Krull dimension of Iwasawa algebras and some related topics.

Konstantin Ardakov,

Christ's College.

A dissertation submitted for the degree of
Doctor of Philosophy at the University of Cambridge.

March, 2004.

Abstract

Let G be a uniform pro-p group. We study certain algebraic properties of the completed group algebra $\Lambda_G = \mathbb{Z}_p[[G]]$ of G and of other related rings.

First, we consider the Krull dimension $\mathcal{K}(\Lambda_G)$ of Λ_G. We establish upper and lower bounds on $\mathcal{K}(\Lambda_G)$ in terms of the $\mathbb{Q}_p$-Lie algebra $\mathcal{L}(G)$ of G. We show these bounds coincide in certain cases, including when $\mathcal{L}(G)$ is solvable, and equal $\dim G + 1$. We also show that $\mathcal{K}(\Lambda_G) < \dim G + 1$ when $\mathcal{L}(G)$ is split simple over $\mathbb{Q}_p$. This answers a question of Brown, Hajarnavis and McEacharn.

Next we study 1-critical modules over the $\mathbb{F}_p$-version of Iwasawa algebras, $\Omega_G = \mathbb{F}_p[[G]]$. We show that the endomorphism ring of such a module M is finite dimensional over $\mathbb{F}_p$ and that $\mathcal{K}(\Omega_G/\operatorname{Ann}(M)) \geq 2$, whenever $\mathcal{L}(G)$ is split semisimple over $\mathbb{Q}_p$. We also establish a useful technical result which allows us to compute the centre of Ω_G as well as obtain information about endomorphism rings of certain induced modules for Ω_G.

Finally, we show that a deformation of Λ_G is naturally isomorphic to a completed universal enveloping algebra $\Pi_{\mathfrak{g}}$. This allows Λ_G to be embedded into a ring whose multiplication is easier to understand. We also compute the centre of $\Pi_{\mathfrak{g}}$, in the case when $\mathcal{L}(G)$ is split semisimple over $\mathbb{Q}_p$.

Preface

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration. The work contained herein is entirely original, except where explicit reference is made to the work of others or where results are described as well known. Furthermore, I declare that this dissertation is not substantially the same as any I have submitted for a degree or diploma or any other qualification at any other university and that no part of it has already been or is being concurrently submitted for any such degree, diploma or other qualification.

I would like to thank my supervisor Dr Chris Brookes for introducing me to this subject and for many helpful conversations. Thanks are also due to Simon Wadsley for his continued interest in my work.

This research was supported by an EPSRC studentship.

Contents

Chapter 1

Introduction

In recent years, there has been an increased amount of interest in completed group algebras (Iwasawa algebras)

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

of compact p-adic Lie groups G, for example, because of their connections with number theory and arithmetic geometry; see the paper by Coates, Schneider and Sujatha ([6]) for more details.

When G is a uniform pro-p group, Λ_G is a concrete example of a complete local Noetherian ring (noncommutative, in general) with good homological properties. We will mainly be concerned with the representation theory of Λ_G and with the algebraic structure of several rings closely related to Λ_G.

We begin by giving a discussion of filtered rings, pro-p groups, Iwasawa algebras and other subjects in Chapter 2, which is used as a foundation for the remainder of this thesis.

We study the Krull (Gabriel-Rentschler) dimension $\mathcal{K}(\Lambda_G)$ of Λ_G in Chapter 3. This study is motivated by the following question of Brown, Hajarnavis and MacEacharn:

Question ([1], Section 5). *Let R be a local right Noetherian ring, whose Jacobson radical satisfies the Artin-Rees property. Is the Krull dimension of R always equal to the global dimension of R?*

First, we reduce the problem of computing $\mathcal{K}(\Lambda_G)$ to that of computing $\mathcal{K}(\Omega_G)$, where $\Omega_G := \Lambda_G/p\Lambda_G$ is the $\mathbb{F}_p$-version of Iwasawa algebras (3.1.4). Then we establish a general lower bound on $\mathcal{K}(\Omega_G)$ in 3.2.2. Finally, we establish an upper bound on $\mathcal{K}(\Omega_G)$, when $p \geq 5$ and the Lie algebra of G is split simple over $\mathbb{Q}_p$ (3.3.1). This allows us to deduce a negative answer to the above question in 3.4.5.

In the first half of Chapter 4, we compute the centre $Z(\Omega_G)$ of Ω_G for an arbitrary pro-p group G (4.1.2). In the case when G is uniform, $Z(\Omega_G) = \Omega_Z$ where Z is the centre of G (4.1.3). We also determine when the endomorphism ring of a certain induced module for Ω_G is finite dimensional over $\mathbb{F}_p$ (4.2.1).

Because the Iwasawa algebra Ω_G is local, it has a unique simple module - the vector space $\mathbb{F}_p$ with trivial G-action. This motivates the study of Krull 1-critical modules for Ω_G - modules which are not Artinian, but whose every quotient is finite dimensional over $\mathbb{F}_p$ (these are also known as *just infinite* modules). The idea is to view these as some kind of substitute for the simple modules.

We obtain some results about these modules in the second half of Chapter 4, when G is a uniform pro-p group with split semisimple $\mathbb{Q}_p$-Lie algebra

$\mathcal{L}(G)$. It is shown that the endomorphism ring of any such module M is finite dimensional over $\mathbb{F}_p$ (4.3.1). Also, we give a lower bound of 2 on the Krull dimension of the ring $\Omega_G/\operatorname{Ann}(M)$ in 4.4.1. This shows that annihilators of 1-critical modules are "small" in some sense.

In Chapter 5, we study the completed universal enveloping algebra $\Pi_\mathfrak{g}$ of a $\mathbb{Z}_p$-Lie algebra $\mathfrak{g}$ which is free of finite rank over $\mathbb{Z}_p$. It turns out that when $\mathfrak{g} = p^{-1}L_G$ for some uniform pro-p group G, Λ_G embeds naturally into $\Pi_\mathfrak{g}$ (5.1.4) and that $\Pi_\mathfrak{g}$ can be viewed as an analytic deformation of Λ_G (5.1.5).

The multiplication in $\Pi_\mathfrak{g}$ is easier to understand than that in Λ_G, so we hope that this embedding will yield further information about Λ_G and its modules in the future. For the time being, we make do by computing the centre of $\Pi_\mathfrak{g}$ in the case when $\mathfrak{g}$ is the $\mathbb{Z}_p$-form of a complex semisimple Lie algebra (5.2.1). This involves making some restrictions on the prime p.

All rings that we will consider are associative with 1. The term "module" will mean right module, unless specified otherwise. Since all examples that we consider arise from a group or a Lie algebra, we could equally well deal with left modules, and all our results will hold. When we say that a ring is Noetherian, we mean it is both right and left Noetherian. The symbol p will always denote a fixed prime.

Chapter 2

Preliminaries

2.1 Filtrations, completions and gradations

One of the most fruitful ring-theoretic techniques which can be applied to the study of Iwasawa algebras is the approach via filtered rings and their associated graded rings. The idea is that by filtering the object in question and then studying the associated graded object, one obtains something which is easier to understand but which nonetheless retains a lot of information about the original object. Since Iwasawa algebras can be defined by completing a certain group algebra with respect to a suitable filtration, we first develop the required machinery involving filtrations, completions and gradations in this section.

Unless stated otherwise, R denotes a ring and M denotes an R-module.

Definition 2.1.1. *A* filtration *on R is a set of additive subgroups $FR = \{F_nR : n \in \mathbb{Z}\}$, satisfying $1 \in F_0R$, $F_nR \subseteq F_{n+1}R$ and $F_nR.F_mR \subseteq F_{n+m}R$ for all $n, m \in \mathbb{Z}$, and $\cup_{n\in\mathbb{Z}}F_nR = R$. If R has a filtration, R is said to be a* filtered ring.

Note that if R is a filtered ring, F_0R is automatically a subring of R.

Definition 2.1.2. *Let R be a filtered ring, M an R-module. A* filtration *on M is a set of additive subgroups of M, $FM = \{F_nM : n \in \mathbb{Z}\}$, satisfying $F_nM \subseteq F_{n+1}M$ and $F_nM.F_mR \subseteq F_{n+m}M$ for all $n, m \in \mathbb{Z}$ and $\cup_{n\in\mathbb{Z}}F_nM = M$. If M has a filtration, M is said to be a* filtered R-module. *The filtration on M is said to be*

(i) Separated *if $\cap_{n\in\mathbb{Z}}F_nM = 0$*

(ii) Negative *if $F_nM = M$ for all $n \geq 0$*

(iii) Positive *if $F_nM = 0$ for all $n < 0$.*

A notable example of a filtration on R is the I-adic filtration where I is a two-sided ideal of R, given by $F_nR := I^{-n}$ if $n \leq 0$ and $F_nR = R$ otherwise. This is a negative filtration. Also note that R itself becomes a filtered R-module with the given filtration FR.

If N is a submodule of M, a filtered R-module, we can use the filtration on M to define filtrations on N and M/N: $F_nN := F_nM \cap N$ (the *induced* filtration) and $F_n(M/N) := (F_nM + N)/N$ (the *quotient* filtration). Note that if FM is separated then so is FN, but $F(M/N)$ need not be, in general.

Given a filtered ring R and a filtered R-module M, we can associate with R and M certain graded rings and modules, as follows.

Let $\operatorname{gr} M := \oplus_{n\in\mathbb{Z}}F_nM/F_{n-1}M$. Let $e_n : F_nM/F_{n-1}M \to \operatorname{gr} M$ denote the canonical injection of $F_nM/F_{n-1}M$ into the direct sum. For $x \in M$ define the *degree* $\deg(x)$ of x to be the integer n such that $x \in F_nM\backslash F_{n-1}M$;

if no such n exists, define $\deg(x) = -\infty$. Also define the *symbol* of x to be $\sigma(x) := e_n(x + F_{n-1}M)$ where $n = \deg(x)$, and $\sigma(x) := 0$ if $\deg(x) = -\infty$.

Definition 2.1.3. $\operatorname{gr} R = \oplus_{n\in\mathbb{Z}} F_nR/F_{n-1}R$ *forms a graded ring with multiplication given by* $\sigma(x).\sigma(y) = e_{\deg(x)+\deg(y)}(xy)$ *for* $x, y \in R$*, called the* associated graded ring *of* R*.*

$\operatorname{gr} M = \oplus_{n\in\mathbb{Z}} F_nM/F_{n-1}M$ *forms a graded* $\operatorname{gr} R$*-module with the* $\operatorname{gr} R$*-action given by* $\sigma(x).\sigma(y) = e_{\deg(x)+\deg(y)}(xy)$ *for* $x \in M, y \in R$*, called the* associated graded module *of* M*.*

Note that if $\sigma(x)\sigma(y) \neq 0$ for $x, y \in R$, then the definition of multiplication simplifies down to $\sigma(x)\sigma(y) = \sigma(xy)$.

Associated graded modules behave well with respect to induced and quotient filtrations. In particular, we have the easily checked

Lemma 2.1.4. *Suppose* $0 \to N \to M \to M/N \to 0$ *is an exact sequence of* R*-modules, where* R *is a filtered ring,* M *is a filtered* R*-module and* N*,*M/N *are equipped with the induced and quotient filtrations, respectively. Then there is an exact sequence* $0 \to \operatorname{gr} N \to \operatorname{gr} M \to \operatorname{gr} M/N \to 0$ *of* $\operatorname{gr} R$ *modules.*

Given a filtered ring R and a filtered R-module M, we can associate with M a natural topology, given by the filtration.

Definition 2.1.5. *FM forms a base for the neighbourhoods of 0 for a topology of an additive topological group on* M*, called the* filtration topology*.*

Suppose FM is separated. Fix a real number $c > 1$ and let $\|x\| = c^k$ where $k = \inf\{n \in \mathbb{Z} : x \in F_nM\}$ if $x \neq 0$, and let $\|0\| = 0$. It's easy to check that $\|x - y\|$ defines a metric on M which generates the filtration topology (hence the choice of the constant c is irrelevant), so we can form the completion of M with respect to this metric. It turns out that there is another way of viewing this completion.

Definition 2.1.6. *Let M be a filtered R-module with filtration FM. The additive group $\widehat{M} = \varprojlim M/F_nM$ is called the* completion *of M. M is said to be* complete *if the natural map $M \to \widehat{M}$ given by $m \mapsto (m + F_nM)_{n\in\mathbb{Z}}$ is an isomorphism.*

Note that any positive filtration is automatically complete, and that a complete module is necessarily separated.

Suppose the filtration on R is negative, that is $F_0R = R$. Because FR is a filtration, each F_nR is a two-sided ideal of R, so we can define multiplication on $\widehat{R}$ by setting $(x_n+F_nR).(y_n+F_nR) = (x_ny_n+F_nR)$. A similar formula also turns $\widehat{M}$ into an $\widehat{R}$-module. Note also that $F_n\widehat{M} = \varprojlim_{m\leq n} M_n/M_m$ defines a filtration on $\widehat{M}$ which turns $\widehat{R}$ into a filtered ring and $\widehat{M}$ into a filtered $\widehat{R}$-module.

There is a natural (but slightly more complicated) way of defining multiplication on $\widehat{R}$ and an $\widehat{R}$-module structure on $\widehat{M}$ in general (i.e. when the filtration on R is not necessarily negative), but we shall not require this - see Chapter I.3 of [16] for more details.

Completing a module doesn't change the associated graded module, since $\widehat{M}/F_n\widehat{M} \cong M/F_nM$ for all $n \in \mathbb{Z}$. Hence

Lemma 2.1.7. *If M is a filtered R-module, $\operatorname{gr} M \cong \operatorname{gr} \widehat{M}$.*

Because the metric on a separated filtered module M is given by a non-archimedean norm (that is, a function $\|.\| : M \to \mathbb{R}$ satisfying $\|m\| \geq$

$0, \|m\| = 0 \iff m = 0, \|m \pm n\| \leq \max\{\|m\|, \|n\|\}$ for all $m, n \in M$), analysis in a complete module M is quite simple. In particular, the series $\sum a_n$ converges to an element of M if and only if the sequence (a_n) converges to 0, in sharp contrast to the corresponding situation in elementary analysis.

2.2 Zariskian filtrations

The idea behind the method of filtered and graded rings is to lift information from the graded object to the filtered object. Certain filtrations, namely the *Zariskian* ones, are especially well-suited to this task.

Definition 2.2.1. *Let R be a filtered ring. The* Rees ring *of R is defined to be*

$$\widetilde{R} = \bigoplus_{n \in \mathbb{Z}} F_n R.$$

If e_n denotes the canonical injection of F_nR into $\widetilde{R}$, the multiplication in $\widetilde{R}$ is given by $e_n(x).e_m(y) = e_{n+m}(xy)$, where $x \in F_nR$ and $y \in F_mR$.

We will always denote the central homogeneous element $e_1(1)$ of $\widetilde{R}$ by t. Note that with this convention, there is a natural injection of $\widetilde{R}$ into the Laurent polynomial ring $R[t, t^{-1}]$, given by $e_n(x) \mapsto xt^n$.

Definition 2.2.2. *Let M be a filtered R-module. The* Rees module *of M is defined to be*

$$\widetilde{M} = \bigoplus_{n \in \mathbb{Z}} F_n M.$$

With the same notation as above, $\widetilde{M}$ becomes a graded $\widetilde{R}$-module, via the formula $e_n(x).e_m(y) = e_{n+m}(xy)$ where $x \in F_nM$ and $y \in F_nR$.

There is a certain amount of interplay between a filtered module M and its associated graded and Rees modules. The following is easy to check.

Lemma 2.2.3. *Let R be a filtered ring and M a filtered R-module. Then*

(i) $\widetilde{R}/\widetilde{R}t \cong \operatorname{gr} R$.

(ii) $\widetilde{M}/\widetilde{M}t \cong \operatorname{gr} M$ *as* $\operatorname{gr} R$*-modules.*

(iii) $\widetilde{R}/\widetilde{R}(t-1) \cong R$.

(iv) $\widetilde{M}/\widetilde{M}(t-1) \cong M$ *as R-modules.*

This shows that we can think of $\operatorname{gr} M$ as a kind of "deformation" of M.

Definition 2.2.4. *Let M be a filtered R-module with filtration FM. We say that FM is a* good filtration *if the Rees module $\widetilde{M}$ of M is finitely generated over $\widetilde{R}$, the Rees ring of R.*

It is easy to see that FM is a good filtration on M if and only if there exist $m_1, \ldots, m_s \in M$ and $k_1, \ldots, k_s \in \mathbb{Z}$ such that for all $n \in \mathbb{Z}$

$$F_n M = \sum_{i=1}^{s} m_i F_{n-k_i} R.$$

Note that a finitely generated R-module M always has a good filtration: it is sufficient to pick a generating set X and define $F_n M = X.F_n R$ for all $n \in \mathbb{Z}$.

Note also that because of Lemma 2.2.3, if FM is a good filtration on M then M is finitely generated over R and $\operatorname{gr} M$ is finitely generated over $\operatorname{gr} R$. In fact, under certain (mild) conditions, the converse is also true.

Theorem 2.2.5. *Let R be a complete filtered ring and M a filtered R-module with separated filtration FM. Then FM is good if and only if* $\operatorname{gr} M$ *is finitely generated over* $\operatorname{gr} R$*.*

Proof. This is Theorem 5.7 of Chapter I of [16]. □

We can now consider Zariskian filtrations.

Definition 2.2.6. *The filtration FR on a ring R is said to be* Zariskian *if*

(i) The Rees ring $\widetilde{R}$ of R is Noetherian, and

(ii) The Jacobson radical $J(F_0R)$ of F_0R is contained in $F_{-1}R$.

If R possesses a Zariskian filtration, we say that R is a Zariski ring.

Note that because of Lemma 2.2.3, both R and $\operatorname{gr} R$ are automatically Noetherian if FR is Zariskian. The following proposition provides a large collection of rings with Zariskian filtrations.

Proposition 2.2.7. *Suppose R is a complete filtered ring such that* $\operatorname{gr} R$ *is Noetherian. Then R is Zariski.*

Proof. This is Proposition 2.2.1 of Chapter II of [16]. □

In particular, any ring R equipped with a positive filtration with respect to which the associated graded ring is Noetherian is Zariski, since any positive filtration is complete. Examples include universal enveloping algebras of finite dimensional Lie algebras over a field k and the Weyl algebras $A_n(k)$. Note that the filtrations that are considered in, for example, [23], are usually only the positive ones.

We list some of the properties that can be lifted from $\operatorname{gr} R$ to R in the case when R is Zariski.

Theorem 2.2.8. *Let R be a Zariski ring.*

(i) $\mathcal{K}(R) \leq \mathcal{K}(\operatorname{gr} R)$

(ii) $\operatorname{gld}(R) \leq \operatorname{gld}(\operatorname{gr} R)$

(iii) If $\operatorname{gr} R$ *is Auslander regular, then so is R.*

Proof. Here $\mathcal{K}$ denotes the Krull dimension, as discussed in section 2.3, and gld denotes the global homological dimension. For more information on the global dimension, see Chapter 7 of [23]. For an introduction to Auslander regularity, see [8] or Section 2 of Chapter III of [16].

