subseteq wR$, for every $r \in R$ there exists $\sigma(r) \in R$ such that $rw = w\sigma(r)$. Since w is regular, $r \mapsto \sigma(r)$ is an injective ring endomorphism of R. We will show that σ is surjective, which will complete the proof.

Let $r \in R$ be nonzero, so that $\sigma(r)$ is nonzero. Since $\operatorname{gr} w$ is central and regular,

$$\operatorname{gr} r \operatorname{gr} w = \operatorname{gr}(rw) = \operatorname{gr}(w\sigma(r)) = \operatorname{gr} w \operatorname{gr} \sigma(r) = \operatorname{gr} \sigma(r) \operatorname{gr} w$$

and therefore $\operatorname{gr} \sigma(r) = \operatorname{gr} r$ for any nonzero $r \in R$. Now let $s \in R$ be a nonzero element of degree n. Set $r_n := s$, so that

$$s \equiv \sigma(r_n) \mod F_{n-1}R.$$

Set $r_{n-1} = s - \sigma(r_n) \in F_{n-1}R$, so that

$$s - \sigma(r_n) \equiv \sigma(r_{n-1}) \mod F_{n-2}R.$$

Continuing this process, we can construct a sequence of elements $r_n, r_{n-1}, r_{n-2}, \ldots$ of R such that $r_i \in F_i R$ for all $i \leqslant n$. Because R is complete, the infinite sum $\sum_{k=0}^{\infty} r_{n-k}$ converges to an element r of R and $\sigma(r) = s$ by construction. The result follows. □

5. A control theorem for reflexive ideals

In this section we state and prove our main result.

5.1. **Microlocalisation of Frobenius pairs.** Let (A, A_1) be a Frobenius pair. Because $B = \operatorname{gr} A$ is noetherian and the filtration on A is complete, the remarks made in §4.1 show that we may apply the theory developed in §4.

If Z is a nonzero homogeneous element of B, then $T := \{1, Z, Z^2, \ldots\}$ is an Ore set in B consisting of regular homogeneous elements, since B is a commutative domain by assumption. By abuse of notation, we will denote the corresponding microlocalisation $Q_T(A)$ by $Q_Z(A)$.

It turns out that Frobenius pairs are stable under microlocalisation.

Proposition. *Let (A, A_1) be a Frobenius pair and $Z \in B$ be a nonzero homogeneous element.*

(a) Then $(Q_Z(A), Q_{Z^p}(A_1))$ is also a Frobenius pair.
(b) If $\mathbf{a}$ is a source of derivations for (A, A_1), then it is also a source of derivations for $(Q_Z(A), Q_{Z^p}(A_1))$.
(c) Suppose B is a UFD. If (A, A_1) satisfies the derivation hypothesis, then so does $(Q_Z(A), Q_{Z^p}(A_1))$.

Proof. (a) By Proposition 4.3(c), we can identify A with its image in $Q_Z(A)$. We will also identify $\operatorname{gr} A_1$ with its image B_1 in B. By Definition 2.2(iii), Z^p lies in B_1 so the microlocalisation $Q_{Z^p}(A_1)$ makes sense.

Let T and T_1 denote the multiplicatively closed sets in B and B_1 generated by Z and Z^p and let S and S_1 be the corresponding right Ore sets in A and A_1. Clearly $S_1 \subseteq S$, so the Ore localisation $(A_1)_{S_1}$ naturally embeds into A_S. Moreover, using Lemma 4.2 we see that

$$(F_n A_S) \cap (A_1)_{S_1} = F_n (A_1)_{S_1}$$

for all $n \in \mathbb{Z}$, which means that the filtration on $(A_1)_{S_1}$ induced from A_1 coincides with the subspace filtration induced from A_S. Passing to completions we see that $Q_{Z^p}(A_1)$ can be identified with a closed subalgebra of $Q_Z(A)$. Moreover, one can easily check that

$$(F_n Q_Z A) \cap Q_{Z^p}(A_1) = F_n Q_{Z^p}(A_1)$$

for all n. Hence Definition 2.2(i) is satisfied for the new pair $(Q_Z(A), Q_{Z^p}(A_1))$.

Next, $\operatorname{gr} Q_Z(A) \cong B_Z$ and $\operatorname{gr} Q_{Z^p}(A_1) \cong (B_1)_{Z^p}$ by Proposition 4.3(e). Since B_Z is a commutative noetherian domain and $(B_Z)^{[p]} = B_{Z^p}^{[p]} \subseteq (B_1)_{Z^p}$, Definitions 2.2(ii, iii) are satisfied.

Finally, $B_Z \cong B_{Z^p}$ because Z is becomes a unit when Z^p gets inverted. Hence

$$B_Z = B_{Z^p} = \bigoplus_{\alpha \in \mathbb{N}_t^p} (B_1)_{Z^p} \mathbf{y}^\alpha = \bigoplus_{\alpha \in \mathbb{N}_t^p} (B_Z)_1 \mathbf{y}^\alpha,$$

which shows that Definition 2.2(iv) is inherited by B_Z.

(b) Let $a \in A$ and let the integers k, n be such that $[a, F_k A] \subseteq F_{k-n} A$. For any $y \in A$ and $s \in S$ we have

$$[a, ys^{-1}] = [a, y]s^{-1} - ys^{-1}[a, s]s^{-1},$$

which together with Lemma 4.2 implies that

$$[a, F_k A_S] \subseteq F_{k-n} A_S.$$

Now $F_k Q_Z(A)$ is the closure of $F_k A_S$ in $Q_Z(A)$ by Proposition 4.3(b) and the bracket operation $[a, -]$ is continuous, so

$$[a, F_k Q_Z(A)] \subseteq F_{k-n} Q_Z(A).$$

A similar argument shows that if $[a, F_k A_1] \subseteq F_{k-n} A$, then

$$[a, F_k Q_{Z^p}(A_1)] \subseteq F_{k-n} Q_Z(A).$$

Part (b) follows.

(c) Let X, Y be homogeneous elements of B_Z and suppose that Y lies in the $\mathbf{a}$-closure of XB_Z for all $\mathbf{a} \in \mathcal{S}(Q_Z(A), Q_{Z^p}(A_1))$.

Let $\mathbf{a}$ be a source of derivations for (A, A_1). Note that the derivation D_r of $\operatorname{gr} Q_Z(A) \cong B_Z$ induced by the element $a_r \in Q_Z(A)$ coincides with the extension to B_Z of the derivation $\{a_r, -\}_{\theta(a_r)}$ of B induced by $a_r \in A$.

Because Y lies in the $\mathbf{a}$-closure of XB_Z, $D_r(Y) \in XB_Z$ for all $r \gg 0$. We can find an integer n such that $Z^{p^n} Y \in B$. Then

$$D_r(Z^{p^n} Y) \in XB_Z \cap B$$

for all $r \gg 0$. Since B_Z is a flat B-module, $XB_Z \cap B$ is a reflexive ideal of B by Proposition 1.2(b). Since B is a UFD, Lemma 1.4 implies that $XB_Z \cap B = X'B$ for some homogeneous element $X' \in B$. Hence

$$D_r(Z^{p^n} Y) \in X'B$$

for all $r \gg 0$ and therefore $Z^{p^n} Y$ lies in the $\mathbf{a}$-closure of $X'B$ for any source of derivations $\mathbf{a}$ for (A, A_1). Because (A, A_1) satisfies the derivation hypothesis, it follows that $\mathcal{D}(Z^{p^n} Y) \subseteq X'B$. By Proposition 2.4(b), the localised B_Z-module $\mathcal{D}_Z$ can be identified with the set of all $(B_1)_{Z^p}$-linear derivations of B_Z. But $\mathcal{D}_Z(Y) \subseteq XB_Z$ and part (c) follows. $\square$

5.2. **Applying Theorem 3.1.** We can now use the Control Theorem for normal elements to deduce some information about arbitrary two-sided ideals. Recall the definition of pseudo-null modules from §1.3.