Parts (i) and (ii) follow from Corollary 3.1.3 and Theorem 3.1.4 of Chapter II of [16], whereas part (iii) is Theorem 2.2.5 of Chapter III of [16]. □

2.3 Krull dimension

If R is a commutative ring, the Krull dimension of R is usually defined to be the maximal length of a chain of prime ideals of R and can be thought of as a measure of how far R is from being Artinian. However for noncommutative rings, this definition is not very appropriate since there exist simple rings (that is, rings with no nontrivial ideals) which are far from being Artinian, for example the Weyl algebras A_n. Instead, the Krull dimension for noncommutative rings is defined using the lattice of right ideals; for example the dimension is zero if the ring is (right) Artinian and one if every decreasing chain of right ideals has only finitely many non-Artinian factors.

The definitions and basic facts about the Krull dimension can be found in Chapter 6 of [23]. Here we recall this definition, and list some of the properties that Krull dimension enjoys that will be useful to us.

Definition 2.3.1. *Let R be a ring, $M \neq 0$ an R-module. If M is Artinian, define $\mathcal{K}_R(M) = 0$. Let $\alpha > 0$ be an ordinal and assume (by induction) that we have defined what it means to say $\mathcal{K}_R(N) = \beta$ for all ordinals $\beta < \alpha$. Then we say that $\mathcal{K}_R(M) = \alpha$ if*

(i) For all ordinals $\beta < \alpha$ there exists a chain $M \geq M_0 \geq M_1 \geq \ldots \geq M_k \geq \ldots$ of submodules of M such that $\mathcal{K}_R(M_i/M_{i+1}) = \beta$ for all $i \geq 0$,

(ii) For any chain $M \geq M_0 \geq M_1 \geq \ldots \geq M_k \geq \ldots$ of submodules of M, all but finitely many factors M_i/M_{i+1} have $\mathcal{K}_R(M_i/M_{i+1}) < \alpha$.

If there exists an ordinal α such that $\mathcal{K}_R(M) = \alpha$, M is said to have Krull dimension *α, denoted by $\mathcal{K}_R(M)$. Finally, if $M = 0$, define $\mathcal{K}_R(M) = -\infty$. By the* Krull dimension *of the ring R we mean the Krull dimension of the right R-module R_R.*

Note that if $\alpha > 0$ is finite, "for all $\beta < \alpha$" can be replaced by "for $\beta = \alpha - 1$" in part (i) of the above definition. Also, when there is no danger of confusion, we will write $\mathcal{K}(R)$ for $\mathcal{K}_R(R_R)$.

We single out a basic property of the Krull dimension, which we will use in what follows without particular mention.

Lemma 2.3.2. *If* $0 \to N \to M \to M/N \to 0$ *is an exact sequence of* R*-modules, then*

$$\mathcal{K}(M) = \max(\mathcal{K}(N), \mathcal{K}(M/N)).$$

Proof. See Lemma 6.2.4 of [23]. □

A very useful concept related to the notion of a module with Krull dimension is the notion of a *critical* module, an analogue of the notion of a simple module.

Definition 2.3.3. *A nonzero module* M *is called* α-critical *for some ordinal* α *if* $\mathcal{K}_R(M) = \alpha$ *and* $\mathcal{K}_R(M/N) < \alpha$ *for all nonzero submodules* N *of* M*.*

Clearly, a 0-critical module is nothing other than a simple module.

The following (well known) Lemma is the basis for many arguments involving the Krull dimension. Since we shall not require the general case of ordinal-valued Krull dimensions, we restrict ourselves to the case when the dimension is finite. We write $\mathrm{Lat}(R)$ for the lattice of all right ideals of a ring R.

Lemma 2.3.4. *Let* R *and* S *be rings, with* R *Noetherian of finite Krull dimension. Let* $f : \mathrm{Lat}(R) \to \mathrm{Lat}(S)$ *be an increasing function and let* $k, n \in \mathbb{N}$*. Let* $X, Y \lhd_r R$ *and suppose* $Y \subseteq X$ *and* $\mathcal{K}_R(X/Y) + k \leq \mathcal{K}_S(f(X)/f(Y))$ *whenever* X/Y *is* n*-critical. Then* $\mathcal{K}_R(X/Y)+k \leq \mathcal{K}_S(f(X)/f(Y))$ *whenever* $\mathcal{K}_R(X/Y) \geq n$*.*

In particular, $\mathcal{K}_R(R) + k \leq \mathcal{K}_S(S)$*.*

Proof. Proceed by induction on $m = \mathcal{K}_R(X/Y)$.

Suppose $m = n$. We can find $L \lhd_r R$ such that $Y \subseteq L \subseteq X$ and X/L is n-critical, because R is Noetherian - take $L \supseteq Y$ to be maximal subject to $\mathcal{K}_R(X/L) = n$. Then $\mathcal{K}_R(X/Y) + k = \mathcal{K}_R(X/L) + k \leq \mathcal{K}_S(f(X)/f(L)) \leq \mathcal{K}_S(f(X)/f(Y))$.

Now assume $m > n$. Since $m \leq \mathcal{K}_R(R)$ is finite, we can find a chain

$$X = L_0 \supseteq L_1 \supseteq \ldots \supseteq L_i \supseteq \ldots \supseteq Y$$

of right ideals of R such that $\mathcal{K}_R(L_i/L_{i+1}) = m - 1$ for all $i \in \mathbb{N}$. Applying the increasing function f yields the chain

$$f(X) = f(L_0) \supseteq f(L_1) \supseteq \ldots \supseteq f(L_i) \supseteq \ldots \supseteq f(Y)$$

of right ideals of S. By induction, $\mathcal{K}_S(f(L_i)/f(L_{i+1})) \geq \mathcal{K}_R(L_i/L_{i+1}) + k = m + k - 1$ for all $i \in \mathbb{N}$, whence $\mathcal{K}_S(f(X)/f(Y)) \geq m + k$, as required. □

For future applications, we will need to know the relationship between the Krull dimensions of a ring T and an subring R, as well as the Krull dimension of a polynomial algebra over a field.

Proposition 2.3.5. *(i) Let R be a ring with Krull dimension, T a ring extension of R which is a free left R-module and a finitely generated right R-module. Then $\mathcal{K}_R(R) = \mathcal{K}_T(T)$.*

(ii) If $R = k[x_1, \ldots, x_n]$ where k is a field, $\mathcal{K}_R(R) = n$.

Proof. See Lemma 6.5.3 of [23] for (i) and Corollary 6.4.8 of [23] for (ii). □

2.4 Dimension theory

Throughout this section, R denotes a filtered ring with filtration FR such that $\operatorname{gr} R$ is commutative, Noetherian and has finite Krull dimension.

Lemma 2.4.1. *Let M be a filtered R-module with two good filtrations FM and $F'M$. Let $\operatorname{gr}_F M$ and $\operatorname{gr}_{F'} M$ denote the associated graded modules of M with respect to FM and FM', respectively. Then*

$$\sqrt{\operatorname{Ann} \operatorname{gr}_F M} = \sqrt{\operatorname{Ann} \operatorname{gr}_{F'} M.}$$

Proof. This is Lemma 4.1.9 of Chapter III of [16]. □

Definition 2.4.2. *Let M be a finitely generated R-module, equipped with some good filtration FM. The* characteristic ideal *of M is defined to be*

$$J(M) := \sqrt{\operatorname{Ann} \operatorname{gr} M}.$$

The graded dimension *of M is defined to be*

$$d(M) := \mathcal{K}(\operatorname{gr} R/J(M)).$$

Lemma 2.4.1 shows that $J(M)$ does not depend on the choice of good filtration, so the above definition makes sense. The following result provides a slightly different way of defining the graded dimension of M.

Lemma 2.4.3. *Let M be a finitely generated R-module with a good filtration FM. Then $d(M) = \mathcal{K}(\operatorname{gr} M)$.*

Proof. Let $Q = \operatorname{Ann} \operatorname{gr} M$. Note that if $\operatorname{gr} M = \sum_{i=1}^{k} x_i \operatorname{gr} R$, then there is a surjection $\oplus_{i=1}^{k} (\operatorname{gr} R)/Q \to M$ whence $\mathcal{K}((\operatorname{gr} R)/Q) \geq \mathcal{K}(\operatorname{gr} M)$.

On the other hand, as $\operatorname{gr} R$ is commutative, we have an injection of $(\operatorname{gr} R)/Q$ into $\oplus_{i=1}^{k} \operatorname{gr} M$ given by

$$r + Q \mapsto \sum_{i=1}^{k} x_i r$$

This shows that $\mathcal{K}(\operatorname{gr} M) = \mathcal{K}((\operatorname{gr} R)/Q)$.

Since $\operatorname{gr} R$ is Noetherian, we can find $n \in \mathbb{N}$ such that $J(M)^n \subseteq Q$. It follows that $d(M) = \mathcal{K}((\operatorname{gr} R)/J(M)) = \mathcal{K}((\operatorname{gr} R)/Q) = \mathcal{K}(\operatorname{gr} M)$, as required. □

2.5 Compact p-adic Lie groups

Iwasawa algebras are completed group algebras of compact p-adic Lie groups (also called p-adic analytic groups), so we consider the latter first. A *p-adic Lie group* is a p-adic analytic manifold which is also a group, with the group operations being given by analytic functions. It turns out that there is a description of these in terms of *uniform pro-p groups*, namely we have the following result due to Lazard:

Theorem 2.5.1. *The following are equivalent for a topological group G:*

(i) G is a compact p-adic analytic group

(ii) G is a profinite group containing an open normal uniform pro-p subgroup.

Proof. See Corollary 8.34 of [11]. □

In particular, uniform pro-p groups are themselves p-adic Lie groups. The advantage of studying uniform pro-p groups is that their definition is almost entirely group theoretic and involves no analytic machinery required to describe p-adic analytic manifolds.

Definition 2.5.2. *A* profinite group *is a compact Hausdorff topological group G whose open subgroups form a base for the open neighbourhoods of the identity. G is said to be* finitely generated *if $G = \overline{\langle X \rangle}$ for some finite subset X of G; then X is said to be a* topological generating set *for G and $d(G)$ will denote the minimal cardinality such an X.*

Note that if G is profinite and N is an open subgroup, $G = \cup_{x \in G} Nx$ is an open cover which has a finite subcover by compactness. Hence every open subgroup has finite index in G.

Definition 2.5.3. *A* pro-p group *is a profinite group whose open subgroups have index equal to some power of p.*

The most basic example of a pro-p group is given by the p-adics $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. The topology on $\mathbb{Z}_p$ is given by declaring that the open neighbourhoods of 0 will be all the subgroups of finite index. In fact, any profinite group can be thought as an inverse limit, namely $G \cong \varprojlim_{N \triangleleft_o G}(G/N)$; here $N \triangleleft_o G$ means N is an open normal subgroup of G. This is

Proposition 2.5.4. *A topological group G is a profinite (pro-p) group if and only if it is topologically isomorphic to an inverse limit of finite groups (finite p-groups).*

Proof. See Propositions 1.3 and 1.12 of [11]. □

Definition 2.5.5. *Let G be a pro-p group. Define $P_1(G) = G_1 = G$ and $P_{i+1}(G) = G_{i+1} = \overline{P_i(G)^p[P_i(G), G]}$, for $i \geq 1$. The decreasing chain of subgroups $G = P_1(G) \geq P_2(G) \geq \ldots \geq P_k(G) \geq \ldots$ is called the* lower p-series *of G.*

(i) G is powerful *if p is odd and $G/\overline{G^p}$ is abelian, or if $p = 2$ and $G/\overline{G^4}$ is abelian.*

(ii) G is uniform *if G is powerful, finitely generated and $[G : P_2(G)] = [P_i(G) : P_{i+1}(G)]$ for all $i \geq 1$.*

Powerful pro-p groups enjoy some very nice properties, as summarized in the following proposition.

Proposition 2.5.6. *Let $G = \overline{\langle a_1, \ldots, a_d \rangle}$ be a finitely generated powerful pro-p group. Then*

(i) $G_{i+k} = G_i^{p^k} = \{g^{p^k} : g \in G_i\}$ for all $k \geq 0, i \geq 1$.

(ii) The map $\varphi_k : G \to G, x \mapsto x^{p^k}$ induces a homomorphism from G_i/G_{i+1} onto G_{i+k}/G_{i+k+1} for all i,k.

(iii) If G is uniform, $\varphi_k : G \to G_{k+1}$ is a bijection (but not necessarily a group homomorphism), so every element of $x \in G_{k+1}$ has a unique p^k-th root in G, denoted by $x^{p^{-k}}$.

(iv) If G is uniform, so is G_i for each $i \geq 1$.

(v) $d(A) = d(B)$ *for any open uniform subgroups* A, B *of* G*; this enables us to define the* dimension $\dim(G)$ *of* G *to be* $d(H)$ *for any open uniform subgroup* H *of* G*.*

Proof. See Theorem 3.6 and Lemmas 4.6 and 4.10 of [11]. □

This result implies that each G_i is itself a finitely generated powerful pro-p group. Since $[G_1 : G_2] \geq [G_2 : G_3] \geq \ldots \geq [G_i : G_{i+1}] \geq \ldots$ by the second part, it's clear that G_i is uniform for sufficiently large i.

Definition 2.5.7. *A* $\mathbb{Z}_p$-Lie algebra *is a free* $\mathbb{Z}_p$*-module* L *equipped with a* $\mathbb{Z}_p$*-bilinear antisymmetric map* $[.,.] : L \times L \to L$ *satisfying the Jacobi identity* $[x[yz]] + [y[zx]] + [z[xy]] = 0$ *for all* $x, y, z \in L$*.* L *is said to be* powerful *if it has finite rank as a* $\mathbb{Z}_p$*-module and also satisfies* $[L, L] \subseteq pL$*.*

It is possible to define a $\mathbb{Z}_p$-Lie algebra structure on a given uniform pro-p group, as follows:

Theorem 2.5.8. *Let* G *be a uniform pro-p group,* $x, y \in G$*. Then the operations*

$$x + y = \lim_{n\to\infty} (x^{p^n} y^{p^n})^{p^{-n}} \qquad \text{and}$$

$$(x, y) = \lim_{n\to\infty} [x^{p^n}, y^{p^n}]^{p^{-2n}}$$

define the structure of a powerful $\mathbb{Z}_p$*-Lie algebra on* G*, denoted by* L_G*. Here* $[a, b] = a^{-1}b^{-1}ab$ *if* $a, b \in G$*. Moreover,* $L_G \cong \mathbb{Z}_p^d$ *as a* $\mathbb{Z}_p$*-module.*

Proof. See Theorem 4.30 of [11]. □

Definition 2.5.9. *Let* G *be a uniform pro-p group. The* $\mathbb{Q}_p$*-Lie algebra* $\mathcal{L}(G) = L_G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ *is called the* Lie algebra of G*.*

In what follows, the term "powerful Lie algebra" will always mean "powerful $\mathbb{Z}_p$-Lie algebra".

The remarkable thing about a powerful Lie algebra L is that there is a way of using the Lie bracket on L to turn L into a uniform pro-p group. The group law on L is given by the *Campbell-Hausdorff formula*

$$x * y = \Phi(x, y) = x + y + \frac{1}{2}[x, y] + \ldots,$$

which is a certain infinite sum of terms involving x, y and the bracket operation on L. Of course, if we start off with a uniform pro-p group G and view it as a powerful Lie algebra using Theorem 2.5.8, the Campbell-Hausdorff formula gives us back the group we started with. More precisely, we have

Theorem 2.5.10. *The assignments*

$$G \mapsto L_G, L \mapsto (L, *)$$

are mutually inverse isomorphisms between the category of uniform pro-p groups and the category of powerful Lie algebras over $\mathbb{Z}_p$.

Proof. This is Theorem 9.10 of [11]. □

Thus, a uniform pro-p group and a powerful Lie algebra are essentially the same thing (or at least as far as their finite dimensional $\mathbb{Q}_p$-representations are concerned). In particular, there is a tight correspondence between certain $\mathbb{Z}_p$- Lie subalgebras of L_G and closed uniform subgroups of G:

Proposition 2.5.11. *Let G be a uniform pro-p group. Let N be a $\mathbb{Z}_p$-Lie subalgebra of L_G such that the $\mathbb{Z}_p$-module L_G/N is torsion-free. Then N is* *a closed uniform subgroup of G.*

Proof. This is Theorem 7.15 of [11]. □

We use this result to make the transition between uniform groups and their Lie algebras more smooth.

Corollary 2.5.12. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}$ and let $\mathfrak{h}$ be a $\mathbb{Q}_p$-Lie subalgebra of $\mathfrak{g}$. Then $H = \mathfrak{h} \cap L_G$ is a closed uniform subgroup of G with $\mathbb{Q}_p$-Lie algebra $\mathfrak{h}$.*

Proof. As L_G/H injects into $\mathfrak{g}/\mathfrak{h}$ which is torsion-free, the result follows from Proposition 2.5.11. □

We will call H the *isolated* uniform subgroup of G with Lie algebra $\mathfrak{h}$.

We also have the following natural connection between the centre of a uniform pro-p group and the centre of its $\mathbb{Z}_p$-Lie algebra:

Lemma 2.5.13. *Let G be a uniform pro-p group with centre $Z(G)$. Then*

(i) $L_{Z(G)} = Z(L_G)$.

(ii) $Z(G) = (Z(L_G), *)$.

(iii) $Z(G)$ is the isolated uniform subgroup of G with Lie algebra $Z(\mathcal{L}(G))$.

Proof. If $x \in Z(G)$ and $y \in G$ then $(x, y) = \lim_{n\to\infty} [x^{p^n}, y^{p^n}]^{p^{-2n}} = 1$ as x is central, so $L_{Z(G)} \subseteq Z(L_G)$. If $x \in Z(L_G)$ and $y \in L_G$ then $x * y = x + y + \frac{1}{2}(x, y) + \ldots = x + y = y + x = y * x$ since each term in the Campbell-Hausdorff series after $x + y$ lies in (x, L_G) which is 0 since $x \in Z(L_G)$. Part (i) follows, and part (ii) is a consequence of (i) and Theorem 2.5.10.

As $Z(L_G) = Z(\mathcal{L}(G)) \cap L_G$, part (iii) follows from (ii) and Corollary 2.5.12. □

2.6 Iwasawa algebras

We can finally begin to consider Iwasawa algebras.

Definition 2.6.1. *Let G be a profinite group. The* completed group algebra (Iwasawa algebra) *of G is defined to be the inverse limit*

$$\Lambda_G = \mathbb{Z}_p[[G]] := \varprojlim_{N \lhd_o G} \mathbb{Z}_p[G/N]$$

as N runs over all open normal subgroups of G.

If G is a profinite group, every open subgroup N contains an open normal subgroup (e.g. $\cap_{g \in G} N^g$); since G is Hausdorff, for all $g \in G \backslash \{1\}$ we can find an open normal subgroup N with $g \notin N$. This makes it clear that there is a natural embedding $G \hookrightarrow \mathbb{Z}_p[[G]]$, given by $g \mapsto (gN)_{N \lhd_o G}$.

Lemma 2.6.2. *Let G be a profinite group, H an open normal subgroup. Then Λ_G is a free right and left Λ_H-module of finite rank.*

Proof. Let $N \lhd_o G$. Since the topology on H is induced from the topology on G, $N \cap H \lhd_o H$. Since H has finite index in G, $N \cap H$ is an open normal subgroup of G contained in H and N.

Thus every open normal subgroup of G contains an open normal subgroup of G contained in H.

It follows that $\Lambda_G \cong \varprojlim_{N \in \mathcal{C}} \mathbb{Z}_p[G/N]$, where $\mathcal{C} = \{N \lhd_o G : N \subseteq H\}$, and similarly $\Lambda_H \cong \varprojlim_{N \in \mathcal{C}} \mathbb{Z}_p[H/N]$.