Theorem. *Let (A, A_1) be a Frobenius pair satisfying the derivation hypothesis, such that B and B_1 are UFDs. Let I be a two-sided ideal of A and $J = (I \cap A) \cdot A_1$. Then $\operatorname{gr} I / \operatorname{gr} J$ is pseudo-null.*

Proof. The right ideal J is clearly contained in I, and we have the following chain of inclusions of graded ideals in B:

$$\operatorname{gr} J \subseteq \operatorname{gr} I \subseteq \overline{\operatorname{gr} I} \subseteq \operatorname{gr} R,$$

where $\overline{\operatorname{gr} I}$ denotes the reflexive closure of $\operatorname{gr} I$ in B defined in §1.2. Since B is a UFD, $\overline{\operatorname{gr} I} = XB$ for some homogeneous element $X \in B$ by Lemma 1.4.

Let Z be a nonzero homogeneous element of B such that $ZX \in \operatorname{gr} I$, and consider the microlocalisations $A' := Q_Z(A)$ and $A'_1 := Q_{Z^p}(A_1)$. By construction, $(\operatorname{gr} I)_Z = X \cdot B_Z$, so the two-sided ideal $I' := Q_Z(I)$ of A' is generated by a normal element w of A' by Proposition 4.5. Because the Frobenius pair (A', A'_1) satisfies the derivation hypothesis by Proposition 5.1(c), the ideal $I' = wA'$ is controlled by A'_1 by Theorem 3.1:

$$I' = (I' \cap A'_1) \cdot A'.$$

By Lemma 2.3, $A = \bigoplus_{\alpha \in [p-1]^t} \mathbf{u}^\alpha A_1$ and $A' = \bigoplus_{\alpha \in [p-1]^t} \mathbf{u}^\alpha A'_1$; note that the *same* generators occur in both expressions. Hence

$$A' = A \cdot A'_1 \quad \text{and} \quad I' = I \cdot A' = I \cdot A \cdot A'_1 = I \cdot A'_1.$$

Because A is a finitely generated A_1-module, Lemma 4.4(e) implies that

$$Q_{Z^p}(I) \cap Q_{Z^p}(A_1) = Q_{Z^p}(I \cap A_1)$$

or equivalently, $(I \cdot A'_1) \cap A'_1 = (I \cap A_1) \cdot A'_1$. Hence

$$I' = (I' \cap A'_1) \cdot A' = (I \cap A_1) \cdot A'_1 \cdot A' = (I \cap A_1) A \cdot A'$$

and hence $I \cdot A' = J \cdot A'$. Passing to the graded ideals and using Lemma 4.4(a), we obtain $(\operatorname{gr} I)_Z = (\operatorname{gr} J)_Z$, which means that $Z^n \operatorname{gr} I \subseteq \operatorname{gr} J$ for some integer n.

This holds for any $Z \in X^{-1} \operatorname{gr} I$, a finitely generated ideal in B. Hence

$$(X^{-1} \operatorname{gr} I)^m \subseteq \operatorname{Ann}_B(\operatorname{gr} I / \operatorname{gr} J)$$

for some integer m. But $B/X^{-1} \operatorname{gr} I \cong XB/I$ is pseudo-null by Lemma 1.4, so $C := B/(X^{-1} \operatorname{gr} I)^m$ is also pseudo-null by Lemma 1.3. Since $\operatorname{gr} I / \operatorname{gr} J$ is a finitely generated B-module, it must be a quotient of a direct sum of finitely many copies of C and is therefore pseudo-null, again by Lemma 1.3. $\square$

5.3. **A control theorem for reflexive ideals.** We can now prove our main result. Recall from §0.3 that a reflexive two-sided ideal is a two-sided ideal which is reflexive as a right and left ideal. See also the remark below.

Theorem. *Let (A, A_1) be a Frobenius pair satisfying the derivation hypothesis, such that B and B_1 are UFDs. Let I be a reflexive two-sided ideal of A. Then $I \cap A_1$ is a reflexive two-sided ideal of A_1 and I is controlled by A_1:*

$$I = (I \cap A_1) \cdot A.$$

Proof. Retain the notation of §5.2. Note that A is a free right and left A_1-module by Lemma 2.3. It follows from Proposition 1.2 that $I \cap A_1$ is a reflexive ideal of A_1 and $J = (I \cap A_1)A$ is a reflexive right ideal of A. It will clearly be enough to show that $I \subseteq J$.

Let N be a right submodule of I/J. If we equip N with the subquotient filtration, then $\operatorname{gr} N$ is a submodule of $\operatorname{gr} I / \operatorname{gr} J$ and is hence pseudo-null by Theorem 5.2 and Lemma 1.3. In particular, $E^0(\operatorname{gr} N) = E^1(\operatorname{gr} N) = 0$.

Since the filtration on A is zariskian by the remarks made in §4.1, there is a good filtration on $E^1(N)$ such that $\operatorname{gr} E^1(N)$ is a subquotient of $E^1(\operatorname{gr} N)$ by [Bj, Proposition 3.1]. Hence $\operatorname{gr} E^1(N) = 0$. It now follows from [LV, Chapter II, §1.2, Lemma 9] that $E^1(N) = 0$. Similarly $E^0(N) = 0$, and so I/J is a pseudo-null right A-module.

Let $x \in I$ and $(J : x) := \{a \in A : xa \in J\}$ be the annihilator of the image of x in I/J. By Proposition 1.3(a) we know that $(J : x)^{-1} = A$. Now $J^{-1}x(J : x) \subseteq J^{-1}J \subseteq A$ so $J^{-1}x \subseteq (J : x)^{-1} = A$. Hence $x \in \overline{J} = J$, as required. $\square$

Remark. If B is a UFD, then B is completely integrally closed. In other words, B is a maximal order [MR, Proposition 5.1.3]. It follows from [MaR, X.2.1] that A is also a maximal order. Now it is well known that a two-sided ideal I of a maximal order A is reflexive as a right ideal if and only if it is reflexive as a left ideal [MR, Proposition 5.1.8].

6. Iwasawa algebras

6.1. **The Campbell-Hausdorff series.** Following [DDMS], we define

$$\epsilon := \begin{cases} 2 & \text{if} \quad p = 2 \\ 1 & \text{otherwise.} \end{cases}$$

Recall [DDMS, §9.4] that a $\mathbb{Z}_p$-Lie algebra L is said to be *powerful* if L is free of finite rank as a module over $\mathbb{Z}_p$ and $[L, L] \subseteq p^\epsilon L$.

Let $\Phi(X, Y)$ be the *Campbell-Hausdorff series* [DDMS, Definition 6.26].

Lemma. *Let L be a powerful $\mathbb{Z}_p$-Lie algebra, $v, w \in L$ and $k \geqslant 0$. Then*

$$\Phi(-v + p^k w, v) \equiv p^k w \mod p^{k+1} L.$$

Proof. By the definition of the Campbell-Hausdorff series,

$$\Phi(X, Y) = X + Y + \frac{1}{2}[X, Y] + \sum_{n \geqslant 3} \sum_{\langle \mathbf{e} \rangle = n-1} q_{\mathbf{e}} (X, Y)_{\mathbf{e}}$$

where $\mathbf{e} = (e_1, \ldots, e_s)$ ranges over all possible sequences of positive integers such that $\langle \mathbf{e} \rangle := e_1 + \ldots + e_s = n - 1$, $q_{\mathbf{e}}$ is a certain rational number and

$$(X, Y)_{\mathbf{e}} = [\cdots [\cdots [\cdots [[X, Y], \cdots, Y], X], \cdots, X], \cdots]$$

is a repeated Lie commutator depending on $\mathbf{e}$ of length n. Fix the integer $n \geqslant 3$ and the sequence $\mathbf{e}$ for the time being.

Substitute $X = -v + p^k w$ and $Y = v$ into this repeated commutator and expand: this gives a $\mathbb{Z}_p$-linear combination of repeated commutators of v and $p^k w$ of length n. With the exception of $[v, v, \ldots, v] = 0$, each one of these involves at least one $p^k w$ and hence is contained in $p^k L^n$, where $L^1 = L, L^2 = [L, L], L^3 = [[L, L], L], \ldots$ is the lower central series of L.

Using the fact that L is powerful, we deduce that

$$(-v + p^k w, v)_{\mathbf{e}} \in p^k L^n \subseteq p^{k + \epsilon(n-1)} L.$$

Now as $n \geqslant 3$, $p^{\epsilon(n-1)} q_{\mathbf{e}} \in p^\epsilon \mathbb{Z}_p$ by [DDMS, Theorem 6.28], so

$$q_{\mathbf{e}}(-v + p^k w, v)_{\mathbf{e}} \in p^k q_{\mathbf{e}} p^{\epsilon(n-1)} L \subseteq p^{k+\epsilon} L$$

for all $n \geqslant 3$ and all $\mathbf{e}$ such that $\langle \mathbf{e} \rangle = n - 1$. Hence

$$\Phi(-v + p^k w, v) \equiv p^k w + \frac{p^k}{2}[w, v] \mod p^{k+\epsilon} L.$$

Now $\frac{p^k}{2}[w, v] \in p^{k+1} L$ since $[w, v] \in p^\epsilon L$ and the result follows. $\square$

6.2. **The exponential map.** Recall that there is an isomorphism between the category of uniform pro-p groups and group homomorphisms and the category of powerful $\mathbb{Z}_p$-Lie algebras and Lie homomorphisms [DDMS, Theorem 9.10].

If L is a powerful $\mathbb{Z}_p$-Lie algebra and G is the corresponding uniform pro-p group, then there is a bijection

$$\exp : L \to G$$

which allows us to write every element of G in the form $\exp(u)$ for some $u \in L$. The Campbell-Hausdorff series allows us to recover the group multiplication in G from the Lie structure on L [DDMS, Proposition 6.27]:

$$\exp(u) \cdot \exp(v) = \exp \Phi(u, v)$$

for all $u, v \in L$. We collect together some useful properties of exp in the following

Lemma. *Let L be a powerful $\mathbb{Z}_p$-Lie algebra, $u, v \in L$ and G be the corresponding uniform pro-p group. Then*
(a) $\exp(mu) = \exp(u)^m$ *for all* $m \in \mathbb{Z}$,
(b) $\exp(p^k L) = G^{p^k}$ *for all* $k \geqslant 0$,
(c) if $u \equiv v \mod p^k L$ *for some* $k \geqslant 0$, *then* $\exp(u) \equiv \exp(v) \mod G^{p^k}$,
(d) exp *induces an* $\mathbb{F}_p$*-linear isomorphism* $L/pL \to G/G^p$:

$$\exp(u + v) \equiv \exp(u) \exp(v) \mod G^p.$$

Proof. For parts (a), (b) and (d) see the proof of [DDMS, Theorem 9.8]. Now Lemma 6.1 implies that $\Phi(-u, v) \in p^k L$, so

$$\exp(u)^{-1} \exp(v) = \exp(-u) \exp(v) = \exp \Phi(-u, v) \in \exp(p^k L) = G^{p^k}$$

and part (c) follows. □

Let $(g, h) = g^{-1}h^{-1}gh$ denote the group commutator of $g, h \in G$.

Proposition. *Let $u \in L$ be such that $[u, L] \subseteq p^k L$ for some $k \geqslant \epsilon$. Then*

$$(\exp(u), \exp(v)) \equiv \exp([u, v]) \mod G^{p^{k+1}}$$

for all $v \in L$. In particular, $(\exp(u), G) \subseteq G^{p^k}$.

Proof. We can compute the conjugate $\exp(-u)\exp(-v)\exp(u)$ in G using [DDMS, Exercise 6.12]: $\exp(-u)\exp(-v)\exp(u) = \exp(-z)$, where

$$z := v.\exp(\mathrm{ad}(u)) = v + [v, u] + \frac{1}{2}[[v, u], u] + \frac{1}{6}[[[v, u], u], u] + \cdots \in L.$$

Now $\exp(p^k) = 1 + p^k + \frac{1}{2}p^{2k} + \ldots \equiv 1 + p^k \mod p^{k+1}\mathbb{Z}_p$ and $L \cdot \mathrm{ad}(u) \subseteq p^k L$, so

$$\frac{v \cdot \mathrm{ad}(u)^n}{n!} \in \frac{p^{kn}}{n!} L \subseteq p^{k+1} L$$

for all $n \geqslant 2$. Hence $z = v + p^k w$ for some $w \in L$ such that $p^k w \equiv [v, u] \mod p^{k+1} L$.

Applying Lemma 6.1, we deduce that

$$\Phi(-z, v) = \Phi(-v - p^k w, v) \equiv -p^k w \equiv [u, v] \mod p^{k+1} L.$$

Using Lemma 6.2(c), we finally obtain

$$(\exp(u), \exp(v)) = \exp(-z) \cdot \exp(v) = \exp \Phi(-z, v) \equiv \exp([u, v]) \mod G^{p^{k+1}},$$

as required. □

6.3. **Subalgebras and subgroups.** From now on, we will assume that L is a powerful $\mathbb{Z}_p$-Lie algebra of rank d and we will fix a subalgebra L_1 of L which contains pL. We can find a subset $\{v_1, \ldots, v_d\}$ of L such that

- $\{v_i + pL : 1 \leqslant i \leqslant d\}$ is an $\mathbb{F}_p$-basis for L/pL, and
- $\{v_i + L_1 : 1 \leqslant i \leqslant t\}$ is an $\mathbb{F}_p$-basis for L/L_1 for some t.

In many interesting cases, L_1 will in fact be equal to pL.

Lemma. *Let $G = \exp(L)$ be the uniform pro-p group corresponding to L, let $G_1 = \exp(L_1)$ and let $g_i = \exp(v_i)$ for all i. Then*
(a) G_1 is a subgroup *of G,*
(b) $\{g_1, \ldots, g_d\}$ is a topological generating set for G, and
(c) $\{g_1^p, \ldots, g_t^p, g_{t+1}, \ldots, g_d\}$ is a topological generating set for G_1.

Proof. (a) This is not entirely trivial, since $\exp(M)$ doesn't have to be a subgroup of G for arbitrary subalgebras M of L — see [I]. However, $\exp(u)\exp(v) \equiv \exp(u+v) \mod G^p$ for all $u, v \in L$ by Lemma 6.2 and $G^p = \exp(pL) \subseteq \exp(L_1) = G_1$, so $xy \in G_1$ for all $x, y \in G_1$ and G_1 *is* a subgroup.

(b) Let M be the $\mathbb{Z}_p$-submodule of L generated by $\{v_1, \ldots, v_d\}$. Because

$$M + pL = L$$

by assumption, $M = L$ by Nakayama's Lemma and hence $\{v_1, \ldots, v_d\}$ is a $\mathbb{Z}_p$-basis for L since L has rank d. Part (b) now follows from [DDMS, Theorem 9.8].

(c) By [DDMS, Theorem 3.6(iii)] and part (b), $\{g_1^p, \ldots, g_d^p\}$ is a topological generating set for G^p. Since $\{g_{t+1}G^p, \ldots, g_d G^p\}$ is a basis for G_1/G^p by Lemma 6.2(d), $\{g_1^p, \ldots, g_t^p, g_{t+1}, \ldots, g_d\}$ must be a topological generating set for G_1, as required. □

6.4. **The group algebra of a uniform pro-p group.** Let G is a uniform pro-p group and let K be a field of characteristic p. Let J be the augmentation ideal of the group algebra $K[G]$ of G. If $\{g_1, \ldots, g_d\}$ is a topological generating set for G and set $b_i := g_i - 1$ for all $i = 1, \ldots, d$, then these elements all lie in J.