Since each $\mathbb{Z}_p[G/N]$ is a free right and left $\mathbb{Z}_p[H/N]$-module of finite rank for every $N \in \mathcal{C}$ with a basis independent of N (a transversal for H in G will do), the result follows. □

As any compact p-adic Lie group G contains an open uniform pro-p group H (Theorem 2.5.1), the above result shows that Λ_G is closely related to Λ_H. For example, the Krull dimension of Λ_G is equal to that of Λ_H, by Proposition 2.3.5(i). As a consequence, we will often only consider uniform G.

When G is uniform, the Iwasawa algebra of G posesses many nice properties. Its topology is given by a norm and in fact Λ_G can be obtained from the ordinary group algebra $\mathbb{Z}_p[G]$ by completing it with respect to this norm. Moreover, every element of Λ_G can be written uniquely as a power series in a finite number of variables; thus Λ_G can be viewed as a "skew power series ring".

Theorem 2.6.3. *Let G be a uniform pro-p group with topological generating set $\{a_1, \ldots, a_d\}$. Let $R_0 = \mathbb{Z}_p[G]$ and $J_0 = \ker(R_0 \twoheadrightarrow \mathbb{F}_p)$. Let $b_i = a_i - 1 \in R_0$ and $\mathbf{b}^\alpha = b_1^{\alpha_1} \ldots b_d^{\alpha_d} \in R_0$ for $\alpha \in \mathbb{N}^d$. Then*

(i) Λ_G is isomorphic to the completion of R_0 with respect to the J_0-adic filtration.

(ii) Each element of Λ_G is equal to the sum of a uniquely determined convergent series

$$\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha,$$

where $\lambda_\alpha \in \mathbb{Z}_p$ for all $\alpha \in \mathbb{N}^d$.

(iii) Λ_G is a local ring with unique maximal ideal $J = \ker(\Lambda_G \twoheadrightarrow \mathbb{F}_p)$.

Proof. Parts (i) and (ii) are Theorems 7.1 and 7.20 in [11], respectively.

The term "commutative local ring" is standard: the ring has a unique maximal ideal. When the ring R is noncommutative, there are several possible definitions. One of these is to insist that $R/J(R)$ is simple Artinian, where $J(R)$ is the Jacobson radical of R. In the case when $R/J(R)$ is a division ring, R is sometimes called a "scalar local ring".

For us however, R is a local ring whenever $R/J(R)$ is a commutative field F. Note that such rings have a unique simple module isomorphic to F.

Part (iii) is well known, but we prove it for completeness. Since $\Lambda_G/J \cong \mathbb{F}_p$, it's sufficient to show that every element $x \in \Lambda_G - J$ is invertible. Viewing x as a power series in $b_1, \ldots, b_d$ as in (i) with coefficients λ_α for $\alpha \in \mathbb{N}^d$, we see that $\lambda_0 \notin p\mathbb{Z}_p$ and is hence a unit in $\mathbb{Z}_p$. Without loss of generality, $\lambda_0 = 1$ so $x = 1 - y$ where $y \in J$. Now from (i), Λ_G is complete with respect to the J-adic filtration, whence $z = 1 + y + y^2 + \ldots$ is a well-defined element of Λ_G and is easily seen to be the required inverse for x. □

One of the main tools for studying Λ_G is the associated graded ring. For uniform G this is a well-understood polynomial algebra.

Theorem 2.6.4. *Let G be a uniform pro-p group. There exists a (natural) separated filtration $F\Lambda_G$ on Λ_G with respect to which the associated graded ring of Λ_G is isomorphic to a polynomial algebra in $d+1$ variables over $\mathbb{F}_p$:*

$$\operatorname{gr} \Lambda_G \cong \mathbb{F}_p[X_0, \ldots, X_d]$$

Also, this filtration refines the J-adic filtration of Λ_G, whence Λ_G is complete with respect $F\Lambda_G$. Here $J = \ker(\Lambda_G \twoheadrightarrow \mathbb{F}_p)$.

Proof. See Theorem 7.22 of [11]. □

Using this filtration, we can lift many of the properties of $\operatorname{gr} \Lambda_G$ back to Λ_G. We summarize some of these below.

Theorem 2.6.5. *Let G be a uniform pro-p group of dimension d.*

(i) Λ_G *is Noetherian ring with no zero divisors*

(ii) $\mathcal{K}(\Lambda_G) \leq d+1$

(iii) $\operatorname{gld}(\Lambda_G) \leq d+1$

(iv) Λ_G *is Auslander regular.*

Proof. We see from Proposition 2.2.7 and Theorem 2.6.4 that $F\Lambda_G$ is a Zariskian filtration on Λ_G. Therefore $\widetilde{\Lambda_G}$ is Noetherian, and hence so is Λ_G, by Lemma 2.2.3.

Suppose $x, y \in \Lambda_G$ are nonzero. Then $\sigma(x), \sigma(y) \in \operatorname{gr}\Lambda_G$ are nonzero (because the filtration is separated) and hence $\sigma(x).\sigma(y) \neq 0$ as $\operatorname{gr}\Lambda_G$ has no zero divisors. But in this case $\sigma(xy) = \sigma(x).\sigma(y) \neq 0$ and so $xy \neq 0$.

We note that $\mathcal{K}(\operatorname{gr}\Lambda_G) = d+1$ by Proposition 2.3.5(ii) and $\operatorname{gld}(\operatorname{gr}\Lambda_G) = d+1$, by Theorem 7.5.3(iii) of [23]. Also, the polynomial algebra is Auslander regular by Theorem 2.3.5 of Chapter III of [16].

The remaining assertions follow from Theorem 2.2.8. □

In fact, the global dimension of Λ_G is known to attain the upper bound established above.

Theorem 2.6.6. *Let G be a uniform pro-p group. Then* $\operatorname{gld}(\Lambda_G) = d+1$.

Proof. See Theorem 4.1 of [5], where this result is proved in somewhat greater generality. □

2.7 The $\mathbb{F}_p$-version of Iwasawa algebras

Also of interest is the $\mathbb{F}_p$-version of Iwasawa algebras, Ω_G.

Definition 2.7.1. *Let G be a profinite group. The* completed group algebra of G over $\mathbb{F}_p$ *is defined to be*

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

We will always write J_G for the augmentation ideal $\ker(\Omega_G \twoheadrightarrow \mathbb{F}_p)$ *of Ω_G.*

It is easy to see that $\Omega_G \cong \Lambda_G / p\Lambda_G$ for any profinite G, so one can expect a close connection between the ring-theoretic properties of Λ_G and Ω_G.

We record some properties of Ω_G, similar to those listed in Theorems 2.6.4 and 2.6.5. We collect them all together as follows.

Theorem 2.7.2. *Let G be a uniform pro-p group with topological generating set $\{a_1, \ldots, a_d\}$. Let $R_0 = \mathbb{F}_p[G]$ and $J_0 = \ker(R_0 \twoheadrightarrow \mathbb{F}_p)$. Let $b_i = a_i - 1 \in R_0$ and $\mathbf{b}^\alpha = b_1^{\alpha_1} \ldots b_d^{\alpha_d} \in R_0$ for $\alpha \in \mathbb{N}^d$. Then*

(i) Ω_G is isomorphic to the completion of R_0 with respect to the J_0-adic filtration.

(ii) Each element of Ω_G is equal to the sum of a uniquely determined convergent series

$$\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha,$$

where $\lambda_\alpha \in \mathbb{F}_p$ for all $\alpha \in \mathbb{N}^d$.

(iii) $J_G^n = \{ \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha : \lambda_\alpha = 0$ if $\alpha_1 + \ldots + \alpha_d < n\}$.

(iv) Ω_G *is a local ring with unique maximal ideal* J_G*.*

(v) The associated graded ring of Ω_G *with respect to the* J_G*-adic filtration is isomorphic to a polynomial algebra in* d *variables over* $\mathbb{F}_p$*,*

$$\operatorname{gr}\Omega_G \cong \mathbb{F}_p[X_1, \ldots, X_d]$$

and Ω_G *is complete with respect to this filtration.*

(vi) Ω_G *is Noetherian ring with no zero divisors.*

(vii) $\mathcal{K}(\Omega_G) \leq d$*.*

(viii) $\operatorname{gld}(\Omega_G) \leq d$*.*

(ix) Ω_G *is Auslander regular.*

Proof. Parts (ii), (iii) and (v) are Theorems 7.23(i), 7.23(ii) and 7.24 of [11], respectively, whereas a proof of part (i) can be found in the remarks preceding Theorem 7.23 of [11].

As $\Omega_G = \Lambda_G/p\Lambda_G$, (iv) follows from part (iii) of Theorem 2.6.3.

The proofs of the remaining assertions are obtained *mutatis mutandis* from the proofs of Theorem 2.6.5. □

Corollary 2.7.3. *Let* $H \subseteq G$ *be uniform pro-p groups with torsion-free* L_G/L_H*. Then the subspace filtration on* Ω_H *induced from the* J_G*-adic filtration on* Ω_G *coincides with the* J_H*-adic filtration.*

Proof. The condition on L_G/L_H allows us to find a topological generating set $\{a_1, \ldots, a_d\}$ for G such that $\{a_1, \ldots, a_t\}$ is a topological generating set for H.

By part (iii) of the preceding Theorem, $J_H^n = \{\sum_{\alpha\in\mathbb{N}^d} \lambda_\alpha \mathbf{b}^\alpha : \lambda_\alpha = 0$ if $\alpha_1 + \ldots + \alpha_d < n$ or $\alpha_i \neq 0$ for some $i > t\} = J_G^n \cap \Omega_H$, as required. □

Inspection of the proof of Lemma 2.6.2 shows that we can replace $\mathbb{Z}_p$ everywhere with $\mathbb{F}_p$ without changing the validity of this result. Hence

Lemma 2.7.4. *Let G be a profinite group, H an open normal subgroup. Then Ω_G is a free right and left Ω_H-module of finite rank, and $\mathcal{K}(\Omega_G) = \mathcal{K}(\Omega_H)$.*

2.8 Chevalley groups

We will frequently be interested in a uniform pro-p group G with split simple Lie algebra $\mathcal{L}(G)$. Such a Lie algebra is completely determined by its root system $X \in \{A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2\}$. For more information about root systems, see [19] or [15] or Chapter 3 of [7].

Starting from a root system X and a commutative ring R, it is possible to construct the adjoint Chevalley group $X(R)$. In the case when $R = \mathbb{Z}_p$, the resulting group $X(\mathbb{Z}_p)$ is closely related to the $\mathbb{Q}_p$-Lie algebra $X_{\mathbb{Q}_p}$ with root system X and hence provides useful information about uniform pro-p groups G with Lie algebra $X_{\mathbb{Q}_p}$.

In what follows, X will denote an indecomposable root system and R an arbitrary commutative ring (with 1).

When $\mathfrak{g}$ is a simple Lie algebra over $\mathbb{C}$, there is a basis for $\mathfrak{g}$, known as the Chevalley basis, with structure constants of Lie multiplication with respect to this basis being rational integers. This is

Theorem 2.8.1. *Let $\mathfrak{g}$ be a simple Lie algebra over $\mathbb{C}$ with root system X. Choose a fundamental system of roots Π and let $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{r\in X} \mathfrak{e}_r$ be a Cartan* *decomposition of $\mathfrak{g}$. Let $h_r \in \mathfrak{h}$ be the co-root corresponding to the root $r \in X$. Then we can find elements $e_r \in \mathfrak{e}_r$ such that*

$$\mathcal{B} = \{h_r : r \in \Pi\} \cup \{e_r : r \in X\}$$

forms a basis for $\mathfrak{g}$, called a Chevalley basis. *The basis elements multiply as follows:*

$$\begin{aligned}
&[h_r, h_s] = 0 \\
&[h_r, e_s] = A_{rs} e_s \\
&[e_r, e_{-r}] = h_r \\
&[e_r, e_s] = 0 && \textit{if } r + s \notin X, r + s \neq 0 \\
&[e_r, e_s] = N_{r,s} e_{r+s} && \textit{if } r + s \in X
\end{aligned}$$

Here $A_{rs} = \frac{2(r,s)}{(r,r)}$ and $N_{r,s} = \pm(a+1)$ where a is the greatest integer for which $s - ar \in X$. All the multiplication constants of the algebra with respect to this basis are integers, whence $[\mathbb{Z}\mathcal{B}, \mathbb{Z}\mathcal{B}] \subseteq \mathbb{Z}\mathcal{B}$.

Proof. See Theorem 4.2.1 of [7]. □

Definition 2.8.2. *Let $\mathfrak{g}$ be the simple Lie algebra over $\mathbb{C}$ with root system X and Chevalley basis $\mathcal{B}$. The Lie algebra of type X over R is defined to be*

$$X_R = R \otimes_{\mathbb{Z}} \mathbb{Z}\mathcal{B}.$$

Since $[\mathbb{Z}\mathcal{B}, \mathbb{Z}\mathcal{B}] \subseteq \mathbb{Z}\mathcal{B}$ by Theorem 2.8.1, X_R *is* a Lie algebra over R. Note that $X_{\mathbb{C}}$ is just $\mathfrak{g}$, in the above notation. We require some information about certain automorphisms of $X_{\mathbb{C}}$.

Proposition 2.8.3. *Let $\zeta \in \mathbb{C}$ and let $r \in X$. The map*

$$x_r(\zeta) = \exp(\zeta \operatorname{ad}\ e_r) = 1 + \frac{\zeta}{1!} \operatorname{ad}\ e_r + \frac{\zeta^2}{2!}(\operatorname{ad}\ e_r)^2 + \ldots : X_{\mathbb{C}} \to X_{\mathbb{C}}$$

is an automorphism of $X_{\mathbb{C}}$. The action of $x_r(\zeta)$ on the Chevalley basis $\mathcal{B}$ is given by

$$\begin{aligned} &x_r(\zeta).h_u = h_u - A_{ur}\zeta e_r, \qquad && u \in X \\ &x_r(\zeta).e_r = e_r \\ &x_r(\zeta).e_{-r} = e_{-r} + \zeta h_r - \zeta^2 e_r \\ &x_r(\zeta).e_s = \textstyle\sum_{i=0}^{b} M_{r,s,i}\zeta^i e_{ir+s} \end{aligned}$$

where $s \in X$ is a root linearly independent from r, $b \in \mathbb{Z}$ is the largest integer such that $s + br \in X$ and

$$M_{r,s,i} = \pm\binom{a+i}{i}.$$

Proof. See Lemma 4.3.1 of [7] and the subsequent remarks. □

Let $\Theta_R(t) : M_n(\mathbb{Z}[T]) \to M_n(R)$ be the map induced from the natural map $\mathbb{Z}[T] \to R$ defined by evaluating T at $t \in R$. The above proposition could be interpreted as asserting the existence of elements $C_r \in M_n(\mathbb{Z}[T])$ for each $r \in X$, such that the matrix of $x_r(\zeta)$ with respect to $\mathcal{B}$ is given by $\Theta_{\mathbb{C}}(\zeta)(C_r)$. Here $n = \dim \mathfrak{g} = |X| + |\Pi|$.

Proposition 2.8.4. *If $r \in X$ and $t \in R$, let $x_r(t) : X_R \to X_R$ be the R-linear map whose matrix with respect to $\{1 \otimes v : v \in \mathcal{B}\}$ is $\Theta_R(t)(C_r)$. Then $x_r(t)$ is an automorphism of X_R.*

Proof. When $R = K$ is a field, this is precisely the content of Proposition

4.4.2 of [7]. The proof given there does not use the fact that K is a field and carries over *mutatis mutandis.* □

Definition 2.8.5. *The* Chevalley group *of type X over R is defined to be*

$$X(R) = \quad < x_r(t) : r \in X, t \in R > \quad \subseteq \mathrm{Aut}(X_R).$$

Proposition 2.8.6. *Let S be the subgroup of $SL_2(R)$ generated by the elements*

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \textit{ and } \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

for $t \in R$. Then there exists a homomorphism $\phi_r : S \to X(R)$ such that

$$\phi_r \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_r(t) \textit{ and } \phi_r \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-r}(t)$$

for all $t \in R$.

Proof. When $R = K$ is a field, this is Theorem 6.3.1 of [7], since in this case $S = SL_2(R)$ by Lemma 6.1.1 of [7]. The proof can be easily modified to give the required result. □

Certain elements of $X(R)$ and their actions on X_R will be of interest to us in what follows.

Definition 2.8.7. *Let R^* denote the group of units of R. When $t \in R^*$ and $r \in X$, define*

$$\begin{aligned} n_r(t) &= x_r(t)x_{-r}(-t^{-1})x_r(t) \quad \textit{and} \\ h_r(t) &= n_r(t)n_r(-1). \end{aligned}$$

Proposition 2.8.8. *When $t \in R^*$ and $r \in X$, the actions of $h_r(t)$ and $n_r = n_r(1)$ on X_R are given below:*

$$\begin{aligned}
&h_r(t).h_s = h_s, && s \in \Pi\\
&h_r(t).e_s = t^{A_{rs}} e_s, && s \in X\\
&n_r.h_s = h_{w_r(s)}\\
&n_r.e_s = \eta_{r,s} e_{w_r(s)}
\end{aligned}$$

Here w_r is the Weyl reflection on X corresponding to the root r and $\eta_{r,s} = \pm 1$.

Proof. The proofs of Propositions 6.4.1 and 6.4.2 of [7] carry over, in view of Proposition 2.8.6. □

Proposition 2.8.9. *The following relations hold in $X(R)$:*

$$\begin{aligned}
&h_r(t_1)h_r(t_2) = h_r(t_1t_2), && t_1, t_2 \in R^*\\
&x_r(t)x_s(u)x_r(t)^{-1} = x_s(u). \textstyle\prod_{i,j>0} x_{ir+js}(C_{ijrs}t^iu^j), && t, u \in R\\
&h_s(u)x_r(t)h_s(u)^{-1} = x_r(u^{A_{sr}}t), && t \in R, u \in R^*
\end{aligned}$$

for each $r, s \in X$. Here C_{ijrs} are certain integers such that $C_{i1rs} = M_{r,s,i}$.

Proof. See Theorem 5.2.2 and the remarks preceding Lemma 7.1.2 of [7]. □

2.9 Restricted Lie algebras

Throughout this section, k denotes a field of characteristic $p > 0$.

Definition 2.9.1. *A Lie algebra $\mathfrak{g}$ over k is said to be* restricted *if there exists a map $x \mapsto x^{[p]}$ of $\mathfrak{g}$ into itself, known as a p-*structure on $\mathfrak{g}$*, satisfying*

$$\begin{array}{lcll} (\alpha a)^{[p]} & = & \alpha^p a^{[p]}, & \qquad \alpha \in k \\ (\operatorname{ad} a)^p & = & \operatorname{ad} a^{[p]} & \\ (a+b)^{[p]} & = & a^{[p]} + b^{[p]} + \Lambda(a,b) & \end{array}$$

for all $a, b \in \mathfrak{g}$, where $\Lambda(a,b) \in \mathfrak{g}$ is defined by $\Lambda(a,b) = \sum_{j=1}^{p-1} \Lambda_j(a,b)$, where

$$\sum_{j=1}^{p-1} j\Lambda_j(a,b)T^{j-1} = \operatorname{ad}(Ta+b)^{p-1}a.$$

Here T is an indeterminate.