Proposition. *The associated graded ring of $K[G]$ with respect to the J-adic filtration is isomorphic to the polynomial algebra $K[y_1, \ldots, y_d]$.*

Proof. As in the proof of [DDMS, Theorem 7.22], the b_i's commute modulo J^3. We can therefore define a K-algebra homomorphism $\varphi : K[y_1, \ldots, y_d] \to \operatorname{gr} K[G]$ by setting $\varphi(y_i) = b_i + J^2$. When the field K is $\mathbb{F}_p$, [DDMS, Theorem 7.24] implies that φ is an isomorphism. The general case now follows, using a simple "extension of scalars" argument. □

From now on we will identify $K[y_1, \ldots, y_d]$ with $\operatorname{gr} K[G]$ via the map φ. For each $\alpha \in \mathbb{N}^t$, let $\mathbf{b}^\alpha := b_1^{\alpha_1} \cdots b_d^{\alpha_d} \in K[G]$ and define

$$\mathcal{M} := \{\mathbf{b}^\alpha : \alpha \in \mathbb{N}^d\}.$$

Writing $|\alpha| := \alpha_1 + \ldots + \alpha_d$, we can define

$$\mathcal{M}_{<n} := \{\mathbf{b}^\alpha \in \mathcal{M} : |\alpha| < n\}$$

for each $n \geqslant 0$, the subsets $\mathcal{M}_{=n}$ and $\mathcal{M}_{\geqslant n}$ being defined similarly.

Corollary. $K[G] = J^n \oplus K[\mathcal{M}_{<n}]$ *for all $n \geqslant 0$.*

Proof. The above proposition implies that $J^{n+1} = J^n \oplus K[\mathcal{M}_{=n}]$ for all $n \geqslant 0$. The corollary follows from this by an easy induction. □

6.5. **Subgroups.** Recall the notation of §6.3, so that $\{g_1^p, \ldots, g_t^p, g_{t+1}, \ldots, g_d\}$ is a topological generating set for G_1. Now define

$$\mathcal{N} := \{\mathbf{b}^\alpha \in \mathcal{M} : p|\alpha_i \quad \text{for all} \quad i \leqslant t\}$$

and note that the K-linear span $K[\mathcal{N}]$ of $\mathcal{N}$ is contained in $K[G_1]$.

Lemma. *(a) $K[\mathcal{N}]$ is dense in $K[G_1]$ with respect to the J-adic topology.*
(b) $K[\mathcal{N}] \cap J^n = K[\mathcal{N} \cap \mathcal{M}_{\geqslant n}]$, for all $n \geqslant 0$.
(c) The image of $\operatorname{gr} K[\mathcal{N}]$ inside $\operatorname{gr} K[G]$ is equal to $K[y_1^p, \ldots, y_t^p, y_{t+1}, \ldots, y_d]$.

Proof. (a) Let $x \in G_1$ and $n \geqslant 0$. It will be enough to show that $x \equiv y \mod J^n$ for some $y \in K[\mathcal{N}]$. Since G/G^{p^n} is a finite powerful p-group, by [DDMS, Corollary 2.8] we can find non-negative integers $\lambda_1, \ldots, \lambda_d$ such that

$$x = g_1^{\lambda_1} \cdots g_d^{\lambda_d} u$$

for some $u \in G^{p^n}$. Considering the image of x in G/G^p and using the fact that $x \in G_1$, we see that λ_i is divisible by p for all $i \leqslant t$. Write $\lambda_i = p\mu_i$ for some $\mu_i \in \mathbb{N}$, for each $i \leqslant t$. Let $y := g_1^{\lambda_1} \cdots g_d^{\lambda_d}$; then

$$y = (1 + b_1^p)^{\mu_1} \cdots (1 + b_t^p)^{\mu_t} (1 + b_{t+1})^{\lambda_{t+1}} \cdots (1 + b_d)^{\lambda_d} \in K[\mathcal{N}].$$

Because $G^{p^n} - 1 \subseteq J^n$, the element u is congruent to 1 modulo J^n, and hence

$$x = yu \equiv y \mod J^n$$

as required.

(b) It will be enough to show that $K[\mathcal{N}] \cap J^n \subseteq K[\mathcal{N} \cap \mathcal{M}_{\geqslant n}]$, so let $a \in K[\mathcal{N}] \cap J^n$. We can decompose a uniquely as $a = b + c$, where $b \in K[\mathcal{N} \cap \mathcal{M}_{<n}]$ and $c \in K[\mathcal{N} \cap \mathcal{M}_{\geqslant n}]$. Now $c \in K[\mathcal{M}_{\geqslant n}] \subseteq J^n$ so $b = a - c \in J^n \cap K[\mathcal{M}_{<n}] = 0$ by Corollary 6.4. Hence $a = c \in K[\mathcal{N} \cap \mathcal{M}_{\geqslant n}]$, as required.

(c) This follows immediately from part (b). □

6.6. **Completed group algebras.** Let H be a compact p-adic analytic group. The *completed group algebra* KH is by definition the inverse limit

$$KH := \varprojlim K[H/N],$$

as N runs over all the open normal subgroups of H. When the field K is finite, this algebra is sometimes called the *Iwasawa algebra* of H.

Proposition. *Let $A := KG$ and $A_1 := KG_1$. Then (A, A_1) is a Frobenius pair.*

Proof. For each open normal subgroup N of G, let $w_{N,G}$ be the kernel of the natural map from $K[G]$ to $K[G/N]$. By the proof of [DDMS, Lemma 7.1], this family of ideals of $K[G]$ is cofinal with the powers of the augmentation ideal $J = w_{G,G}$. Therefore A is isomorphic to the completion of $K[G]$ with respect to the J-adic filtration on $K[G]$. Let $(F_n A)$ be the associated filtration on A; explicitly,

$$F_n A := \begin{cases} \overline{J^{-n}} & \text{if} \quad n \leqslant 0 \\ A & \text{otherwise.} \end{cases}$$

In this way, A becomes a complete filtered K-algebra, and

$$B := \operatorname{gr} A \cong \operatorname{gr} K[G] \cong K[y_1, \ldots, y_d]$$

is a commutative noetherian domain, by Proposition 6.4.

Now if N is an open normal subgroup of G, then $N \cap G_1$ is an open normal subgroup of G_1 and

$$w_{N,G} \cap K[G_1] = w_{N \cap G_1, G_1}.$$

Conversely, if N_1 is an open normal subgroup of G_1, then we can find an open normal subgroup N of G such that $N \cap G_1 \subseteq N_1$, so that

$$w_{N_1,G_1} \supseteq w_{N \cap G_1, G_1} = w_{N,G} \cap K[G_1].$$

Hence the subspace topology on $K[G_1]$ induced from the J-adic topology on $K[G]$ coincides with the natural topology on $K[G_1]$ used in the definition of A_1. We may therefore identify A_1 with the closure of $K[G_1]$ inside A. In this way A_1 becomes a closed subalgebra of A.

Finally, Lemma 6.5 implies that the image of $\operatorname{gr} A_1 \cong \operatorname{gr} K[G_1] \cong \operatorname{gr} K[\mathcal{N}]$ inside $\operatorname{gr} A$ can be identified with the subalgebra $B_1 := K[y_1^p, \ldots, y_t^p, y_{t+1}, \ldots, y_d]$ of B. This clearly contains $B^{[p]}$ and moreover

$$B = \bigoplus_{\alpha \in [p-1]^t} B_1 \mathbf{y}^\alpha,$$

as required. $\square$

6.7. **Sources of derivations for Iwasawa algebras.**

Proposition. *Let $u \in L$ be such that $[u, L] \subseteq p^k L$ and $[u, L_1] \subseteq p^{k+1} L$ for some $k \geqslant \epsilon$, and let $a = \exp(u)$. Then*

(a) $(a, G) \subseteq G^{p^k}$,
(b) $(a, G_1) \subseteq G^{p^{k+1}}$,
(c) $[a, F_n A] \subseteq F_{n-p^k+1} A$ *for all* $n \in \mathbb{Z}$, *and*
(d) $[a, F_n A_1] \subseteq F_{n-p^{k+1}+p} A$ *for all* $n \in \mathbb{Z}$.