Note that if A is any (not necessarily associative nor commutative) k-algebra and D is a derivation of A (that is, a k-linear map satisfying $D(ab) = a(Db) + (Da)b$ for all $a, b \in A$), then D^p is also a derivation, by the Leibniz identity. It can be shown that $\mathfrak{g}$ is restricted if and only if each derivation $(\operatorname{ad} a)^p$ for $a \in \mathfrak{g}$ is *inner*, that is, there exists $a^{[p]} \in \mathfrak{g}$ such that $(\operatorname{ad} a)^p = \operatorname{ad} a^{[p]}$.

The following examples (see [21]) show that this definition is quite natural:

Example 2.9.2. *Let A be an associative algebra over k, viewed as a Lie algebra with the commutator Lie bracket. Then A is restricted, with p-structure given by $a^{[p]} = a^p$.*

Example 2.9.3. *Let k be algebraically closed and let G be an affine algebraic group over k. Let $\mathfrak{g}$ be its Lie algebra, viewed as the set of all derivations D of $k[G]$ which commute with the left translations in G. Then $D^{[p]} = D^p$ is a p-structure on $\mathfrak{g}$.*

The existence of the p-structure on $\mathfrak{g}$ has a dramatic effect on the structure of the universal enveloping algebra $\mathcal{U}(\mathfrak{g})$ of $\mathfrak{g}$. See [10] for information about these algebras.

Proposition 2.9.4. *Let $\mathfrak{g}$ be a restricted Lie algebra over k. Then*

(i) For $a \in \mathfrak{g}$ the element $a^p - a^{[p]}$ lies in the centre of $\mathcal{U}(\mathfrak{g})$.

(ii) The map $\varphi : \mathfrak{g} \to Z(\mathcal{U}(\mathfrak{g}))$ defined by $a \mapsto a^p - a^{[p]}$ is semilinear*, that is it satisfies $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(\alpha a) = \alpha^p \varphi(a)$ for all $a, b \in \mathfrak{g}$ and $\alpha \in k$.*

(iii) Suppose $\mathfrak{g}$ is finite dimensional with basis $\{x_1, \ldots, x_d\}$. Let $\mathcal{O}$ denote the central k-subalgebra of $\mathcal{U}(\mathfrak{g})$ generated by $\varphi(\mathfrak{g})$. Then $\mathcal{O}$ is isomorphic to a polynomial algebra $k[\varphi(x_1), \ldots, \varphi(x_d)]$, and $\mathcal{U}(\mathfrak{g})$ is finitely generated as a module over $\mathcal{O}$.

Proof. Parts (i) and (ii) are the content of Lemma 2 of [21], but also follows easily from the above examples and definitions. Part (iii) follows from the Poincare-Birkhoff-Witt Theorem ([10], 2.1.11). □

The central subalgebra $\mathcal{O}$ of $\mathcal{U}(\mathfrak{g})$ is known as the *p-centre* of $\mathcal{U}(\mathfrak{g})$.

Chapter 3

Bounds on the Krull Dimension

3.1 Reduction to Ω_G

It turns out that the Krull dimension of Λ_G is completely determined by that of Ω_G. This follows from a more general result due to Walker:

Theorem 3.1.1 (Walker, [31]1.8). *Suppose R is Noetherian and x is a regular normal element belonging to the Jacobson radical of R. If $\mathcal{K}(R) < \infty$ then*

$$\mathcal{K}(R) = \mathcal{K}(R/xR) + 1.$$

The same result holds if Krull dimension is replaced by global dimension, see Theorem 7.3.7 of [23].

Note that the statement of Theorem 1.8 in [31] does not contain the constraint $\mathcal{K}(R) < \infty$. This is because the definition of Krull dimension was extended to take ordinal values after this paper was published; in any case, the conclusion of the theorem would have to be modified in order to deal with limit ordinals. Consequently we restrict ourselves to finite values of $\mathcal{K}(R)$.

In this section we provide a provide a more elementary proof of this theorem than that contained in [31].

Let R be a ring. Recall that $x \in R$ is said to be *normal* if $xR = Rx$, and *regular* if $xy = 0$ or $yx = 0$ in R implies $y = 0$, that is, x is not a zero-divisor. Suppose x is a normal element of R and M is an R-module. It's clear that Mx is an R-submodule of M; recall that M is said to be *x-torsion free* if $mx = 0 \Rightarrow m = 0$ for all $m \in M$. Note also that $\{m \in M : mx^n = 0$ for some $n \in \mathbb{N}\}$ is also an R-submodule of M, the *x-torsion submodule.*

The following result summarizes various elementary properties of modules.

Lemma 3.1.2. *Let x be a normal element of a ring R and let $B \subseteq A$ be R-modules with Krull dimension. Then:*

(a) If A/B and B are x-torsion free then A is also x-torsion free.

(b) If A/B is x-torsion free then $Ax \cap B = Bx$ and $\mathcal{K}(B/Bx) \leq \mathcal{K}(A/Ax)$.

(c) If A is x-torsion free then $\mathcal{K}(A/Ax) = \mathcal{K}(Ax^{n-1}/Ax^n) = \mathcal{K}(A/Ax^n)$ for all $n \geq 1$.

The main step comes next.

Lemma 3.1.3. *Let R be a Noetherian ring, x a normal element of the Jacobson radical $J(R)$ of R. Suppose M is a finitely generated x-torsion free R-module with finite Krull dimension. Then $\mathcal{K}(M/Mx) \geq \mathcal{K}(M) - 1$.*

Proof. Proceed by induction on $\mathcal{K}(M) = \beta$. Since $x \in J(R)$, the base case $\beta = 0$ follows from Nakayama's Lemma. We can find a chain $M = M_1 > M_2 > \ldots > M_k > \ldots$ such that M_i/M_{i+1} is $(\beta - 1)$-critical for all $i \geq 1$.

Case 1: $\exists i \geq 1$ such that M_i/M_{i+1} is not x-torsion free.

Pick a least such i. Let N/M_{i+1} be the x-torsion part of M_i/M_{i+1}; thus M_i/N is x-torsion free.

As each M_j/M_{j+1} is x-torsion free for all $j < i$, M/N is also x-torsion free by Lemma 3.1.2(a). Hence, by Lemma 3.1.2(b), $\mathcal{K}(M/Mx) \geq \mathcal{K}(N/Nx)$.

Since M is x-torsion free and $0 < N \subseteq M$, N is also x-torsion free. Hence, by Lemma 3.1.2 (c), $\mathcal{K}(N/Nx) = \mathcal{K}(N/Nx^n)$ for all $n \geq 1$.

As M is Noetherian and N/M_{i+1} is x-torsion, there exists $n \geq 1$ such that $(N/M_{i+1})x^n = 0$. Hence $Nx^n \subseteq M_{i+1}$, so $N/Nx^n \twoheadrightarrow N/M_{i+1}$ and $\mathcal{K}(N/Nx^n) \geq \mathcal{K}(N/M_{i+1})$.

Since N/M_{i+1} is a nonzero submodule of the $(\beta-1)$-critical M_i/M_{i+1}, we deduce that $\mathcal{K}(N/M_{i+1}) = \beta - 1 = \mathcal{K}(M) - 1$. The result follows.

Case 2: M_i/M_{i+1} is x-torsion free $\forall i \geq 1$.

Consider the chain

$$M = Mx + M_1 \geq Mx + M_2 \geq \ldots \geq Mx. \qquad (\dagger)$$

Now, M_i/M_{i+1} is x-torsion free and has Krull dimension $\beta - 1$, so by induction, $\mathcal{K}((M_i/M_{i+1})/(M_i/M_{i+1}).x) \geq \beta - 2$. But

$$\frac{M_i/M_{i+1}}{(M_i/M_{i+1}).x} = \frac{M_i/M_{i+1}}{(M_ix + M_{i+1})/M_{i+1}} \cong \frac{M_i}{M_ix + M_{i+1}}, \quad \text{and}$$

$$\frac{M_i + Mx}{M_{i+1} + Mx} \cong \frac{M_i}{(M_{i+1} + Mx) \cap M_i} = \frac{M_i}{M_{i+1} + (M_i \cap Mx)}.$$

Since M/M_i is x-torsion free by Lemma 3.1.2 (a), $M_i \cap Mx = M_ix$ by Lemma 3.1.2(b), so every factor of $(\dagger)$ has Krull dimension $\geq \beta - 2$. Hence

$\mathcal{K}(M/Mx) \geq \beta - 1 = \mathcal{K}(M) - 1.$ □

Proof of Theorem 3.1.1. Since x is regular, R_R is x-torsion free. By Lemma 3.1.2 (c), the chain $R > xR > \ldots > x^kR > \ldots$ has infinitely many factors with Krull dimension equal to $\mathcal{K}(R/xR)$, so $\mathcal{K}(R) > \mathcal{K}(R/xR)$. The result follows from Lemma 3.1.3. □

We remark that as x is normal, xR is an ideal of R and so the Krull dimensions of R/xR over R and over the ring R/xR coincide.

Corollary 3.1.4. *Let G be a uniform pro-p group. Then*

$$\mathcal{K}(\Lambda_G) = \mathcal{K}(\Omega_G) + 1.$$

Proof. Λ_G is local by Theorem 2.6.3(iii) and p is clearly a central nonunit; thus $p \in J(\Lambda_G)$. By Theorem 2.6.5 (i), p is regular and Λ_G is Noetherian. The result follows from Theorem 3.1.1. □

3.2 A lower bound

Definition 3.2.1. *Let $\mathfrak{g}$ be a finite dimensional Lie algebra over a field k. Define $\lambda(\mathfrak{g})$ to be the maximum length m of chains $0 = \mathfrak{g}_0 < \mathfrak{g}_1 < \ldots < \mathfrak{g}_m = \mathfrak{g}$ of sub-Lie-algebras of $\mathfrak{g}$.*

This section is devoted to proving the following lower bound for the Krull dimension of Ω_G:

Theorem 3.2.2. *Let G be a uniform pro-p group with Lie algebra $\mathfrak{g} = \mathcal{L}(G)$. Then $\lambda(\mathfrak{g}) \leq \mathcal{K}(\Omega_G)$.*

First we collect together some equivalent conditions for a cyclic Ω_G-module to be Artinian.

Proposition 3.2.3. *Let G be a uniform pro-p group with lower p-series $\{G_n, n \geq 1\}$. Let $M = \Omega_G/I$ be a cyclic Ω_G-module. The following are equivalent:*

(i) M is Artinian.

(ii) $J_G^n \subseteq I$ for some $n \in \mathbb{N}$.

(iii) $J_{G_m} \subseteq I$ for some $m \geq 1$.

(iv) M is finite dimensional over $\mathbb{F}_p$.

Proof. Recall that G_n is uniform for each $n \geq 1$ by Proposition 2.5.6(iv), and that J_{G_n} denotes the maximal ideal of Ω_{G_n}.

(i) $\Rightarrow$ (ii). As Ω_G is Noetherian, M has finite composition length. Also Ω_G/J_G is the unique simple Ω_G-module, as Ω_G is local. Hence $MJ_G^n = 0$.

(ii) $\Rightarrow$ (iii). Suppose $J_G^n \subseteq I$. Choose m such that $p^{m-1} \geq n$. Then $g^{p^{m-1}} - 1 = (g-1)^{p^{m-1}} \in J_G^n \subseteq I$ for all $g \in G$. As $G_m = G^{p^{m-1}}$ by Proposition 2.5.6(i), we see that $G_m - 1 \subseteq I$ so $J_{G_m} \subseteq I$ as required.

(iii) $\Rightarrow$ (iv). If $J_{G_m} \subseteq I$, $J_{G_m}\Omega_G \subseteq I$ as I is a right ideal of Ω_G. Hence $\mathbb{F}_p[G/G_m] \cong \Omega_G/J_{G_m}\Omega_G \twoheadrightarrow \Omega_G/I = M$. Since $|G : G_m|$ is finite, the result follows.

(iv) $\Rightarrow$ (i). This is clear. □

Next comes a flatness result.

Lemma 3.2.4. *Let G be a profinite group and H a closed subgroup of G. Then Ω_G is a projective and hence flat Ω_H-module.*

Proof. This is Lemma 4.5 of [5]. □

The main step comes next.

Proposition 3.2.5. *Let G be a uniform pro-p group and let H be a closed uniform subgroup such that $|G : H| = \infty$. Then:*

(i) The induced module $M = \mathbb{F}_p \otimes_{\Omega_H} \Omega_G$ is not Artinian over Ω_G.

(ii) $\mathcal{K}(\Omega_H) < \mathcal{K}(\Omega_G)$.

Proof. (i) Since $\mathbb{F}_p \cong \Omega_H/J_H$ and since $- \otimes_{\Omega_H} \Omega_G$ is flat by Lemma 3.2.4, we see that $M \cong \Omega_G/J_H\Omega_G$ as right Ω_G-modules.

Suppose M is Artinian. Then $J_{G_m} \subseteq J_H\Omega_G$ for some $m \geq 1$, by Proposition 3.2.3. It is easy to check that $(1 + J_H\Omega_G) \cap G = H$ for any closed subgroup H of any profinite group G. Hence

$$G_m = (1 + J_{G_m}\Omega_G) \cap G \subseteq (1 + J_H\Omega_G) \cap G = H$$

which forces $|G : H|$ to be finite, a contradiction.

(ii) Consider the increasing function $f : \mathrm{Lat}(\Omega_H) \to \mathrm{Lat}(\Omega_G)$, given by $I \mapsto I \otimes_{\Omega_H} \Omega_G$. Suppose $X, Y \lhd_r \Omega_H$ are such that X/Y is simple. Since Ω_H is local, $X/Y \cong \mathbb{F}_p$ so $f(X)/f(Y) \cong \mathbb{F}_p \otimes_{\Omega_H} \Omega_G \cong M$ as Ω_G is a flat Ω_H-module. As M is not Artinian by part (i), $\mathcal{K}(f(X)/f(Y)) \geq 1$, so by Lemma 2.3.4 $\mathcal{K}(\Omega_H) + 1 \leq \mathcal{K}(\Omega_G)$, as required. □

Note that the analogous proposition for universal enveloping algebras is false: for example, the Verma module of highest weight zero for $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{C})$ is Artinian ([10], 7.6.1), and indeed, $\mathcal{K}(\mathcal{U}(\mathfrak{g})) = \mathcal{K}(\mathcal{U}(\mathfrak{b})) = 2$, where $\mathfrak{b}$ is a Borel subalgebra of $\mathfrak{g}$ (see [27]).

Proof of Theorem 3.2.2. Proceed by induction on $\lambda(\mathfrak{g})$. Let $0 = \mathfrak{g}_0 < \mathfrak{g}_1 < \ldots < \mathfrak{g}_k = \mathfrak{g}$ be a chain of maximal length $k = \lambda(\mathfrak{g})$ in $\mathfrak{g}$.

Let H be the isolated uniform subgroup of G with Lie algebra $\mathfrak{g}_{k-1}$ (see the remarks following Corollary 2.5.12). Since $\mathfrak{h} < \mathfrak{g}$, $|G : H| = \infty$.

By the inductive hypothesis, $k - 1 = \lambda(\mathfrak{g}_{k-1}) \leq \mathcal{K}(\Omega_H)$. By Proposition 3.2.5, $\mathcal{K}(\Omega_H) < \mathcal{K}(\Omega_G)$, so $k = \lambda(\mathfrak{g}) \leq \mathcal{K}(\Omega_G)$, as required. □

Theorem 3.2.2 stimulates interest in the length $\lambda(\mathfrak{g})$ of a finite dimensional Lie algebra $\mathfrak{g}$. The following facts about this invariant are known:

Proposition 3.2.6. *Let $\mathfrak{g}$ be a finite dimensional Lie algebra over a field k.*

(i) If $\mathfrak{h}$ is an ideal of $\mathfrak{g}$, $\lambda(\mathfrak{g}) = \lambda(\mathfrak{h}) + \lambda(\mathfrak{g}/\mathfrak{h})$.

(ii) If $\mathfrak{g}$ is solvable, $\lambda(\mathfrak{g}) = \dim_k(\mathfrak{g})$,

(iii) If $\mathfrak{g}$ is split semisimple, $\lambda(\mathfrak{g}) \geq \dim \mathfrak{b} + \dim \mathfrak{t}$, where $\mathfrak{t}$ and $\mathfrak{b}$ are some Cartan and Borel subalgebras of $\mathfrak{g}$, respectively.

(iv) $\lambda(\mathfrak{sl}_2(k)) = 3$.

Proof. (i)Putting together two chains of maximal length in $\mathfrak{h}$ and $\mathfrak{g}/\mathfrak{h}$ shows that $\lambda(\mathfrak{g}) \geq \lambda(\mathfrak{h}) + \lambda(\mathfrak{g}/\mathfrak{h})$. The reverse inequality follows by considering the chains $0 = \mathfrak{g}_0 \cap \mathfrak{h} \subseteq \ldots \subseteq \mathfrak{g}_i \cap \mathfrak{h} \subseteq \ldots \subseteq \mathfrak{h}$ and $\mathfrak{h} \subseteq \mathfrak{g}_1 + \mathfrak{h} \subseteq \ldots \subseteq \mathfrak{g}_i + \mathfrak{h} \subseteq \ldots \subseteq \mathfrak{g}$ whenever $0 = \mathfrak{g}_0 < \ldots < \mathfrak{g}_i < \ldots < \mathfrak{g}_n = \mathfrak{g}$ is a chain of subalgebras of maximal length in $\mathfrak{g}$.

(ii) This follows directly from (i).

(iii) Let $l = \dim \mathfrak{t}$. Given a Borel subalgebra $\mathfrak{b}$, there are exactly 2^l parabolic subalgebras containing it, corresponding bijectively with the subsets of the set of simple roots of $\mathfrak{g}$. This correspondence preserves inclusions, so we can find a chain of subalgebras of length l starting with $\mathfrak{b}$. Combining this together with a maximal chain of length $\dim \mathfrak{b}$ in $\mathfrak{b}$ gives the result.

(iv) This follows from (iii), since for $\mathfrak{g} = \mathfrak{sl}_2(k)$, $\dim \mathfrak{t} = 1, \dim \mathfrak{b} = 2$ and $\dim \mathfrak{g} = 3$. □

As a consequence, we can compute the Krull dimension of Ω_G in many cases:

Corollary 3.2.7. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}$. Let $\mathfrak{r}$ be the solvable radical of $\mathfrak{g}$, and suppose that the semisimple part $\mathfrak{g}/\mathfrak{r}$ of $\mathfrak{g}$ is isomorphic to a direct sum of copies of of $\mathfrak{sl}_2(\mathbb{Q}_p)$. Then $\mathcal{K}(\Omega_G) = \dim G$. In particular, this applies when $\mathfrak{g}$ is solvable or $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{Q}_p)$.*

Proof. By Proposition 3.2.6, $\lambda(\mathfrak{g}) = \dim \mathfrak{g}$, so $\dim \mathfrak{g} \leq \mathcal{K}(\Omega_G)$ by Theorem 3.2.2. On the other hand, $\mathcal{K}(\Omega_G) \leq \mathcal{K}(\operatorname{gr} \Omega_G) = \dim G = \dim \mathfrak{g}$ by Theorem 2.7.2(iv). The result follows. □

3.3 An upper bound

Proposition 3.2.6 suggests that when looking for uniform G with $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}$ such that $\mathcal{K}(\Omega_G) < \dim \mathfrak{g}$, we can restrict ourselves to semisimple $\mathfrak{g}$. Our main result is

Theorem 3.3.1. *Let $p \geq 5$ and let G be a uniform pro-p group with $\mathbb{Q}_p$ Lie algebra $\mathfrak{g}$. Suppose $\mathfrak{g}$ is split simple over $\mathbb{Q}_p$ and that $\mathfrak{g} \neq \mathfrak{sl}_2(\mathbb{Q}_p)$. Then*

$$\mathcal{K}(\Omega_G) \leq \dim \mathfrak{g} - 1.$$

The method of proof is similar in spirit to that used by S.P.Smith in his proof of the following theorem, providing an analogous better upper bound for $\mathcal{K}(\mathcal{U}(\mathfrak{g}))$ when $\mathfrak{g}$ is semisimple:

Theorem 3.3.2 (Smith). *Let $\mathfrak{g}$ be a complex semisimple Lie algebra. Let $2r+1$ be the dimension of the largest Heisenberg Lie algebra contained in $\mathfrak{g}$. Then $\mathcal{K}(\mathcal{U}(\mathfrak{g})) \leq \dim \mathfrak{g} - r - 1$.*

Proof. See Corollary 4.3 of [26], bearing in mind the comments contained in section 3.1 of that paper. □

Definition 3.3.3. *Let k be a field. The* Heisenberg k-Lie algebra *of dimension $2r+1$ is defined by the presentation*

$$\mathfrak{h}_{2r+1} = k < w, u_1, \ldots, u_r, v_1, \ldots, v_r : [u_i, v_j] = \delta_{ij} w, [w, u_i] = [w, v_i] = 0 >$$

Here δ_{ij} is the Kronecker delta.

First we establish some facts about uniform H with Lie algebra $\mathfrak{h}_{2r+1}$.

Lemma 3.3.4. *Let H be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{h}_{2r+1}$. Then*

(i) $Z(H) = \overline{< z >} \cong \mathbb{Z}_p$ is the isolated uniform subgroup of H with $\mathbb{Q}_p$-Lie algebra $\mathbb{Q}_p w$.

(ii) There exist $x, y \in H$ and $k \in \mathbb{N}$ such that $[x, y] = z^{p^k}$.

Proof. (i) This follows from Lemma 2.5.13, since $\mathbb{Q}_p w = Z(\mathfrak{h}_{2r+1})$.

(ii) To avoid confusion, we will denote by $(,)$ the Lie bracket on $\mathcal{L}(H) = \mathfrak{h}_{2r+1}$. Since $(L_H, (L_H, L_H)) \subseteq (\mathfrak{h}_{2r+1}, (\mathfrak{h}_{2r+1}, \mathfrak{h}_{2r+1})) = 0$, the group law on

L_H given by the Campbell-Hausdorff series reduces to

$$\alpha * \beta = \alpha + \beta + \frac{1}{2}(\alpha, \beta)$$

for $\alpha, \beta \in L_H$. It's then easily checked that the group commutator satisfies

$$[\alpha, \beta] = \alpha^{-1} * \beta^{-1} * \alpha * \beta = (\alpha, \beta).(\dagger)$$

Now as $\mathbb{Q}_p L_H = \mathfrak{h}_{2r+1}$ there exists $n \in \mathbb{N}$ such that $p^n u_1, p^n v_1 \in L_H$, whence $(p^n u_1, p^n v_1) \in L_H \cap \mathbb{Q}_p w = \mathbb{Z}_p z$. Hence $(p^n u_1, p^n v_1) = p^k \lambda z$ for some unit $\lambda \in \mathbb{Z}_p$ and some $k \in \mathbb{N}$, an equation inside L_H. We may now take $x = p^n \lambda^{-1} u_1$, $y = p^n v_1$ and apply (†). □

The following proposition is the main step in our proof of the upper bound for $\mathcal{K}(\Omega_G)$.

Proposition 3.3.5. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}$ such that $\mathfrak{h}_3 \subseteq \mathfrak{g}$. Let H be the uniform subgroup of G with Lie algebra $\mathfrak{h}_3$. Let $Z = Z(H) = \overline{< z >}$, say. Let M be a finitely generated Ω_G-module such that $d(M) \leq 1$. Then $\sigma(z-1) \in J(M)$.*

Proof. See Section 2.4 for the definition of the characteristic ideal $J(M)$ and the graded dimension $d(M)$ of M.

Let A be a uniform subgroup of G with torsion-free L_G/L_A. By Corollary 2.7.3, the subspace filtration on Ω_A induced from the J_G-adic filtration on Ω_G coincides with the J_A-adic filtration.

It follows that the Rees ring $\widetilde{\Omega}_A$ of Ω_A embeds into $\widetilde{\Omega}_G$ and that $\widetilde{\Omega}_A \cap t\widetilde{\Omega}_G = t\widetilde{\Omega}_A$, so this embedding induces a natural embedding of graded rings

$$\operatorname{gr}\Omega_A = \widetilde{\Omega}_A/t\widetilde{\Omega}_A \hookrightarrow \widetilde{\Omega}_G/t\widetilde{\Omega}_G = \operatorname{gr}\Omega_G.$$

Note that by Lemma 3.3.4(i), L_H/L_Z is torsion-free. Hence L_G/L_Z is also torsion-free, so the above discussion applies to both Z and H.

We remind the reader that $\operatorname{gr}\Omega_G$ and $\operatorname{gr}\Omega_A$ are polynomial algebras over $\mathbb{F}_p$, by Theorem 2.7.2.

Now, equip M with a good filtration FM and consider the Rees module $\widetilde{M}$. This is an $\widetilde{\Omega}_G$-module, so we can view it as an $\widetilde{\Omega}_H$-module by restriction.

Let $S = \widetilde{\Omega}_Z - t\widetilde{\Omega}_Z$. This is a central multiplicatively closed subset of the domain $\widetilde{\Omega}_H$, so we may form the localisations $\widetilde{\Omega}_Z S^{-1} \hookrightarrow \widetilde{\Omega}_H S^{-1}$ and the localised $\widetilde{\Omega}_H.S^{-1}$-module $\widetilde{M}S^{-1}$.

Let $R = \varprojlim \widetilde{\Omega}_Z S^{-1}/t^n.\widetilde{\Omega}_Z S^{-1}$ and let $N = \varprojlim \widetilde{M}S^{-1}/t^n.\widetilde{M}S^{-1}$.

It's clear that N is an R-module. Also, as t is central in $\widetilde{\Omega}_H S^{-1}$, N has the structure of a $\widetilde{\Omega}_H S^{-1}$-module. In particular, as H embeds into $\widetilde{\Omega}_H S^{-1}$, N is an H-module.

Now, consider the t-adic filtration on R. It's easy to see that

$$R/tR = \widetilde{\Omega}_Z S^{-1}/t\widetilde{\Omega}_Z S^{-1} \cong \operatorname{gr}\Omega_Z.\bar{S}^{-1},$$

where $\bar{S} = \operatorname{gr}\Omega_Z - \{0\}$. Thus $R/tR \cong k$, the field of fractions of $\operatorname{gr}\Omega_Z$.

As t acts injectively on $\widetilde{\Omega}_Z S^{-1}$, $t^n R/t^{n+1}R \cong k$ for all $n \geq 0$. Hence the graded ring of R with respect to the t-adic filtration is

$$\operatorname{gr}_t R = \bigoplus_{n=0}^{\infty} \frac{t^n R}{t^{n+1}R} \cong k[s],$$

where $s = t + t^2 R \in tR/t^2 R$.

We can also consider the t-adic filtration on N. Again, we see that $N/tN \cong t^n N/t^{n+1}N \cong \operatorname{gr} M.\bar{S}^{-1}$. Hence

$$\operatorname{gr}_t N = \bigoplus_{n=0}^{\infty} t^n N/t^{n+1}N \cong (\operatorname{gr} M.\bar{S}^{-1}) \otimes_k k[s].$$

Now, because $d(M) \leq 1$, $\operatorname{gr} M.\bar{S}^{-1}$ is finite dimensional over k. It follows that $\operatorname{gr}_t N$ is a finitely generated $\operatorname{gr}_t R$-module.

Because N is complete with respect to the t-adic filtration, this filtration on N is separated. Also R is complete, so by Theorem 2.2.5, N is finitely generated over R.

Now $\widetilde{\Omega}_Z S^{-1}$ is a local ring with maximal ideal $t\widetilde{\Omega}_Z S^{-1}$. Hence R is a commutative local ring with maximal ideal tR; since $\cap_{n=0}^{\infty} t^n R = 0$, the only ideals of R are $\{t^n R : n \geq 0\}$.

Hence R is a commutative principal ideal domain and N is a finitely generated t-torsionfree R-module. This forces N to be free over R, say $N \cong R^n$, for some $n \geq 0$.

Now, Z embeds into R and the action of R commutes with the action of H on N. Hence we get a group homomorphism

$$\rho : H \to GL_n(R)$$

such that $\rho(z) = zI$, where I is the $n \times n$ identity matrix.

But H is a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{h}_3$, so by Lemma 3.3.4(ii) we can find elements $x, y \in H$ such that $[x, y] = z^{p^k}$ for some $k \geq 1$.

Hence $[\rho(x), \rho(y)] = \rho(z)^{p^k} = z^{p^k}.I$. Taking determinants yields $z^{np^k} = 1$. Since $Z = \overline{< z >} \cong \mathbb{Z}_p$, this is only possible if $n = 0$.

Therefore $N = 0$ and so $N/tN = \operatorname{gr} M.\bar{S}^{-1} = 0$. Hence $Q \cap \bar{S} \neq 0$, where $Q = \operatorname{Ann}_{\operatorname{gr} \Omega_G} \operatorname{gr} M$. Because Q is graded and because $\operatorname{gr} \Omega_Z \cong \mathbb{F}_p[\sigma(z-1)]$, we see that $\sigma(z-1)^m \in Q$ for some $m \geq 0$. Hence $\sigma(z-1) \in J(M) = \sqrt{Q}$. □

Let G be a uniform pro-p group, and consider the set G/G_2, where $G_2 = P_2(G) = G^p$. We know that G/G_2 is a vector space over $\mathbb{F}_p$ of dimension $d = \dim(G)$. The automorphism group $\operatorname{Aut}(G)$ of G acts naturally on G/G_2; this action commutes with the $\mathbb{F}_p$-linear structure on G/G_2. Because $[G, G] \subseteq G_2$ the action of $\operatorname{Inn}(G)$ is trivial, so we see that G/G_2 is naturally an $\mathbb{F}_p[\operatorname{Out}(G)]$-module.

Similarly, we obtain an action of $\operatorname{Aut}(G)$ on J/J^2 where $J = J_G \triangleleft \Omega_G$; it's easy to see that $\operatorname{Inn}(G)$ again acts trivially, so J/J^2 is also an $\mathbb{F}_p[\operatorname{Out}(G)]$-module.

Lemma 3.3.6. *The map $\varphi : G/G_2 \to J/J^2$ given by $\varphi(gG_2) = \sigma(g-1) = g - 1 + J^2$ is an isomorphism of $\mathbb{F}_p[\mathrm{Out}(G)]$-modules.*

Proof. It is easy to check that φ is an $\mathbb{F}_p$-linear map preserving the $\mathrm{Out}(G)$-structure.

Now $\{g_1G_2, \ldots, g_dG_2\}$ is a basis for G/G_2, if $\{g_1, \ldots, g_d\}$ is a topological generating set for G. By Theorem 2.7.2(v), $\{X_1, \ldots, X_d\}$ is a basis for J/J^2, where $X_i = \sigma(g_i - 1) = \varphi(g_iG_2)$. The result follows. □

Theorem 3.3.7. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}$, such that $\mathfrak{h}_3 \hookrightarrow \mathfrak{g}$. Let $z \in G - G_2$ be such that $\mathbb{Q}_p z = Z(\mathfrak{h}_3)$. Suppose zG_2 generates the $\mathbb{F}_p[\mathrm{Out}(G)]$-module G/G_2. Then*

(i) Ω_G has no finitely generated modules M with $d(M) = 1$

(ii) $\mathcal{K}(\Omega_G) \leq \dim \mathfrak{g} - 1$.

Proof. Let M be a finitely generated Ω_G-module with $d(M) \leq 1$. By Lemma 3.3.6, $G/G_2 \cong J/J^2$ as $\mathbb{F}_p[\mathrm{Out}(G)]$-modules. Because zG_2 generates G/G_2, $\varphi(zG_2) = \sigma(z-1) \in J/J^2$ generates J/J^2. In other words, $\mathbb{F}_p.\{\sigma(z-1)^\alpha : \alpha \in \mathrm{Out}(G)\} = J/J^2$.

Now, we can find a uniform subgroup H of G with Lie algebra isomorphic to $\mathfrak{h}_3$ such that $Z(H) = \overline{< z >}$. Let $\theta \in \mathrm{Aut}(G)$. By Proposition 3.3.5 applied to H^θ, $\sigma(z^\theta - 1) = \sigma(z-1)^{\bar{\theta}} \in J(M)$, where $^-$: $\mathrm{Aut}(G) \to \mathrm{Out}(G)$ is the natural surjection.

Hence $J/J^2 = \mathbb{F}_p.\{\sigma(z-1)^\alpha : \alpha \in \mathrm{Out}(G)\} \subseteq J(M)$. This forces $(X_1, \ldots, X_d) \subseteq J(M) \subseteq \mathbb{F}_p[X_1, \ldots, X_d] = \mathrm{gr}\,\Omega_G$, whence $d(M) = 0$ and part (i) follows.

Consider the increasing map $\mathrm{gr} : \mathrm{Lat}(\Omega_G) \to \mathrm{Lat}(\mathrm{gr}\,\Omega_G)$, where we endow each right ideal of Ω_G with the subspace filtration from the J_G-adic filtration on Ω_G. If $X, Y \triangleleft_r \Omega_G$ are such that $M = X/Y$ is 1-critical, then $\mathcal{K}(\mathrm{gr}\,M) = \mathcal{K}(\mathrm{gr}\,X/\,\mathrm{gr}\,Y) \geq 1$, giving M the subquotient filtration from Ω_G. This filtration is good since $\widetilde{\Omega_G}$ is Noetherian, so $d(M) \geq 1$ by Lemma 2.4.3. By part (i), $\mathcal{K}(\mathrm{gr}\,X/\,\mathrm{gr}\,Y) \geq 2$ so part (ii) follows by Lemma 2.3.4. □

We will use this result to deduce Theorem 3.3.1, but first we must establish some facts about Chevalley groups defined over $\mathbb{Z}_p$.

3.4 Chevalley groups over $\mathbb{Z}_p$

Let X be an indecomposable root system. We have a $\mathbb{Z}_p$-Lie algebra $X_{\mathbb{Z}_p}$, defined in section 2.8. Since $[pX_{\mathbb{Z}_p}, pX_{\mathbb{Z}_p}] = p^2[X_{\mathbb{Z}_p}, X_{\mathbb{Z}_p}] \subseteq p.pX_{\mathbb{Z}_p}$, we see that $pX_{\mathbb{Z}_p}$ is a powerful $\mathbb{Z}_p$-Lie algebra. Let $Y = (pX_{\mathbb{Z}_p}, *)$ be the uniform pro-p group constructed from $pX_{\mathbb{Z}_p}$ using the Campbell-Hausdorff formula in Theorem 2.5.10.

There is a group homomorphism $\mathrm{Ad} : Y \to GL(pX_{\mathbb{Z}_p})$ given by $\mathrm{Ad}(g)(u) = gug^{-1}$. It is shown in Exercise 9.10 of [11] that $\mathrm{Ad} = \exp \circ \mathrm{ad}$ where $\exp : \mathfrak{gl}(pX_{\mathbb{Z}_p}) \to GL(pX_{\mathbb{Z}_p})$ is the exponential map.

It's clear that $\ker \mathrm{Ad} = Z(Y)$. By Lemma 2.5.13, $\mathcal{L}(Z(Y)) = Z(\mathcal{L}(Y)) = 0$ since the Lie algebra $X_{\mathbb{Q}_p}$ of Y is simple; hence $\ker \mathrm{Ad} = 1$ and Ad is an injection.

Lemma 3.4.1. *Let $N = \mathrm{Ad}(Y)$ and $G = X(\mathbb{Z}_p)$. Then $N \triangleleft G$.*

Proof. First we show that $N \subseteq G$. The set $p\mathcal{B}$ is a $\mathbb{Z}_p$-basis for $pX_{\mathbb{Z}_p}$ and hence a topological generating set for Y by Theorem 9.8 of [11]. By Proposition 3.7 of [11], Y is equal to the product of the procyclic subgroups $pu\mathbb{Z}_p$ as u ranges over $\mathcal{B}$. Hence it's sufficient to show that $\mathrm{Ad}(pu\mathbb{Z}_p) \subseteq G$ for all $u \in \mathcal{B}$.

It's clear that the $\mathbb{Z}_p$-linear action of N on $pX_{\mathbb{Z}_p}$ extends naturally to a $\mathbb{Z}_p$-linear action of N on $X_{\mathbb{Z}_p}$. Now, direct computation using Proposition 2.8.8 shows that

$$\begin{aligned} \mathrm{Ad}(te_r) &= x_r(t), & t \in p\mathbb{Z}_p, r \in X \text{ and} \\ \mathrm{Ad}(th_r) &= h_r(\exp(t)), & t \in p\mathbb{Z}_p, r \in \Pi. \end{aligned}$$

Hence $N \subseteq G$.

Now, let $r, s \in X$, $t \in \mathbb{Z}_p$ and $u \in p\mathbb{Z}_p$. By Proposition 2.8.9, we have

$$x_r(t)x_s(u)x_r(t)^{-1} = x_s(u). \prod_{i,j>0} x_{ir+js}(C_{ijrs}t^iu^j) \in N$$

$$x_r(t)h_s(\exp(u))x_r(t)^{-1} = h_s(\exp(u))x_r(\exp(-A_{sr}u)t)x_r(-t) \in N$$

since $C_{ijrs}t^iu^j \in p\mathbb{Z}_p$ and $\exp(-A_{sr}u) - 1 \in p\mathbb{Z}_p$, whenever $u \in p\mathbb{Z}_p$.

Hence $N \lhd G$, as required. □

Theorem 3.4.2. *There exists a commutative diagram of group homomorphisms:*

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "\beta"'] & X(\mathbb{F}_p) \arrow[r, "\iota"] & \mathrm{Aut}(X_{\mathbb{F}_p}) \arrow[d, "\varphi^*"] \\ \mathrm{Aut}(N) \arrow[r, "\pi"'] & \mathrm{Out}(N) \arrow[r, "\gamma"'] & \mathrm{Aut}(N/N_2) \end{tikzcd}$$

Proof. We begin by defining all the relevant maps. Any automorphism f of $X_{\mathbb{Z}_p}$ must fix $pX_{\mathbb{Z}_p}$ and hence induces an automorphism $\alpha(f)$ of $X_{\mathbb{F}_p} \cong$

$X_{\mathbb{Z}_p}/pX_{\mathbb{Z}_p}$. It's clear from the definition of the Chevalley groups that $\alpha(x_r(t)) = x_r(\bar{t})$, where$^-$: $\mathbb{Z}_p \to \mathbb{F}_p$ is reduction mod p.