Proof. Parts (a) and (b) follow from Proposition 6.2:

$$\begin{array}{rcccccl} (a, G) & = & (\exp(u), \exp(L)) & \subseteq & \exp([u, L]) G^{p^{k+1}} & \subseteq & G^{p^k} \quad \text{and} \\ (a, G_1) & = & (\exp(u), \exp(L_1)) & \subseteq & \exp([u, L_1]) G^{p^{k+1}} & = & G^{p^{k+1}}. \end{array}$$

(c) It is sufficient to prove this for non-positive values of n, since then

$$[a, F_n A] = [a, F_0 A] \subseteq F_{-p^k+1} A \subseteq F_{n-p^k+1} A$$

for all $n \geqslant 0$. Let $h \in G$ and set $b := h - 1$. Then

$$[a, b] = [a, h] = ha((a, h) - 1) \in K[G](G^{p^k} - 1) \subseteq J^{p^k}$$

by (a), so by induction we have

$$[a, b^m] = b[a, b^{m-1}] + [a, b] b^{m-1} \in J^{p^k+m-1}$$

for all $m \geqslant 0$. Therefore

$$[a, \mathbf{b}^\alpha] = [a, b_1^{\alpha_1}] b_2^{\alpha_2} \cdots b_d^{\alpha_d} + \cdots + b_1^{\alpha_1} \cdots b_{d-1}^{\alpha_{d-1}} [a, b_d^{\alpha_d}] \in J^{|\alpha| + p^k - 1}$$

for all $\mathbf{b}^\alpha \in \mathcal{M}$. Now $K[\mathcal{M}_{\geqslant -n}]$ is dense in $F_n A$, so

$$[a, F_n A] = \overline{[g, K[\mathcal{M}_{\geqslant -n}]]} \subseteq \overline{J^{-n+p^k-1}} = F_{n-p^k+1} A,$$

as required.

(d) Again, we may assume that $n \leqslant 0$. Let $h \in G_1$ and set $b = h - 1$. Then

$$[a, b] = [a, h] = ha((a, h) - 1) \in K[G](G^{p^{k+1}} - 1) \subseteq J^{p^{k+1}}$$

by (b). Hence in the notation of §6.5, $[a, b_i^{pm}] \in J^{pm+p^{k+1}-p}$ for all $i \leqslant t$ and $[a, b_i^m] \in J^{m+p^{k+1}-1} \subseteq J^{m+p^{k+1}-p}$ for all $i > t$, whenever $m \geqslant 0$. We can now deduce as in part (a) that

$$[a, \mathbf{b}^\alpha] \in J^{|\alpha|+p^{k+1}-p}$$

for all $\mathbf{b}^\alpha \in \mathcal{N}$, or equivalently, $[a, \mathcal{N} \cap \mathcal{M}_{\geqslant -n}] \subseteq J^{-n+p^{k+1}-p}$. Part (d) now follows because $K[\mathcal{N} \cap \mathcal{M}_{\geqslant -n}]$ is dense in $F_n A_1$ by Lemma 6.5. □

Corollary. *Let $u \in L$ be such that $[u, L] \subseteq p^k L$ and $[u, L_1] \subseteq p^{k+1} L$ for some $k \geqslant \epsilon$, and let $a = \exp(u) \in G$. Then $\mathbf{a} = \{a, a^p, a^{p^2}, \ldots\}$ is a source of derivations for the Frobenius pair (A, A_1).*

Proof. For all $r \geqslant 0$, $[p^r u, L] \subseteq p^{r+k} L$ and $[p^r u, L_1] \subseteq p^{r+k+1} L$. Now let $\theta(a^{p^r}) = p^{r+k} - 1$ and $\theta_1(a^{p^r}) = p\theta(a^{p^r})$ and apply the proposition. □

In particular, if G is a uniform pro-p group and $g \in G$, then $g = \exp(u)$ for some $u \in L$. Since L is powerful, $[u, L] \subseteq p^\epsilon L$ and $[u, pL] \subseteq p^{\epsilon+1} L$. Hence $(g, g^p, g^{p^2}, \ldots)$ is always a source of derivations for (KG, KG^p).

6.8. **Computing the corresponding derivations.** Let $u \in L$ be such that for some $k \geqslant \epsilon$, we have

- $[u, L] \subseteq p^k L$
- $[u, L] \nsubseteq p^{k+1} L$, and
- $[u, L_1] \subseteq p^{k+1} L$.

Note that if such a k exists, then it is uniquely determined by u. Moreover, if $L_1 = pL$, then the third condition automatically follows from the first, and in this case such an integer k always exists for any non-central element u of L.

We can now define a well-defined non-zero $\mathbb{F}_p$-linear map

$$\begin{array}{rccc} \rho_u : & L/L_1 & \to & L/pL \\ & v + L_1 & \mapsto & \frac{1}{p^k}[u, v] + pL. \end{array}$$

Let $a = \exp(u)$. Since $[a, F_n A] \subseteq F_{n-p^k+1} A$ for all $n \in \mathbb{Z}$ by Proposition 6.7(c), u induces a derivation

$$D_u := \{a, -\}_{p^k - 1}$$

of $B = K[y_1, \ldots, y_d]$ as in §3.2. It turns out that there is a very close connection between D_u and ρ_u. Recall from §6.3 that $\{v_i + L_1 : 1 \leqslant i \leqslant t\}$ is an $\mathbb{F}_p$-basis for L/L_1, and $\{v_i + pL : 1 \leqslant i \leqslant d\}$ is an $\mathbb{F}_p$-basis for L/pL.

Theorem. *Let (c_{ij}) be the matrix of ρ_u with respect to these bases. Then*

$$D_u(y_j) = \sum_{i=1}^{d} c_{ij} y_i^{p^k}$$

for all $j = 1, \ldots, t$.

Proof. Choose $\lambda_{ij} \in [p-1]$ such that c_{ij} is the reduction of λ_{ij} modulo p. By the definition of c_{ij},

$$\frac{1}{p^k}[u, v_j] \equiv \sum_{i=1}^{d} \lambda_{ij} v_i \mod pL$$

for all $j = 1, \ldots, t$. Recall from §6.3 that $g_i = \exp(v_i)$ for all i. By Lemma 6.2(d),

$$\exp\left(\frac{1}{p^k}[u, v_j]\right) \equiv \prod_{i=1}^{d} g_i^{\lambda_{ij}} \mod G^p.$$

Now by [DDMS, Theorem 3.6(iv)], $g \mapsto g^{p^k}$ induces an isomorphism between G/G^p and $G^{p^k}/G^{p^{k+1}}$. Using Lemma 6.2(a), we see that

$$\exp([u, v_j]) = \exp\left(\frac{1}{p^k}[u, v_j]\right)^{p^k} \equiv \prod_{i=1}^{d} g_i^{p^k \lambda_{ij}} \mod G^{p^{k+1}}.$$

We can now apply Proposition 6.2 and deduce that

$$(a, g_j) \equiv \exp([u, v_j]) \equiv \prod_{i=1}^{d} g_i^{p^k \lambda_{ij}} \mod G^{p^{k+1}}.$$

Next, recall that $b_j = g_j - 1$ and consider the commutator $[a, b_j]$ inside $K[G]$:

$$[a, b_j] = [a, g_j] = g_j a((a, g_j) - 1) = g_j a \left(h_j \prod_{i=1}^{d} g_i^{p^k \lambda_{ij}} - 1\right)$$

for some $h_j \in G^{p^{k+1}}$. Since we're interested in $\{a, -\}_{p^k - 1}$, we only need to compute $[a, b_j]$ modulo J^{p^k+1}. Now $h_j - 1 \subseteq G^{p^{k+1}} - 1 \subseteq J^{p^{k+1}} \subseteq J^{p^k+1}$, so

$$h_j \equiv 1 \mod J^{p^k+1}.$$

Because $g_j a \equiv 1 \mod J$, we can deduce that

$$[a, b_j] \equiv \prod_{i=1}^{d} (1 + b_i^{p^k})^{\lambda_{ij}} - 1 \equiv \sum_{i=1}^{d} c_{ij} b_i^{p^k} \mod J^{p^k+1}$$

for all $j = 1, \ldots, t$. The result follows. □

6.9. **Verifying the derivation hypothesis.** In a forthcoming paper [AWZ], we will prove the following result.