Since Ad is an isomorphism of Y onto N, N is a uniform pro-p group, and we have an $\mathbb{F}_p$-linear bijection $\varphi : X_{\mathbb{F}_p} \to N/N_2$ given by $\varphi(\bar{x}) = \mathrm{Ad}(px)N_2$, where $^-$: $X_{\mathbb{Z}_p} \to X_{\mathbb{F}_p}$ is the natural map. This induces an isomorphism $\varphi^* : \mathrm{Aut}(X_{\mathbb{F}_p}) \to \mathrm{Aut}(N/N_2)$ given by $\varphi^*(f) = \varphi f \varphi^{-1}$.

We have observed in the remarks preceding Lemma 3.3.6 that $\mathrm{Out}(N)$ acts naturally on N/N_2; we denote this action by γ. By Lemma 3.4.1 N is normal in G, and we denote the conjugation action of G on N by β.

Finally, ι is the natural injection of $X(\mathbb{F}_p)$ into $\mathrm{Aut}(X_{\mathbb{F}_p})$ and π is the natural projection of $\mathrm{Aut}(N)$ onto $\mathrm{Out}(N)$.

It remains to check that $\varphi^*\iota\alpha = \gamma\pi\beta$. It is sufficient to check that $\varphi^*\iota\alpha(x_r(t)) = \gamma\pi\beta(x_r(t))$ for any $r \in X$ and $t \in \mathbb{Z}_p$. We check these maps agree on the basis $\{\mathrm{Ad}(pu).N_2 : u \in \mathcal{B}\}$ of N/N_2. On the one hand, we have

$$\begin{aligned}
\varphi^*\iota\alpha(x_r(t))(\mathrm{Ad}(pe_s)N_2) &= \varphi^*(x_r(\bar{t}))(\mathrm{Ad}(pe_s)N_2) = \varphi(x_r(\bar{t})(\overline{e_s})) = \\
&= \varphi(\sum_{i=0}^{q} M_{r,s,i}\bar{t}^i\overline{e_{ir+s}}) = \\
&= \prod_{i=0}^{q} \mathrm{Ad}(pM_{r,s,i}t^i e_{ir+s})N_2 = \\
&= \prod_{i=0}^{q} x_{ir+s}(pM_{r,s,i}t^i)N_2, (\dagger)
\end{aligned}$$

using the definition of the action of $x_r(\bar{t})$ on $X_{\mathbb{F}_p}$ given in Proposition 2.8.3. On the other hand,

$$\begin{aligned}\gamma\pi\beta(x_r(t))(\mathrm{Ad}(pe_s)N_2) &= x_r(t)x_s(p)x_r(-t)N_2 = \\ &= x_s(p)\prod_{i,j>0} x_{ir+js}(C_{ijrs}t^ip^j)N_2,\end{aligned}$$

using the relations given in Proposition 2.8.9.

Since $x_\alpha(p^2) \in N_2$ for any $\alpha \in X$, we see that the all the terms in the above product with $j > 1$ vanish, and the remaining expression is equal to the result of (†), since $C_{i1rs} = M_{r,s,i}$.

A similar computation shows that $\varphi^*\iota\alpha(x_r(t))$ also agrees with $\gamma\pi\beta(x_r(t))$ on $\mathrm{Ad}(ph_s)N_2$ for any $s \in \Pi$, and the result follows. □

The above theorem shows that the action of $\mathrm{Out}(N)$ on N/N_2 which was of interest in the preceding section is linked to the natural action of $X(\mathbb{F}_p)$ on $X_{\mathbb{F}_p}$. In particular, it's clear that if $\bar{e_r}$ generates $X_{\mathbb{F}_p}$ as an $\mathbb{F}_p[X(\mathbb{F}_p)]$-module, then $\mathrm{Ad}(pe_r)N_2$ generates N/N_2 as an $\mathbb{F}_p[\mathrm{Out}(N)]$-module. We drop the bars in the following proposition.

Proposition 3.4.3. *Suppose $p \geq 5$ and let $R = \mathbb{F}_p[X(\mathbb{F}_p)]$. Then $X_{\mathbb{F}_p} = R.e_r$ for any $r \in X$.*

Proof. This is probably well known and is purely a matter of computation. We use Proposition 2.8.8 in what follows without mention. Let W denote the Weyl group of X.

Note that $(x_{-r}(1)+\eta_{r,r}n_r-1).e_r = h_{-r} \in R.e_r$, whence $h_r = -h_{-r} \in R.e_r$ also.

By Proposition 2.1.8 of [7], we can choose $w \in W$ such that $w(r) = \beta \in \Pi$. Hence $n_w.h_r = h_\beta \in R.e_r$.

Next, $n_\alpha.h_\beta = h_{w_\alpha(\beta)} = h_\beta - A_{\beta\alpha}h_\alpha$ if $\alpha \in \Pi$. Since $p \geq 5$, the tables of Cartan matrices on pages 44-45 of [7] show that $A_{\beta\alpha} \neq 0$ in $\mathbb{F}_p$, whence $h_\alpha \subseteq R.e_r$ for any $\alpha \in \Pi$. Since the fundamental coroots span the Cartan subalgebra over $\mathbb{Z}$, $h_s \in R.e_r$ for any $s \in X$.

Finally. $x_s(1).h_s = h_s - 2e_s$, whence $e_s \in R.e_r$ for any $s \in X$, since $p \neq 2$. Since $\{e_s, h_r : s \in X, r \in \Pi\}$ is a basis for $X_{\mathbb{F}_p}$, the result follows. □

We can finally provide a proof of the main result.

Proof of Theorem 3.3.1. Let X be the root system of $\mathfrak{g}$; thus $\mathfrak{g} = X_{\mathbb{Q}_p}$. Since X is not of type A_1 by assumption on $\mathfrak{g}$, we can find two roots $r, s \in X$ such that $r + s \in X$ but $r + 2s, 2r + s \notin X$; it's then easy to see that the root spaces of r and s generate a subalgebra of $\mathfrak{g}$ isomorphic to $\mathfrak{h}_3$ with centre $\mathbb{Q}_p e_{r+s}$.

Let N be the uniform pro-p group appearing in the statement of Lemma 3.4.1. By construction, $\mathfrak{g}$ is the Lie algebra of N. By Proposition 3.4.3 and the remarks preceding it, we see that $\mathrm{Ad}(pe_{r+s})N_2 \in N/N_2$ generates the $\mathbb{F}_p[\mathrm{Out}(N)]$-module N/N_2. Hence $\mathcal{K}(\Omega_N) \leq \dim \mathfrak{g} - 1$ by Theorem 3.3.7.

Since the Lie algebra of G is $\mathfrak{g} = \mathbb{Q}_p L_G = \mathbb{Q}_p L_N$, we see that $N \cap G$ is an open subgroup of both N and G, so we can find an open normal subgroup K of both N and G. By Lemma 2.7.4, $\mathcal{K}(\Omega_G) = \mathcal{K}(\Omega_K) = \mathcal{K}(\Omega_N) \leq \dim \mathfrak{g} - 1$, as required. □

Putting the two bounds together, we obtain

Corollary 3.4.4. *Suppose $p \geq 5$ and let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{sl}_3(\mathbb{Q}_p)$. Then*

$$\mathcal{K}(\Omega_G) = 7.$$

Proof. By Theorem 3.3.1, $\mathcal{K}(\Omega_G) \leq 7$, since $\dim \mathfrak{g} = 8$. If $\mathfrak{b}$ and $\mathfrak{t}$ denote the Borel and Cartan subalgebras of $\mathfrak{g}$, then $\dim \mathfrak{b} = 5$ and $\dim \mathfrak{t} = 2$. Hence $\mathcal{K}(\Omega_G) \geq 7$ by Proposition 3.2.6(iii) and Theorem 3.2.2. The result follows. □

This allows us to give a negative answer to the question stated in the introduction.

Corollary 3.4.5. *Let $p \geq 5$ and let $G = \ker(SL_3(\mathbb{Z}_p) \to SL_3(\mathbb{F}_p))$. Then Ω_G is a local right Noetherian ring whose Jacobson radical J satisfies the Artin Rees Property, but*

$$\mathcal{K}(\Omega_G) = 7 < \operatorname{gld}(\Omega_G) = 8.$$

Proof. It is readily seen that G is a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{sl}_3(\mathbb{Q}_p)$. Hence $\mathcal{K}(\Omega_G) = 7$ but $\operatorname{gld}(\Omega_G) = 8$, by Theorem 2.6.6.

By Theorem 2.7.2, the J-adic filtration on Ω_G is Zariskian. Hence, by Theorem 2.2 of Chapter II of [16], the J-adic filtration has the Artin Rees property, which is easily seen to imply that the ideal J has the Artin Rees Property in the sense of 4.2.3 of [23]. □

Proposition 3.3.5 should be compared to the Bernstein inequality for finitely generated modules M for the Weyl algebra $A_1(\mathbb{C})$, which gives a restriction on the possible values of the dimension of M. We are tempted to conjecture that the following generalization holds:

Conjecture. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{g}$ such that $\mathfrak{h}_{2r+1} \subseteq \mathfrak{g}$. Let H be the uniform subgroup of G with Lie algebra $\mathfrak{h}_{2r+1}$. Let $Z = Z(H) = \overline{< z >}$, say. Let M be a finitely generated Ω_G-module such that $d(M) \leq r$. Then $\sigma(z-1) \in J(M)$.*

This is a more general analogue of Lemma 3.2 of [26] corresponding to the Bernstein inequality for $A_r(\mathbb{C})$. If this conjecture is correct, we would be able to sharpen the upper bound on $\mathcal{K}(\Omega_G)$ from $\dim \mathfrak{g} - 1$ to $\dim \mathfrak{g} - r$, when G is as in Theorem 3.3.1.

We remark that when $\mathfrak{g}$ is itself a Heisenberg Lie algebra, a stronger result has been proved by Wadsley ([30]):

Theorem 3.4.6. *Let G be a uniform pro-p group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{h}_{2r+1}$ and centre Z. Let M be a finitely generated Ω_G-module such that $d(M) \leq r$. Then*

$$\mathrm{Ann}_{\Omega_G}(M) \cap \Omega_Z \neq 0.$$

Chapter 4

Endomorphism rings

4.1 Fixed points

In this section, we establish a technical but very useful result which will enable us to compute the centre of Ω_G and also the endomorphism ring of the induced module from the trivial module for a closed subgroup of G.

Let X be a group. For any (right) X-space S, let $S^X = \{s \in S : s.X = s\}$ denote the set of fixed points of X in S. Also, let $\mathcal{O}(S)$ denote the collection of all *finite* X-orbits on S, and for any orbit $\mathcal{C} \in \mathcal{O}(S)$, let $\hat{\mathcal{C}}$ denote the orbit sum

$$\hat{\mathcal{C}} = \sum_{s \in \mathcal{C}} s,$$

viewed as an element of the permutation module $\mathbb{F}_p[S]$. Thus, $\mathbb{F}_p[S]^X$ is spanned by all the $\hat{\mathcal{C}}$ as $\mathcal{C}$ ranges over $\mathcal{O}(S)$: $\mathbb{F}_p[S]^X = \mathbb{F}_p[\widehat{\mathcal{O}(S)}]$.

Now let X be a pro-p group. Assume we are given an inverse system

$$\ldots \overset{\pi_{n+1}}{\twoheadrightarrow} A_n \overset{\pi_n}{\twoheadrightarrow} A_{n-1} \overset{\pi_{n-1}}{\twoheadrightarrow} \ldots \overset{\pi_2}{\twoheadrightarrow} A_1$$

of finite X-spaces. We can consider the natural inverse system of permutation modules associated with the A_i:

$$\ldots \overset{\pi_{n+1}}{\twoheadrightarrow} \mathbb{F}_p[A_n] \overset{\pi_n}{\twoheadrightarrow} \mathbb{F}_p[A_{n-1}] \overset{\pi_{n-1}}{\twoheadrightarrow} \ldots \overset{\pi_2}{\twoheadrightarrow} \mathbb{F}_p[A_1]$$

where we keep the same notation for the connecting maps π_n. Now, form the inverse limit

$$Y = \varprojlim A_n,$$

this is clearly an X-space. We can also form the inverse limit

$$\Omega_Y = \varprojlim \mathbb{F}_p[A_n],$$

which is easily seen to be an Ω_X-module.

We are interested in the fixed points of Ω_Y, viewed as an X-space. It's easy to see that there is a natural embedding of $\mathbb{F}_p[Y]$ into Ω_Y and that $\mathbb{F}_p[Y]^X \subseteq \Omega_Y^X$.

Proposition 4.1.1. *With the notations above,* $\Omega_Y^X = \overline{\mathbb{F}_p[Y]}^X = \overline{\mathbb{F}_p[Y]^X}$.

Proof. Because the action of X on Ω_Y is continuous, it's clear that Ω_Y^X is a closed subset of Ω_Y, so by the above remarks $\overline{\mathbb{F}_p[Y]^X} \subseteq \Omega_Y^X$.

Let $\alpha = (\alpha_n)_n \in \Omega_Y^X$. Since the natural maps $\Omega_Y \twoheadrightarrow \mathbb{F}_p[A_n]$ are maps of X-spaces, it's clear that each α_n lies in $\mathbb{F}_p[A_n]^X$.

Let the integer r be least such that $\alpha_r \neq 0$. Consider $\alpha_r \in \mathbb{F}_p[A_r]^X$; thus $\alpha_r = \sum_{\mathcal{C} \in \mathcal{O}(A_r)} \lambda_{\mathcal{C}} \hat{\mathcal{C}}$ and not all the $\lambda_{\mathcal{C}}$ are zero.

Pick a $\mathcal{C} \in \mathcal{O}(A_r)$ with $\lambda_{\mathcal{C}} \neq 0$. Since π_{r+1} is a map of X-spaces, $\pi_{r+1}^{-1}(\mathcal{C}) = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \ldots \cup \mathcal{D}_k$ is a union of X-orbits, with $\pi_{r+1}(\mathcal{D}_j) = \mathcal{C}$ for $j = 1, \ldots, k$ and $\pi_{r+1}(\mathcal{D}_j) \cap \mathcal{C} = \emptyset$ for $j > k$, if we let $\mathcal{D}_{k+1}, \ldots, \mathcal{D}_m$ denote the remaining elements of $\mathcal{O}(A_{r+1})$.

We claim we can find a $\mathcal{D}_j$ with $1 \leq j \leq k$ such that $|\mathcal{D}_j| = |\mathcal{C}|$.

For, suppose not. Then $|\mathcal{D}_j| > |\mathcal{C}|$ for each $j = 1, \ldots, k$. As $\pi_{r+1} : \mathcal{D}_j \twoheadrightarrow \mathcal{C}$ is a surjective map of finite transitive X-spaces, and because X is a pro-p group, we deduce that each fibre $(\pi_{r+1}|\mathcal{D}_j)^{-1}(s)$ for $s \in \mathcal{C}$ has size a power of p greater than 1. But then, because we are working over $\mathbb{F}_p$, we must have $\pi_{r+1}(\hat{\mathcal{D}}_j) = 0$, for each $1 \leq j \leq k$.

Now, since $\alpha_{r+1} \in \mathbb{F}_p[A_{r+1}]^X$, we can write $\alpha_{r+1} = \sum_{j=1}^{m} \mu_j \hat{\mathcal{D}}_j$ for some $\mu_j \in \mathbb{F}_p$. So, $\alpha_r = \pi_{r+1}(\alpha_{r+1}) = \sum_{j=k+1}^{m} \mu_j \pi_{r+1}(\hat{\mathcal{D}}_j)$. But $\pi_{r+1}(\mathcal{D}_j) \cap \mathcal{C} = \emptyset$ for all $j > k$, contradicting the fact that $\mathcal{C} \subseteq \mathrm{supp}(\alpha_\mathrm{r})$.

Hence, we can find $\mathcal{C}_{r+1} \in \mathcal{O}(A_{r+1})$ with $|\mathcal{C}_{r+1}| = |\mathcal{C}_r|$ and $\pi_{r+1}(\mathcal{C}_{r+1}) = \mathcal{C}_r$, where we set $\mathcal{C}_r$ to be $\mathcal{C}$. It's clear that we can continue this process of "lifting" the X-orbits, without ever increasing the sizes. Thus, we get a sequence

$$\cdots \overset{\pi_{n+2}}{\twoheadrightarrow} \mathcal{C}_{n+1} \overset{\pi_{n+1}}{\twoheadrightarrow} \mathcal{C}_n \overset{\pi_n}{\twoheadrightarrow} \ldots \overset{\pi_{r+1}}{\twoheadrightarrow} \mathcal{C}_r$$

of X-orbits, each having the same size as $\mathcal{C}_r$.

Now, pick some $s_r \in \mathcal{C}_r$ and inductively choose lifts $s_n \in \mathcal{C}_n$ for each $n \geq r$. Let s be the element of Y determined by these lifts. It's then clear that the X-orbit of s in Y is finite and that the image of this orbit in A_r equals $\mathcal{C}$. Let $\mathcal{F}_{\mathcal{C}}$ denote this element of $\mathcal{O}(Y)$.

Finally, we can consider the element $\beta = \sum_{\mathcal{C} \in \mathcal{O}(A_r)} \lambda_{\mathcal{C}} \hat{\mathcal{F}}_{\mathcal{C}}$. It's clear that $\beta \in \mathbb{F}_p[Y]^X$ and that the image of β in $\mathbb{F}_p[A_r]$ coincides with α_r. Hence, $\alpha - \beta$ has norm strictly smaller than that of α and also lies in Ω_Y^X. Applying the argument above to $\alpha - \beta$ instead of α and iterating, we see that α can be approximated arbitrarily closely by elements of $\mathbb{F}_p[Y]^X$. □

Corollary 4.1.2. *Let G be a pro-p group, $Z = Z(G)$ its centre. Then $Z(\Omega_G) = \overline{Z(\mathbb{F}_p[G])}$.*

Proof. Apply Proposition 4.1.1 to the G-space G, where G acts on itself by conjugation. □

Corollary 4.1.3. *Let G be a uniform pro-p group with centre $Z = Z(G)$. Then $Z(\Omega_G) = \Omega_Z$ and $Z(\Lambda_G) = \Lambda_Z$.*

Proof. $Z(\mathbb{F}_p[G])$ is spanned over $\mathbb{F}_p$ by all conjugacy class sums $\hat{\mathcal{C}}$, where $\mathcal{C}$ is a *finite* conjugacy class of G. Let $\mathcal{C}$ be such a conjugacy class and let $x \in \mathcal{C}$. Then $C_G(x)$ is a closed subgroup of finite index in G, so there exists $n \in \mathbb{N}$ such that $G_{n+1} \subseteq C_G(x)$. Here G_n denotes the n-th element of the lower p-series of G; see Definition 2.5.5.

Let $y \in G$; then $y^{p^n} \in C_G(x)$ so $(x^{-1}yx)^{p^n} = y^{p^n}$. Since G is uniform, $x^{-1}yx = y$ by Proposition 2.5.6 (iii) and hence $x \in Z$. It follows that $Z(\mathbb{F}_p[G]) = \mathbb{F}_p[Z]$; since the subspace filtration on Ω_Z induced from the J_G-adic filtration on Ω_G coincides with the J_Z-adic filtration by Corollary 2.7.3,

$$Z(\Omega_G) = \overline{Z(\mathbb{F}_p[G])} = \overline{\mathbb{F}_p[Z]} = \Omega_Z,$$

in view of Corollary 4.1.2.

It's clear that $\Lambda_Z \subseteq Z(\Lambda_G)$; a simple completeness argument establishes the reverse inclusion. $\square$

We remark that when G is an open pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, the above result was proved by Howson ([14], 4.2) using similar methods.