Theorem. [AWZ, Theorem A] *Let $\Phi(\mathbb{Z}_p)$ be the Chevalley $\mathbb{Z}_p$-Lie algebra associated to a root system Φ. Let L be the Lie algebra $p^t\Phi(\mathbb{Z}_p)$ for some $t \geqslant 1$ and G be the corresponding uniform pro-p group $\exp(L)$. Suppose that $p \geqslant 5$ and that $p \nmid n + 1$ if Φ has an indecomposable component of type A_n. Then (KG, KG^p) satisfies the derivation hypothesis.*

For the time being, we only verify that the derivation hypothesis holds in the special case when G is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$.

6.10. **Congruence subgroups of $\mathrm{SL}_2(\mathbb{Z}_p)$, $p \geqslant 3$.** Fix an integer $l \geqslant 1$ and let L be the powerful Lie algebra $\mathfrak{sl}_2(p^l\mathbb{Z}_p)$. Thus L has a basis

$$\left\{ e = \begin{pmatrix} 0 & p^l \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ p^l & 0 \end{pmatrix}, h = \begin{pmatrix} p^l & 0 \\ 0 & -p^l \end{pmatrix} \right\}$$

satisfying the following relations:

- $[h, e] = 2p^l e$,
- $[h, f] = -2p^l f$,
- $[e, f] = p^l h$.

Let $\Gamma_l(\mathrm{SL}_2(\mathbb{Z}_p))$ denote the *l-th congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z}_p)$:

$$\Gamma_l(\mathrm{SL}_2(\mathbb{Z}_p)) := \ker\left(\mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{Z}/p^l\mathbb{Z})\right).$$

It is well known that $G := \exp(L)$ is isomorphic to $\Gamma_l(\mathrm{SL}_2(\mathbb{Z}_p))$. We let $L_1 = pL$, so that the corresponding subgroup G_1 is just $G^p \cong \Gamma_{l+1}(\mathrm{SL}_2(\mathbb{Z}_p))$.

We use the same variables $\{e, f, h\}$ for the generators of the associated graded ring $B = \mathrm{gr}\, KG$ and hope that this will cause no confusion. Thus

$$B = K[e, f, h] \quad \text{and} \quad B_1 = K[e^p, f^p, h^p].$$

Let $\{\frac{\partial}{\partial e}, \frac{\partial}{\partial f}, \frac{\partial}{\partial h}\}$ be the corresponding derivations, which were constructed in §2.4. Using Theorem 6.8 and Proposition 2.4(b), we can write down the derivations

$$D_{p^r u} = \{\exp(p^r u), -\}_{p^{r+l}-1} : B \to B$$

generated by u explicitly, for each $u \in \{e, f, h\}$:

$$\begin{array}{rcl} D_{p^r e} & = & h^{p^{l+r}} \frac{\partial}{\partial f} - 2e^{p^{l+r}} \frac{\partial}{\partial h}, \\ D_{p^r f} & = & -h^{p^{l+r}} \frac{\partial}{\partial e} + 2f^{p^{l+r}} \frac{\partial}{\partial h}. \\ D_{p^r h} & = & 2e^{p^{l+r}} \frac{\partial}{\partial e} - 2f^{p^{l+r}} \frac{\partial}{\partial f}. \end{array}$$

Proposition. *Let $l \geqslant 1$ and let $G = \exp(\mathfrak{sl}_2(p^l\mathbb{Z}_p))$ as above. Then the Frobenius pair (KG, KG^p) satisfies the derivation hypothesis.*

Proof. Let X, Y be homogeneous elements of B and suppose that Y lies in the $\mathbf{a}$-closure of XB for all $\mathbf{a} \in \mathcal{S}(KG, KG^p)$. By Corollary 6.7, $(g, g^p, g^{p^2}, \ldots) \in \mathcal{S}(KG, KG^p)$ for all $g \in G$, so we can find an integer s such that

$$D_{p^r u}(Y) \in XB$$

for all $u \in \{e, f, h\}$ and all $r \geqslant s$. Consider the $D_{p^r e}$–equations for $r = s$ and $r = s + 1$. Eliminating the terms involving $\partial Y/\partial f$ yields that

$$2e^{p^{s+l}}\left(h^{p^{s+l}(p-1)} - e^{p^{s+l}(p-1)}\right)\frac{\partial Y}{\partial h} \in XB,$$

and using similar operations with the $D_{p^r f}$-equations we have

$$2f^{p^{s+l}}\left(h^{p^{s+l}(p-1)} - f^{p^{s+l}(p-1)}\right)\frac{\partial Y}{\partial h} \in XB.$$

The coefficients of $\partial Y/\partial h$ appearing in the above two equations are coprime, which allows us to deduce

$$\frac{\partial Y}{\partial h} \in XB.$$

Similar manipulations with the other equations show that $\partial Y/\partial e$ and $\partial Y/\partial f$ also lie in XB. Hence $\mathcal{D}(Y) \subseteq XB$, by Proposition 2.4(b). □

7. Ideals in Iwasawa algebras

7.1. **Canonical dimension function.** Let A be a noetherian ring. We say that A is *Gorenstein* if it has finite injective dimension on both sides. For any finitely generated left (or right) A-module M, the *j-number* or *grade* of M is defined to be

$$j(M) := \inf\{n \mid \mathrm{Ext}^n_A(M, A) \neq 0\}.$$

The ring A is called *Auslander-Gorenstein* if it is Gorenstein and it satisfies the *Auslander condition*:

For every finitely generated left (respectively, right) A-module M and every positive integer q, one has $j(N) \geqslant q$ for every finitely generated right (respectively, left) A-submodule $N \subseteq \operatorname{Ext}^q_A(M, A)$.

An *Auslander-regular* ring is a noetherian, Auslander-Gorenstein ring which has finite global dimension. See [Bj] for some details. Note that a noetherian commutative regular algebra is always Auslander-regular. For any Auslander-Gorenstein ring A, there is a *canonical dimension function* defined by

$$\operatorname{Cdim}(M) = \operatorname{injdim}(A) - j(M)$$

for all finitely generated left (or right) A-modules M [AB1, §5.3]. This is a dimension function in the sense of [MR, §6.8.4]. Recall that a finitely generated A-module is said to be *pure* if $\operatorname{Cdim}(N) = \operatorname{Cdim}(M)$ for all nonzero submodules N of M. We will use the following nice observation of Venjakob [CSS, Lemma 4.12]:

Lemma. *Let A be an Auslander-regular domain and I be a proper nonzero right ideal of A. Then I is reflexive if and only if A/I is pure of grade* 1.

7.2. **Crossed products.** Let R be an Auslander-Gorenstein ring, G be a finite group and $S = R * G$ be a crossed product. We know by [AB2, Lemma 5.4] that the restriction $M_{|R}$ to R of any finitely generated S-module M satisfies

$$\operatorname{Cdim}_S(M) = \operatorname{Cdim}_R(M_{|R}).$$

Hence S is also Auslander-Gorenstein.