4.2 Endomorphism rings of induced modules

Let $G = \varprojlim G/G_n$ be a pro-p group, H a closed subgroup. Let $M = \mathbb{F}_p \otimes_{\Omega_H} \Omega_G$ be the induced module from the trivial module for Ω_H. G acts on the coset space $Y = H\backslash G$ by right translation and we can write $Y = \varprojlim HG_n\backslash G$ as an inverse limit of finite G-spaces. It's easy to see that Ω_Y is then naturally isomorphic to M.

Let R denote the endomorphism ring $\mathrm{End}_{\Omega_G} M$ of M. By Frobenius Reciprocity,

$$R = \mathrm{Hom}_{\Omega_G}(\mathbb{F}_p \otimes_{\Omega_H} \Omega_G, M) \cong \mathrm{Hom}_{\Omega_H}(\mathbb{F}_p, M),$$

and we see that each element of R gives rise to a trivial submodule of M, viewed as an Ω_H-module.

It's clear that the sum of all trivial Ω_H-submodules of M is precisely the set Ω_Y^H, where H acts on Y by right translation; moreover the finite H-orbits on Y are given by the double cosets of H in G which are finite unions of left cosets of H.

Suppose HxH is such a double coset; then $\mathrm{Stab}_H(Hx) = \{h \in H : Hxh = Hx\} = H \cap H^x$, so the set $\mathcal{N}_G(H) = \{x \in G : H \cap H^x \leq_o H\}$ is of interest; we observe that it contains the usual normalizer $N_G(H)$ of H in G. This set is also sometimes called the *commensurator* of H in G.

Now we restrict our attention to uniform pro-p groups G. Let H be a closed subgroup and write $\mathfrak{g} = \mathcal{L}(G)$ and $\mathfrak{h} = \mathcal{L}(H)$ for the $\mathbb{Q}_p$-Lie algebras of G and H, respectively.

We observe that

$$H \cap H^x \leq_o H \Leftrightarrow \mathcal{L}(H \cap H^x) = \mathcal{L}(H) \cap \mathcal{L}(H)^x = \mathcal{L}(H) \Leftrightarrow \mathcal{L}(H)^x = \mathcal{L}(H),$$

and so $\mathcal{N}_G(H) = \mathrm{Stab}_G \mathfrak{h}$ *is* a (closed) subgroup of G in this case. Here we are letting G act by conjugation on its Lie algebra. By Exercise 9.10 of [11], we see that the Lie algebra of $\mathcal{N}_G(H)$ is equal to the normalizer $N_{\mathfrak{g}}(\mathfrak{h})$ of $\mathfrak{h}$ in $\mathfrak{g}$. We remark in passing that this implies that $N_G(H)$ has finite index in $\mathcal{N}_G(H)$ when dealing with uniform pro-p groups; this isn't true in general.

Theorem 4.2.1. *Let G be a uniform pro-p group and H a closed subgroup with $\mathbb{Q}_p$-Lie algebras $\mathfrak{g} = \mathcal{L}(G)$ and $\mathfrak{h} = \mathcal{L}(H)$, respectively. Then the endomorphism ring* $\mathrm{End}_{\Omega_G}(M)$ *of the induced module $M = \mathbb{F}_p \otimes_{\Omega_H} \Omega_G$ is finite dimensional over $\mathbb{F}_p$ if and only if $N_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$.*

Proof. Suppose $N_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$. As $H \leq \mathcal{N}_G(H)$ and because $\mathcal{L}(H) = \mathfrak{h} = N_{\mathfrak{g}}(\mathfrak{h}) = \mathcal{L}(\mathcal{N}_G(H))$ by the above remarks, it follows that H has finite index in $\mathcal{N}_G(H)$. Since any double coset HxH which is a finite union of left cosets of H is contained in $\mathcal{N}_G(H)$, we see that there are only finitely many such double cosets (because H has finite index in $\mathcal{N}_G(H)$). This means that the number of finite H-orbits on $Y = H\backslash G$ is finite, and so $\mathrm{End}_{\Omega_G}(M)$ is finite dimensional over $\mathbb{F}_p$, in view of the preceding remarks and Proposition 4.1.1.

Now suppose $N_{\mathfrak{g}}(\mathfrak{h}) > \mathfrak{h}$; because the usual normalizer $N_G(H)$ also has Lie algebra $N_{\mathfrak{g}}(\mathfrak{h})$, we see that H must have infinite index in $N_G(H)$. But now each double coset HxH with $x \in N_G(H)$ is actually a single left coset Hx and gives rise to a trivial Ω_H-submodule $\mathbb{F}_p.Hx$ of M. Hence the sum of all trivial Ω_H-submodules of M is infinite dimensional over $\mathbb{F}_p$ and hence so is $\operatorname{End}_{\Omega_G}(M)$. □

4.3 Endomorphism rings of 1-critical modules

When the Lie algebra of a uniform pro-p group H is split semisimple, we are able to obtain information about the endomorphism ring of any finitely generated 1-critical Ω_H-module. The main result of this section is

Theorem 4.3.1. *Let H be a uniform pro-p group such that $\mathcal{L}(H)$ is split semisimple over $\mathbb{Q}_p$. Let M be a finitely generated 1-critical Ω_H-module and let $R = \operatorname{End}_{\Omega_H}(M)$. Then R is a finite field extension of $\mathbb{F}_p$. Moreover, if M is cyclic over Ω_H, $R \cong \mathbb{F}_p$.*

We begin with a very useful primality result. Recall that a two-sided ideal I of a (not necessarily commutative) ring R is said to be *prime* if whenever A, B are two-sided ideals of R strictly containing I, AB also strictly contains I.

Proposition 4.3.2. *Let k be a field and let R be a local Noetherian k-algebra such that $R/J(R) \cong k$. Suppose M is a finitely generated Krull 1-critical R-module. Then the global annihilator $I = \operatorname{Ann}_R(M)$ of M is prime.*

Proof. Here $J = J(R)$ denotes the Jacobson radical of R.

Let $S = \{\mathrm{Ann}_R(T) : 0 \neq T \lhd M\}$. Since R is right Noetherian, S has a maximal element $Y = \mathrm{Ann}_R(N)$ say, for some nonzero submodule N of M. It's clear that as $MI = 0$, $I \subseteq Y$.

We claim that Y is prime. If this is false, we can find ideals A and B of R such that $Y \subsetneq A$ and $Y \subsetneq B$ but $AB \subseteq Y$. Now $NA \neq 0$ since $Y = \mathrm{Ann}_R(N)$ and $Y \subsetneq A$; thus $\mathrm{Ann}_R(NA) \in S$. But $NAB = 0$ so $Y \subsetneq B \subseteq \mathrm{Ann}_R(NA)$, contradicting the maximality of Y.

Now, N is a nonzero submodule of the 1-critical module M, so M/N is Artinian. Since R is local with unique simple module k, $M.J^n \subseteq N$ for some integer n. Hence $MJ^nY = 0$, so $J^nY \subseteq I$. Hence the left module Y/I is Artinian. Because R is a k-algebra with unique simple module k, Y/I is finite dimensional over k. Hence Y/I must be Artinian as a right R-module and so $YJ^m \subseteq I$ for some integer m. It follows that $MYJ^m \subseteq MI = 0$ and so MY is Artinian, being a finitely generated right module over the Artinian ring R/J^m. Because M is 1-critical, $MY = 0$ and so $Y = I$ is prime. □

Note that the condition that R is local cannot be removed from the statement of this result, as Theorem 4.2 of [3] shows.

The main step comes next.

Proposition 4.3.3. *Let $\mathfrak{h}$ be a split semi-simple Lie algebra over $\mathbb{Q}_p$. Let $\mathfrak{h} = \mathfrak{h}_1 \times \mathfrak{h}_2 \times \ldots \times \mathfrak{h}_n$ be a decomposition of $\mathfrak{h}$ into simple ideals. Let $H_1, H_2, \ldots, H_n$ be uniform pro-p groups with $\mathbb{Q}_p$-Lie algebras $\mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_n$. Set $H = H_1 \times H_2 \times \ldots \times H_n$ and $G = H \times Z$ where $Z = \overline{<\theta>} \cong \mathbb{Z}_p$. Write $z = \theta - 1 \in \Omega_G$. Let M be a finitely generated 1-critical Ω_G-module. Then either* *(i)* $M.z = 0$, *or*

(ii) $M \cong \mathbb{F}_p \otimes_{\Omega_H} \Omega_G$.

Proof. Note that as $\theta \in Z(G)$, z acts by Ω_G-module endomorphisms on M.

As M is 1-critical, any non-zero endomorphism of M must be an injection ([23], 6.2.3). Assume that $M.z \neq 0$; then z acts injectively on M.

Let $A = \mathbb{F}_p[[z]] \subseteq Z(\Omega_G)$. Now, as M is 1-critical and $M.z \neq 0$, $M/M.z$ is finite dimensional over $\mathbb{F}_p$. Because z acts injectively on M, $M.z^n/M.z^{n+1} \cong M/M.z$ for all $n \geq 1$, which means that the graded module of M with respect to the z-adic filtration is finitely generated over $\operatorname{gr} A \cong \mathbb{F}_p[t]$.

As M is a finitely generated module over Ω_G, M is complete with respect to the J_G-adic filtration; in particular, $\cap_{n=0}^{\infty} M.J_G^n = 0$. Hence $\cap_{n=0}^{\infty} M.z^n = 0$, so the z-adic filtration on M is separated.

Because A is complete with respect to the z-adic filtration, M is finitely generated over A, by Theorem 2.2.5. Also, z acts injectively on M, so $A \hookrightarrow \operatorname{End}_A(M)$. These facts mean that $\operatorname{End}_A(M)$ is finitely generated as a module over A, a commutative subring. It follows from Corollary 13.1.13(iii) of [23] that $\operatorname{End}_A(M)$ is a PI ring.

Fix $i = 1 \ldots n$. As $\mathfrak{h}_i$ is split and simple over $\mathbb{Q}_p$, we can find a subalgebra $\mathfrak{b}$ which is isomorphic to the two-dimensional non-abelian Lie algebra over $\mathbb{Q}_p$. Let B be the corresponding isolated uniform subgroup of H; thus $B = X \ltimes Y \cong \mathbb{Z}_p \ltimes \mathbb{Z}_p$, say.

Because the centre of $\mathfrak{b}$ is trivial, so is the centre of B. It follows that $Z(\Omega_B) = \Omega_{\{1\}} = \mathbb{F}_p$, by Corollary 4.1.3. Hence $\Omega_B.S^{-1} \cong \Omega_B$, where $S = Z(\Omega_B) - \{0\}$.

Let $P = \mathrm{Ann}_{\Omega_G}(M)$ and suppose that $P \cap \Omega_B = 0$. Then $\Omega_B \hookrightarrow \mathrm{End}_A(M)$. It follows that Ω_B is a prime PI-ring. By Posner's Theorem ([23], 13.6.5), $\Omega_B.S^{-1} \cong \Omega_B$ is a central simple algebra. This contradicts the fact that J_B is a non-trivial two-sided ideal of Ω_B. Hence $P \cap \Omega_B \neq 0$.

Now, by a result of Venjakob (Theorem 7.1 of [24]), the only nonzero prime ideals of Ω_B are $y.\Omega_B$ and J_B where $\Omega_Y \cong \mathbb{F}_p[[y]]$. The nonzero two-sided ideal $P \cap \Omega_B$ of Ω_B contains a product of nonzero prime ideals as Ω_B is Noetherian. Since $y \in J_B$, we see that $y^{p^k} \in P$ for some $k \geq 1$ and hence $(1+P) \cap Y \neq 1$.

But $(1+P) \cap H_i$ is then a nontrivial normal subgroup of H_i; since $\mathfrak{h}_i$ is simple, $(1+P) \cap H_i$ is an open subgroup of H_i. Hence $P_{j_i}(H_i) \subseteq 1+P$ for some $j_i \geq 1$ for each $i = 1 \dots n$; see Definition 2.5.5 for the relevant notation. Without loss of generality $j_i = j$ for all i, whence $P_j(H_1) \times P_j(H_2) \times \ldots \times P_j(H_n) = P_j(H) \subseteq 1 + P$ and so $J_H^m \subseteq P$ for some $m \geq 1$.

Let $Q = \ker(\Omega_G \twoheadrightarrow A)$. Then it's easy to see that $Q = J_H.\Omega_G = \Omega_G.J_H$, so $Q^m = (J_H.\Omega_G)^m \subseteq P$. By Theorem 4.3.2, P is prime, so $Q \subseteq P$.

Hence $A \cong \mathbb{F}_p \otimes_{\Omega_H} \Omega_G \twoheadrightarrow \Omega_G/P \twoheadrightarrow M$; since A is itself a 1-critical Ω_G-module, we must have $A \cong M$, so (ii) holds. □

Proof of Theorem 4.3.1. Let G and $z \in \Omega_G$ be as in Proposition 4.3.3; it's clear from Theorem 2.7.2(ii) that $\Omega_G \cong \Omega_H[[z]]$.

Let $\varphi \in \mathrm{Hom}_{\Omega_H}(M, MJ)$, where $J = J_H$. Then we can make M into an Ω_G-module by setting

$$m.\sum_{n=0}^{\infty} r_n z^n = \sum_{n=0}^{\infty} \varphi^n(m).r_n.$$

The right hand side of this expression makes sense because $\varphi(M) \subseteq MJ$, so $\varphi^n(M) \subseteq MJ^n$ for all n. It's clear that this defines an action of Ω_G on M which extends the action of Ω_H and such that z acts as φ. It's easy to check that M must be 1-critical as an Ω_G-module.

By Proposition 4.3.3, either $M.z = 0$ (so $\varphi = 0$), or $M \cong \mathbb{F}_p \otimes_{\Omega_H} \Omega_G$, in which case $M.J_H = 0$. As M is finitely generated over Ω_H, the latter case forces M to be finite dimensional over $\mathbb{F}_p$, contradicting the 1-criticality of M. Hence $\varphi = 0$, and therefore $\mathrm{Hom}_{\Omega_H}(M, MJ) = 0$.

Now, as MJ is a characteristic Ω_H-submodule of M, we have the exact sequence

$$0 \to \mathrm{Hom}_{\Omega_H}(M, MJ) \to \mathrm{Hom}_{\Omega_H}(M, M) \to \mathrm{Hom}_{\Omega_H}(M/MJ, M/MJ)$$

which shows that R embeds into $\mathrm{End}_{\mathbb{F}_p}(M/MJ)$, which is finite dimensional over $\mathbb{F}_p$. Note that if M is cyclic, $R \cong \mathbb{F}_p$ because $M/MJ \cong \mathbb{F}_p$.

Now, as M is critical, any nonzero endomorphism of M is an injection. This means that R is a domain, and is hence a finite division ring. By Wedderburn's Theorem, R is a finite field extension of $\mathbb{F}_p$. □

4.4 Annihilators of 1-critical modules

Theorem 4.4.1. *Let G be a uniform pro-p group with split semisimple Lie algebra $\mathcal{L}(G)$. Let M be a finitely generated 1-critical Ω_G-module and write $I = \mathrm{Ann}_{\Omega_G}(M)$. Then $\mathcal{K}(\Omega_G/I) \geq 2$.*

Proof. Let $R = \Omega_G$. The proof of Proposition 4.3.2 shows that $\mathrm{Ann}_R(N) = I$ for any nonzero submodule N of M. Without loss of generality, we may assume that $M = R/L$ is cyclic; thus, $I \subseteq L \lhd_r R$. Let $\bar{}$ denote the natural projection of R onto R/I. Note that $\bar{R}$ is a prime ring, by Proposition 4.3.2.

Since $\bar{R} \twoheadrightarrow M$ and $\mathcal{K}(M) = 1$, $\mathcal{K}(\bar{R}) \geq 1$ and so $\bar{R}$ is infinite dimensional over $\mathbb{F}_p$, by Proposition 3.2.3.

Let Q be the quotient ring of $\bar{R}$; by Goldie's Theorem ([23]2.3.6) we know that Q is simple Artinian, because $\bar{R}$ is prime Noetherian. Say $Q \cong M_n(D)$ for some division ring D and integer $n \geq 1$. Here $D = \mathrm{End}_Q(V)$ where V is the unique simple Q-module. In what follows, we use the fact that Q is a flat $\bar{R}$-module.

Suppose $\bar{L}Q < \bar{R}Q$, i.e. $MQ \neq 0$. Since M is finitely generated over $\bar{R}$, MQ is finitely generated over Q and is hence isomorphic to a direct sum of k copies of V for some integer $k > 0$. Hence $\mathrm{End}_Q(MQ) \cong M_k(D)$.

Let N be the torsion submodule of M with respect to $\mathcal{C}_{\bar{R}}(0)$ (the set of regular elements of $\bar{R}$), so that M/N is torsionfree with respect to $\mathcal{C}_{\bar{R}}(0)$ and $(M/N)Q \cong MQ$. Now if $N \neq 0$, M/N is finite dimensional over $\mathbb{F}_p$ (because M is 1-critical) and so $\mathrm{End}_R(M/N)$ must also be finite dimensional over $\mathbb{F}_p$; if $N = 0$, $\mathrm{End}_R(M/N)$ is finite dimensional over $\mathbb{F}_p$ by Theorem 4.3.1.

As M/N is finitely generated over $\bar{R}$, torsionfree with respect to $\mathcal{C}_{\bar{R}}(0)$ and as $\bar{R}$ is prime Goldie, M/N is torsionless, by Theorem 3.4.7 of [23]. Hence by Theorem 3.4.6 of [23], $\mathrm{End}_R(M/N)$ is a right order in $\mathrm{End}_Q((M/N)Q) = \mathrm{End}_Q(MQ) \cong M_k(D)$, so $M_k(D)$ and hence $Q \cong M_n(D)$ must be finite dimensional over $\mathbb{F}_p$.

This is impossible as $\bar{R} \hookrightarrow Q$ with $\bar{R}$ infinite dimensional over $\mathbb{F}_p$. So in fact $MQ = 0$ and hence $\bar{L}$ must contain a regular element $\bar{x}$ of $\bar{R}$. Now we get a chain

$$\bar{R} > \bar{x}\bar{R} > \bar{x}^2\bar{R} > \ldots > \bar{0}$$

of right ideals of $\bar{R}$ with each quotient isomorphic to $\bar{R}/\bar{x}\bar{R}$, because $\bar{x}$ is regular in $\bar{R}$. Hence $\mathcal{K}(R/I) = \mathcal{K}(\bar{R}) \geq \mathcal{K}(\bar{R}/\bar{x}\bar{R}) + 1 \geq \mathcal{K}(R/L) + 1 = 2$, as required. □

Chapter 5

A deformation of Λ_G

5.1 Completed universal enveloping algebras

Whenever k is a commutative ring and $\mathfrak{g}$ is a k-Lie algebra, we will write $\mathcal{U}(\mathfrak{g})$ for the universal enveloping algebra of $\mathfrak{g}$ over k. For more information about these objects, see [10].

We begin with a definition.

Definition 5.1.1. *Let $\mathfrak{g}$ be a $\mathbb{Z}_p$-Lie algebra. The* completed universal enveloping algebra *of $\mathfrak{g}$ is defined to be the completion of $\mathcal{U}(\mathfrak{g})$ with respect to the p-adic filtration:*

$$\Pi_{\mathfrak{g}} := \lim_{\longleftarrow} \frac{\mathcal{U}(\mathfrak{g})}{p^n \mathcal{U}(\mathfrak{g})}.$$

We will only consider the case when $\mathfrak{g}$ is free of finite rank d over $\mathbb{Z}_p$. Some algebraic properties of $\Pi_{\mathfrak{g}}$ are recorded below.