Proposition. *R has an ideal I with $\operatorname{Cdim}_R(R/I) = n$ if and only if S has an ideal J with $\operatorname{Cdim}_S(S/J) = n$.*

Proof. ($\Rightarrow$) Choose a set of units $\{\overline{g} : g \in G\}$ in S such that $R\overline{g} = \overline{g}R$ inside S and $S = \bigoplus_{g \in G} R\overline{g}$. Then $\alpha_g : r \mapsto \overline{g}^{-1} r \overline{g}$ is an algebra automorphism of R. Hence $\operatorname{Cdim}_R(R/\alpha_g(I)) = \operatorname{Cdim}_R(R/I)$ for all $g \in G$. We set $I_0 := \bigcap_{g \in G} \alpha_g(I)$, which is a G-invariant ideal in R. It follows from the fact $I_0 \subseteq I$ that $\operatorname{Cdim}_R(R/I_0) \geqslant \operatorname{Cdim}_R(R/I)$. Since

$$R/I_0 \hookrightarrow \bigoplus_{g \in G} R/\alpha_g(I),$$

we actually have equality. Let us set $J = I_0 \cdot S$; where I_0 is G-invariant, J is a twosided ideal in S and by construction

$$\operatorname{Cdim}_S(S/J) = \operatorname{Cdim}_R((S/J)_{|R}) = \operatorname{Cdim}_R(R/I).$$

($\Leftarrow$) We set $I := J \cap R$, which is a G-invariant ideal in R. Then $S/IS = \bigoplus_{g \in G}(R\overline{g}/I\overline{g})$ and hence $(S/IS)_{|R} \cong (R/I)^{|G|}$. Since $S/IS \twoheadrightarrow S/J$, we have

$$\operatorname{Cdim}_R(R/I) = \operatorname{Cdim}_R((S/IS)_{|R}) \geqslant \operatorname{Cdim}_R((S/J)_{|R}).$$

On the other hand $R/I \hookrightarrow (S/J)_{|R}$, so we have equality and the result follows. $\square$

7.3. **Proof of Theorem A.** We present a slightly more general version of Theorem A this section. Let $\mathcal{L}(G)$ denote the $\mathbb{Q}_p$-Lie algebra of G.

Theorem. *Let K be a field of characteristic p. Suppose G is a compact p-adic analytic group of dimension d such that $\mathcal{L}(G)$ is split semisimple over $\mathbb{Q}_p$. Suppose that $p \geqslant 5$, and that $p \nmid n$ in the case when $\mathfrak{sl}_n(\mathbb{Q}_p)$ occurs as a direct summand of $\mathcal{L}(G)$. Then KG has no two-sided ideals I such that*

$$\operatorname{Cdim}_{KG}(KG/I) = d - 1.$$

Proof. Note that KG is a crossed product of the Auslander-Gorenstein ring KN with the finite group G/N, for any open normal uniform subgroup N of G. By Proposition 7.2, we may replace G by any uniform pro-p group N having the same $\mathbb{Q}_p$-Lie algebra without affecting the conclusion of the Theorem.

By considering a suitable Chevalley basis, we can find a sub $\mathbb{Z}_p$-Lie algebra $L \subset \mathcal{L}(G)$ such that $L \cong p^t\Phi(\mathbb{Z}_p)$ where Φ is the root system associated to $\mathbb{Q}_p \otimes \mathcal{L}(G)$. Now take N to be the corresponding uniform pro-p group $\exp(L)$. The $\mathbb{Z}_p$-Lie algebra of N^{p^k} is p^kL, so the Frobenius pair $(KN^{p^k}, KN^{p^{k+1}})$ satisfies the derivation hypothesis for all $k \geqslant 0$ by Theorem 6.9.

Suppose for a contradiction that I is a two-sided ideal of KN such that

$$\mathrm{Cdim}_{KN}(KN/I) = d - 1.$$

By replacing I by the inverse image of the largest pseudo-null submodule of KN/I in KN we may assume that KN/I is pure. Note that I is proper and *nonzero*, since otherwise $d = \mathrm{Cdim}_{KN}(KN) = d - 1$. It follows from Lemma 7.1 that I is a reflexive ideal of KN. Applying Theorem 5.3 repeatedly, we see that I is controlled by KN^{p^k} for each k:

$$I = (I \cap KN^{p^k}) \cdot KN.$$

Since I is a proper ideal of KN, we see that $I \cap KN^{p^k}$ must be contained in the maximal ideal $(N^{p^k} - 1) \cdot KN^{p^k}$ of KN^{p^k} for all $k \geqslant 0$. Hence

$$I \subseteq \bigcap_{k=0}^{\infty} ((N^{p^k} - 1) \cdot KN) = 0,$$

a contradiction. □

8. The case when $p = 2$

8.1. **Congruence subgroups of** $\mathrm{SL}_2(\mathbb{Z}_p), p = 2$**.** The reader might have wondered why we didn't just assume that $L_1 = pL$ from §6.3 onwards. The reason is that the extra generality allows us to be more flexible when choosing the particular open subgroup of G that we should try to "descend" towards. The case of open subgroups in $\mathrm{SL}_2(\mathbb{Z}_p)$ when $p = 2$ should illustrate this flexibility: if $G = \Gamma_l(\mathrm{SL}_2(\mathbb{Z}_p))$ and $p = 2$, then (KG, KG^p) does not satisfy the derivation hypothesis, but we can circumvent this problem by going down to G^p from G in two steps.

So assume that $p = 2$ and fix $l \geqslant 2$. We choose the same basis $\{e, f, h\}$ for $L_0 := \mathfrak{sl}_2(p^l\mathbb{Z}_p)$ as in §6.10, so that the following relations are satisfied:

- $[h, e] = p^{l+1}e$,
- $[h, f] = -p^{l+1}f$,
- $[e, f] = p^l h$.

Let $L_1 = pe\mathbb{Z}_p \oplus pf\mathbb{Z}_p \oplus h\mathbb{Z}_p$ and let $L_2 = pL$. The relations in L_1

- $[h, pe] = p^{l+1}(pe)$,
- $[h, pf] = -p^{l+1}(pf)$,
- $[pe, pf] = p^{l+2}h$

show that L_1 is a powerful $\mathbb{Z}_p$-subalgebra of L_0 which contains L_2. Moreover, $pL_1 \subseteq L_2$, so the pairs (L_0, L_1) and (L_1, L_2) both satisfy the assumptions made in §6.3, and hence (KG_0, KG_1) and (KG_1, KG_2) are Frobenius pairs, by Proposition 6.6. However the parameter t equals 2 in the first case and 1 in the second case.

Proposition. *Let $G_i = \exp(L_i)$ for each $i = 0, 1, 2$. Then the Frobenius pairs (KG_0, KG_1) and (KG_1, KG_2) both satisfy the derivation hypothesis.*

Proof. We first deal with the case (KG_0, KG_1); in this case, $B = K[e, f, h]$ and $B_1 = K[e^p, f^p, h]$. We observe that

$$\begin{array}{lll} [e, L_0] \subseteq p^l L_0, & [e, L_0] \nsubseteq p^{l+1} L_0, & [e, L_1] \subseteq p^{l+1} L_0, \\ [f, L_0] \subseteq p^l L_0, & [f, L_0] \nsubseteq p^{l+1} L_0, & [f, L_1] \subseteq p^{l+1} L_0, \\ [h, L_0] \subseteq p^{l+1} L_0, & [h, L_0] \nsubseteq p^{l+2} L_0, & [h, L_1] \subseteq p^{l+2} L_0. \end{array}$$

By Theorem 6.8, we obtain three sets of derivations of $B = \operatorname{gr} KG_0$ arising from sources of derivations of (KG_0, KG_1):

$$\begin{array}{rcl} D_{p^r e} & = & h^{p^{l+r}} \frac{\partial}{\partial f}, \\ D_{p^r f} & = & h^{p^{l+r}} \frac{\partial}{\partial e}, \\ D_{p^r h} & = & e^{p^{r+l+1}} \frac{\partial}{\partial e} - f^{p^{r+l+1}} \frac{\partial}{\partial f}. \end{array}$$

Let X, Y be homogeneous elements of B and suppose that Y lies in the $\mathbf{a}$-closure of XB for all $\mathbf{a} \in \mathcal{S}(KG_0, KG_1)$; we can thus find an integer s such that

$$D_{p^r u}(Y) \in XB$$

for all $u \in \{e, f, h\}$ and all $r \geqslant s$. Eliminating the terms involving $\partial Y/\partial f$ from the $D_{p^r h}$ equations for $r = s$ and $r = s + 1$ shows that

$$f^{p^{s+l+1}} \left(f^{p^{s+l+1}(p-1)} + e^{p^{s+l+1}(p-1)} \right) \partial Y/\partial f \in XB$$

Since $D_{p^s e}(Y) = h^{p^{s+l}} \partial Y/\partial f \in XB$ and the coefficients of $\partial Y/\partial f$ are coprime,

$$\partial Y/\partial f \in XB.$$

Similarly $\partial Y/\partial e \in XB$, so the derivation hypothesis holds by Proposition 2.4(b).

Now consider the case (KG_1, KG_2). Recycling notation, let $\{e, f, h\}$ be the basis for L_1 considered above, so that $\{e, f, ph\}$ is a basis for L_2, and the relations

- $[h, e] = p^{l+1} e$,
- $[h, f] = -p^{l+1} f$,
- $[e, f] = p^{l+2} h$

hold in L_1. The corresponding graded rings are $B = K[e, f, h]$ and $B_1 = K[e, f, h^p]$. Since

$$\begin{array}{lll} [e, L_1] \subseteq p^{l+1} L_1, & [e, L_1] \nsubseteq p^{l+2} L_1, & [e, L_2] \subseteq p^{l+2} L_1, \\ [f, L_1] \subseteq p^{l+1} L_1, & [f, L_1] \nsubseteq p^{l+2} L_1, & [f, L_2] \subseteq p^{l+2} L_1, \end{array}$$

Theorem 6.8 gives us two sets of derivations of B arising from sources of derivations of (KG_1, KG_2):

$$\begin{array}{rcl} D_{p^r e} & = & e^{p^{l+r+1}} \frac{\partial}{\partial h}, \\ D_{p^r f} & = & f^{p^{l+r+1}} \frac{\partial}{\partial h}. \end{array}$$

Let X, Y be homogeneous elements of B and suppose that Y lies in the $\mathbf{a}$-closure of XB for all $\mathbf{a} \in \mathcal{S}(KG_1, KG_2)$; we can thus find an integer s such that

$$D_{p^r u}(Y) \in XB$$

for all $u \in \{e, f\}$ and all $r \geqslant s$. In particular, $D_{p^r e}(Y) = e^{p^{r+l+1}} \partial Y/\partial h$ and $D_{p^r f}(Y) = f^{p^{r+l+1}} \partial Y/\partial h$ both lie in XB. Since the coefficients of $\partial Y/\partial h$ are coprime, $\partial Y/\partial h \in XB$, so the derivation hypothesis holds. $\square$

Corollary. *Let K be a field of characteristic 2 and suppose that G is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$. Then KG has no two-sided ideals I such that*

$$\mathrm{Cdim}_{KG}(KG/I) = 2.$$

Proof. Follow the proof of Theorem A. $\square$

8.2. **Proof of Theorem C.** Let I be a prime ideal of KG. The dimension of G is three, so the possible values for $c = \mathrm{Cdim}_{KG}(KG/I)$ when I is a two-sided ideal of KG are $0, 1, 2$ or 3. By Theorem 7.3 and Corollary 8.1, c cannot be equal to 2 and by [A, Theorem A], c cannot be equal to 1. Hence $c = 0$, in which case I is the maximal ideal of KG since KG is local, or $c = 3$ in which case $I = 0$. $\square$

Acknowledgments

The authors thank Quanshui Wu for useful conversations. The first author would like to thank Simon Wadsley and Sukhendu Mehrotra for helpful comments, and the Department of Pure Mathematics at the University of Sheffield for financial support. Wei is supported by a research fellowship from the China Scholarship Council and by the Department of Mathematics at the University of Washington. Zhang is supported by the US National Science Foundation and the Royalty Research Fund of the University of Washington.

References

[A] K. Ardakov, *Prime ideals in noncommutative Iwasawa algebras*, Math. Proc. Camb. Phil. Soc., **141** (2006), 197-203.

[A2] K. Ardakov, *Centres of skewfields and completely faithful Iwasawa modules*, preprint.

[AB1] K. Ardakov and K. A. Brown, *Ring-theoretic properties of Iwasawa algebras: a survey*, Documenta Math., Extra Volume Coates (2006), 7-33.

[AB2] K. Ardakov and K. A. Brown, *Primeness, semiprimeness and localisation in Iwasawa algebras*, Trans. Amer. Math. Soc., **359** (2007), 1499-1515.

[AVV] M. J. Asensio, M. Van den Bergh and F. Van Oystaeyen, *A new algebraic approach to microlocalization of filtered rings*, Trans. Amer. Math. Soc., **316** (1989), 537-553.

[AWZ] K. Ardakov, F. Wei, J. J. Zhang, *Nonexistence of reflexive ideals in Iwasawa algebras of Chevalley type*, preprint.

[BCA] N. Bourbaki, *Commutative algebra*, Hermann (1972).

[BFP] J. Bell, J. Farina and C. Pendergrass-Rice, Stably Just Infinite Rings, preprint, (2007) arXiv:math/0703774.

[Bj] J.-E. Björk, The Auslander condition on noetherian rings, Séminaire d'Algbre Paul Dubreil et Marie-Paul Malliavin, 39ème Année (Paris, 1987/1988), 137–173, Lecture Notes in Math., 1404, Springer, Berlin, 1989.

[CSS] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), 73–108.

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163-208.

[DDMS] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal, *Analytic pro−p groups*, 2nd edition, Cambridge University Press, (1999).

[FS] D.R. Farkas and L.W. Small, Algebras which are nearly finite dimensional and their identities, Israel J. Math. **127** (2002), 245–251.

[I] I. Ilani, *Analytic pro-p groups and their Lie algebras*, J. Algebra **176** (1995), 34–58.

[La] M. Lazard, Groupes Analytiques p-adiques, Publ. Math. IHES **26** (1965), 389-603.

[Li] H. Li, *Lifting Ore sets of noetherian filtered rings and applications*, J. Algebra **179** (1996), 686-703.

[LV] H. Li and F. Van Oystaeyen, *Zariskian filtrations*, Kluwer Academic Publishers, K-Monographs in Mathematics, Vol. **2** (1996).

[MaR] G. Maury and J. Raynaud, *Ordres Maximaux au Sens de K. Asano*, Lecture Notes in Math. Vol. **808**, Springer, 1980.

[MR] J. C. McConnell, J. C. Robson, *Noncommutative Noetherian rings*, AMS Graduate Studies in Mathematics, Vol. **30** (2001).

[OV] Y. Ochi and O. Venjakob, On the structure of Selmer groups over p-adic Lie extensions, J. Algebraic Geom. **11** (2002), no. 3, 547–580.

[V1] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*. J. Eur. Math. Soc.(JEMS), **4** (2002), 271-311.

[V2] O. Venjakob, *A noncommutative Weierstrass preparation theorem and applications to Iwasawa Theory*. J. Reine. Angew. Math., **559** (2003), 153-191.

[V3] O. Venjakob, On the Iwasawa theory of p-adic Lie extensions, Compositio Math. **138** (2003), no. 1, 1–54.

(K. Ardakov) School of Mathematical Sciences, University of Nottingham, University Park, Nottingham, NG7 2RD, United Kingdom

E-mail address: Konstantin.Ardakov@nottingham.ac.uk

(F. Wei) Department of Applied Mathematics, Beijing Institute of Technology, Beijing, 100081, P. R. China

E-mail address: daoshuo@bit.edu.cn

(J. J. Zhang) Department of Mathematics, Box 354350, University of Washington, Seattle, Washington 98195, USA

E-mail address: zhang@math.washington.edu