Proposition 5.1.2. *Let $\mathfrak{g}$ be a $\mathbb{Z}_p$-Lie algebra, free of finite rank d over $\mathbb{Z}_p$, and let $\overline{\mathfrak{g}} = \mathfrak{g}/p\mathfrak{g}$. Equip $\Pi_{\mathfrak{g}}$ with the p-adic filtration. Then:*

(i) $\operatorname{gr} \Pi_{\mathfrak{g}} \cong \mathcal{U}(\overline{\mathfrak{g}})[s]$.

(ii) $\Pi_{\mathfrak{g}}$ *is a Noetherian integral domain with global and Krull dimensions bounded above by $d+1$. If $\overline{\mathfrak{g}}$ is restricted, both dimensions are equal to $d+1$.*

Proof. (i) Let $U = \mathcal{U}(\mathfrak{g})$. By Lemma 2.1.7,

$$\operatorname{gr} \Pi_{\mathfrak{g}} = \operatorname{gr} U = \bigoplus_{n=0}^{\infty} p^n U / p^{n+1} U.$$

Letting $s = p + p^2 U \in \operatorname{gr} U$, we see that

$$\operatorname{gr} U = (U/pU)[s] \cong \mathcal{U}(\overline{\mathfrak{g}})[s].$$

(ii) $\Pi_{\mathfrak{g}}$ is complete with respect to the p-adic filtration. The associated graded ring $\operatorname{gr} \Pi_{\mathfrak{g}} \cong \mathcal{U}(\overline{\mathfrak{g}})[s]$ is a Noetherian integral domain, so is $\Pi_{\mathfrak{g}}$ is a Noetherian integral domain as well.

Now, p is a central regular element of $J(\Pi_{\mathfrak{g}})$ and $\Pi_{\mathfrak{g}}/p\Pi_{\mathfrak{g}} \cong \mathcal{U}(\overline{\mathfrak{g}})$. Hence $\mathcal{K}(\Pi_{\mathfrak{g}}) = \mathcal{K}(\mathcal{U}(\overline{\mathfrak{g}})) + 1$ and $\operatorname{gld}(\Pi_{\mathfrak{g}}) = \operatorname{gld}(\mathcal{U}(\overline{\mathfrak{g}})) + 1$, by Theorem 3.1.1 and Theorem 7.3.7 of [23].

Next, $\mathcal{K}(\mathcal{U}(\overline{\mathfrak{g}})) \leq d$ by Corollary 6.5.7 of [23] and $\operatorname{gld}(\mathcal{U}(\overline{\mathfrak{g}})) \leq d$ by Corollary 7.6.19 of [23], giving the required general upper bounds.

Finally, suppose $\overline{\mathfrak{g}}$ is restricted. By Proposition 2.9.4, $\mathcal{U}(\overline{\mathfrak{g}})$ is a free and finitely generated module over $\mathcal{O}$, a polynomial ring in d variables. The result follows from Corollary 6.5.3 and Theorem 7.2.6 of [23]. □

Next, we single out some analytic properties of $\Pi_{\mathfrak{g}}$.

Proposition 5.1.3. *Let $\mathfrak{g}$ be a $\mathbb{Z}_p$-Lie algebra, free of finite rank with basis $\{u_1, \ldots, u_d\}$. Let $\mathbf{u}^\alpha = u_1^{\alpha_1} \ldots u_d^{\alpha_d} \in \Pi_{\mathfrak{g}}$ for $\alpha \in \mathbb{N}^d$. Then*

(i) Every element of $\Pi_{\mathfrak{g}}$ is equal to the sum of a uniquely determined convergent power series

$$\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha,$$

where $\lambda_\alpha \in \mathbb{Z}_p$ and $\lambda_\alpha \to 0$ as $|\alpha| = \alpha_1 + \ldots + \alpha_d \to \infty$.

(ii) Let $||.||$ be the p-adic norm on $\Pi_{\mathfrak{g}}$, defined by $||x|| = p^{-n}$ if $x \in p^n \Pi_{\mathfrak{g}} \backslash p^{n+1} \Pi_{\mathfrak{g}}$ and $||0|| = 0$. Then

$$||x|| = \sup\{|\lambda_\alpha| : \alpha \in \mathbb{N}^d\} \quad \textit{if} \quad x = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha \in \Pi_{\mathfrak{g}}.$$

Proof. (i) Let $U = \mathcal{U}(\mathfrak{g})$. By the Poincare-Birkhoff-Witt Theorem ([10], 2.1.11), every element of U can be written uniquely as a finite sum $x = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha$, where $\lambda_\alpha \in \mathbb{Z}_p$ and $\lambda_\alpha = 0$ whenever $|\alpha|$ is large.

Note that $x \in p^n U \Leftrightarrow \lambda_\alpha \in p^n \mathbb{Z}_p$ for all $\alpha \in \mathbb{N}^d \Leftrightarrow \sup\{|\lambda_\alpha| : \alpha \in \mathbb{N}^d\} \leq p^{-n}$. This shows that $||x|| = \sup\{|\lambda_\alpha| : \alpha \in \mathbb{N}^d\}$ for all $x \in U$.

Let $\lambda \in \mathbb{Z}_p^{\mathbb{N}^d}$. By Proposition 6.9(ii) of [11], the series $\sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha$ converges to an element of $\Pi_{\mathfrak{g}}$ if and only if $||\lambda_\alpha \mathbf{u}^\alpha|| = |\lambda_\alpha| \to 0$ as $|\alpha| \to \infty$. Letting $l_0(\mathbb{Z}_p) = \{\lambda \in \mathbb{Z}_p^{\mathbb{N}^d} : \lambda_\alpha \to 0$ as $|\alpha| \to \infty\}$, we get a $\mathbb{Z}_p$-linear map $\varphi : l_0(\mathbb{Z}_p) \to \Pi_{\mathfrak{g}}$, such that

$$\varphi(\lambda) = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha.$$

It will be sufficient to show that φ is a bijection.

If $\varphi(\lambda) = 0$, $||\sum_{|\alpha|\leq k} \lambda_\alpha \mathbf{u}^\alpha|| \to 0$ as $k \to \infty$. But $||\sum_{|\alpha|\leq k} \lambda_\alpha \mathbf{u}^\alpha|| = \sup\{|\lambda_\alpha| : |\alpha| \leq k\}$, so $\lambda_\alpha = 0$ for all $\alpha \in \mathbb{N}^d$. Hence φ is an injection.

Let $x \in \Pi_{\mathfrak{g}}$. We may write x as a convergent series $x = \sum_{i=0}^\infty p^i y_i$ for some $y_i \in U$. Write $y_i = \sum_{\alpha\in\mathbb{N}^d} \lambda_\alpha^{(i)} \mathbf{u}^\alpha$ where $\lambda_\alpha^{(i)} = 0$ whenever $|\alpha| > N_i$, for some $N_i \in \mathbb{N}$. Let $\lambda_\alpha = \sum_{i=0}^\infty p^i \lambda_\alpha^{(i)} \in \mathbb{Z}_p$; we check that $\lambda_\alpha \to 0$ as $|\alpha| \to \infty$. If $k \geq 0$, let $N = \max_{0\leq i\leq k} N_i$. Then whenever $|\alpha| > N$, $\lambda_\alpha^{(i)} = 0$ for $i = 0, \ldots, k$ whence $\lambda_\alpha = \sum_{i=k+1}^\infty p^i \lambda_\alpha^{(i)} \in p^{k+1}\mathbb{Z}_p$, as required.

Now, consider the double series

$$\sum_{(i,\alpha)\in\mathbb{N}^{d+1}} p^i \lambda_\alpha^{(i)} \mathbf{u}^\alpha.$$

If $k \in \mathbb{N}$, let $T_k = \cup_{i=0}^k \{(i,\alpha) : |\alpha| \leq N_i\}$; this is a finite subset of $\mathbb{N}^{d+1}$. If $(i,\alpha) \notin T_k$, then $||p^i \lambda_\alpha^{(i)} \mathbf{u}^\alpha|| < p^{-k}$. This shows that $p^i \lambda_\alpha^{(i)} \mathbf{u}^\alpha \to 0$ as $(i,\alpha) \to \infty$. By Corollary 6.11 of [11], the double series converges to an element of $\Pi_{\mathfrak{g}}$ and equals

$$x = \sum_{i=0}^\infty p^i (\sum_{\alpha\in\mathbb{N}^d} \lambda_\alpha^{(i)} \mathbf{u}^\alpha) = \sum_{\alpha\in\mathbb{N}^d} (\sum_{i=0}^\infty p^i \lambda_\alpha^{(i)}) \mathbf{u}^\alpha = \sum_{\alpha\in\mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha = \varphi(\lambda),$$

so φ is onto.

(ii) The required formula for $||x||$ was shown to hold when $x \in U$ in part (i). The result follows by continuity of norm. □

We may extend the norm on $\Pi_{\mathfrak{g}}$ to the central localization $\mathbb{Q}_p\Pi_{\mathfrak{g}} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Pi_{\mathfrak{g}}$ of $\Pi_{\mathfrak{g}}$ by setting

$$||\mu \otimes x|| = |\mu|.||x||$$

for $\mu \in \mathbb{Q}_p$ and $x \in \Pi_\mathfrak{g}$; this is well-defined by part (ii) of Proposition 5.1.3. It's easy to check that this turns $\mathbb{Q}_p\Pi_\mathfrak{g}$ into a normed $\mathbb{Q}_p$-algebra, in the sense of Chapter 6 of [11].

Now, let G be a uniform pro-p group. We recall the construction of the norm on $\mathbb{Q}_p\Lambda_G = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda_G$ carried out in Chapter 7 of [11]. This norm is given by $||x|| = p^{-n}$ when $x \in J^n \backslash J^{n+1}$ and $||\lambda x|| = |\lambda| ||x||$ when $\lambda \in \mathbb{Q}_p$ and $x \in \Lambda_G$. Here J denotes the maximal ideal of Λ_G. We will denote the completion $\mathbb{Q}_p[[G]]$ of $\mathbb{Q}_p\Lambda_G$ with respect to this norm by Σ_G.

Theorem 5.1.4. *Let p be odd, let G be a uniform pro-p group with $\mathbb{Z}_p$-Lie algebra L_G and let $\mathfrak{g} = p^{-1}L_G$. Then Σ_G is isometrically isomorphic to $\mathbb{Q}_p\Pi_\mathfrak{g}$ as a normed $\mathbb{Q}_p$-algebra.*

Proof. Here $\mathfrak{g}$ is the $\mathbb{Z}_p$-submodule of $\mathcal{L}(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_G$ given by $\mathfrak{g} = \{p^{-1} \otimes x \in \mathcal{L}(G) : x \in L_G\}$. We note that as L_G is powerful, $[\mathfrak{g}, \mathfrak{g}] \subseteq p^{-2}pL_G = \mathfrak{g}$, i.e. $\mathfrak{g}$ *is* a $\mathbb{Z}_p$-Lie algebra.

Choose a topological generating set $\{a_1, \ldots, a_d\}$ for G, let $b_i = a_i - 1 \in \Sigma_G$ and let $u_i = p^{-1} \otimes a_i \in \mathfrak{g}$, so that $\{u_1, \ldots, u_d\}$ is a $\mathbb{Z}_p$-basis for $\mathfrak{g}$. Write $\mathbf{u}^\alpha = u_1^{\alpha_1} \ldots u_d^{\alpha_d}$ and $\mathbf{b}^\alpha = b_1^{\alpha_1} \ldots b_d^{\alpha_d}$ for $\alpha \in \mathbb{N}^d$.

By Theorem 7.13 and Corollary 7.14 of [11], we have an injection $\log : L_G \to \Sigma_G$ of $\mathbb{Z}_p$-Lie algebras, given by

$$\log(a_i) = b_i - b_i^2/2 + b_i^3/3 - \cdots \in \Sigma_G.$$

This extends to an injection of $\mathbb{Z}_p$-Lie algebras $\beta : \mathfrak{g} \to \Sigma_G$ and to a $\mathbb{Z}_p$-algebra homomorphism $\beta : U \to \Sigma_G$, where $U = \mathcal{U}(\mathfrak{g})$. The action of β on basis elements of U is given by

$$\beta(\mathbf{u}^\alpha) = p^{-|\alpha|}(b_1 - b_1^2/2 + \cdots)^{\alpha_1} \dots (b_d - b_d^2/2 + \cdots)^{\alpha_d} = p^{-|\alpha|}\mathbf{b}^\alpha + \epsilon_\alpha$$

for some $\epsilon_\alpha \in \Sigma_G$ with $||\epsilon_\alpha|| < 1$. It follows that if $x = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha \in U$ (finite sum) then

$$\beta(x) = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha p^{-|\alpha|}\mathbf{b}^\alpha + \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \epsilon_\alpha.$$

Now $|| \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \epsilon_\alpha|| < \sup\{|\lambda_\alpha| : \alpha \in \mathbb{N}^d\} = || \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha p^{-|\alpha|}\mathbf{b}^\alpha||$, using Theorem 7.5 of [11]. Hence $||\beta(x)|| = \sup\{|\lambda_\alpha| : \alpha \in \mathbb{N}^d\} = ||x||$ for all $x \in U$, using part (ii) of Proposition 5.1.3. It follows that $\beta : U \to \Sigma_G$ is an isometry and hence extends to a isometric $\mathbb{Z}_p$-algebra homomorphism $\beta : \Pi_{\mathfrak{g}} \hookrightarrow \Sigma_G$. Tensoring with $\mathbb{Q}_p$ gives an isometric embedding $\beta : \mathbb{Q}_p\Pi_{\mathfrak{g}} \hookrightarrow \Sigma_G$ of normed $\mathbb{Q}_p$-algebras.

Let $l_0(\mathbb{Q}_p) = \{\lambda \in \mathbb{Q}_p^{\mathbb{N}^d} : \lambda_\alpha \to 0 \text{ as } |\alpha| \to \infty\}$ and let $||\lambda|| = \sup_{\alpha \in \mathbb{N}^d} |\lambda_\alpha|$ be the sup norm on $l_0(\mathbb{Q}_p)$. Standard arguments from functional analysis show that $l_0(\mathbb{Q}_p)$ is a *complete* normed $\mathbb{Q}_p$-vector space. Note that since any convergent sequence in $\mathbb{Q}_p$ is bounded, $l_0(\mathbb{Q}_p) = l_0(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

The map $\varphi : l_0(\mathbb{Q}_p) \to \mathbb{Q}_p\Pi_{\mathfrak{g}}$ given by $\varphi(\lambda) = \sum_{\alpha \in \mathbb{N}^d} \lambda_\alpha \mathbf{u}^\alpha$ is an isometric isomorphism, by Proposition 5.1.3. Hence $\mathbb{Q}_p\Pi_{\mathfrak{g}}$ is a complete normed $\mathbb{Q}_p$-algebra.

Now, since $||pu_i|| < 1$ and p is odd, the exponential series $\exp(pu_i)$ converges in $\mathbb{Q}_p\Pi_{\mathfrak{g}}$, by Proposition 6.22 of [11]. Because β is continuous,

$$\beta(\exp(pu_i) - 1) = \exp(\beta(pu_i)) - 1 = \exp(\log(a_i)) - 1 = b_i,$$

so the $\mathbb{Q}_p$-vector subspace V of Σ_G spanned by $\{\mathbf{b}^\alpha : \alpha \in \mathbb{N}^d\}$ is contained in $\mathrm{Im}\beta$. Now, $\mathrm{Im}\beta$ is closed since $\mathbb{Q}_p\Pi_{\mathfrak{g}}$ is complete and β is continuous. But V is dense in Σ_G, whence β is onto. □

Note that in the above proof, β gives an isomorphism of $\Pi_{\mathfrak{g}}$ and the valuation subring $\{x \in \Sigma_G : ||x|| \leq 1\}$ of Σ_G. Since $||x|| \leq 1$ for all $x \in \Lambda_G$, we see that β^{-1} gives an injection of Λ_G into $\Pi_{\mathfrak{g}}$.

Let $\widetilde{\Lambda_G}$ denote the Rees ring of Λ_G with respect to the J-adic filtration:

$$\widetilde{\Lambda_G} = \bigoplus_{n \leq -1} J^{-n}t^n \oplus \Lambda_G[t].$$

The following result shows that we can view $\Pi_{\mathfrak{g}}$ as a deformation of Λ_G.

Proposition 5.1.5. *Let p, G and $\mathfrak{g}$ be as in Theorem 5.1.4. Then $\Pi_{\mathfrak{g}}$ is isomorphic to the p-adic completion of $\widetilde{\Lambda_G}/(pt^{-1}-1)\widetilde{\Lambda_G}$.*

Proof. Since p is invertible in Σ_G, the embedding of Λ_G into Σ_G extends to a ring homomorphism $\gamma : \Lambda_G[t, t^{-1}] \to \Sigma_G$ sending t to p. Now,

$$\gamma(\widetilde{\Lambda_G}) = \sum_{n \leq 0} J^{-n}p^n = \bigcup_{n \geq 0} J^n p^{-n} = \{x \in \mathbb{Q}_p\Lambda_G : \|x\| \leq 1\},$$

because $p \in J$ forces $J^n p^{-n} = J^n p p^{-n-1} \subseteq J^{n+1}p^{-(n+1)}$ for all $n \geq 0$. It follows that $\gamma(\widetilde{\Lambda_G})$ is dense in the valuation subring $\{x \in \Sigma_G : \|x\| \leq 1\}$ of Σ_G, which is isomorphic to $\Pi_{\mathfrak{g}}$ by Theorem 5.1.4.

It now remains to show that $\ker\gamma \cap \widetilde{\Lambda_G} = (pt^{-1}-1)\widetilde{\Lambda_G}$. Since $pt^{-1}-1 \in \widetilde{\Lambda_G}$ and $\gamma(pt^{-1}-1) = 0$, it is sufficient to prove the forward inclusion.

It's easy to see that $\ker\gamma = (pt^{-1}-1)\Lambda_G[t, t^{-1}]$. Let $x = \sum_{n=a}^{b} x_n t^n \in$

$\Lambda_G[t, t^{-1}]$ be such that

$$(pt^{-1} - 1)x = px_a t^{a-1} + \sum_{n=a}^{b-1} (px_{n+1} - x_n)t^n - x_b t^b \in \widetilde{\Lambda_G}.$$

Reading off coefficients starting with x_b gives $x \in \widetilde{\Lambda_G}$, as required. □

5.2 The centre of $\Pi_{\mathfrak{g}}$

When H is the uniform pro-p group such that $\mathfrak{g} := p^{-1}L_H$ equals $X_{\mathbb{Z}_p}$ for some root system X, the Iwasawa algebra Λ_H has trivial centre by Corollary 4.1.3 and Lemma 2.5.13.

However, the larger ring $\Pi_{\mathfrak{g}}$ possesses nontrivial central elements, being closely related to the classical universal enveloping algebra $\mathcal{U}(\mathcal{L}(H))$. The remainder of this chapter is devoted to the computation of $Z(\Pi_{\mathfrak{g}})$. This will involve making some (mild) restrictions on the prime p.

The main result is:

Theorem 5.2.1. *Assume the prime p satisfies conditions (B) and (C) below. Then the centre of $\Pi_{\mathfrak{g}}$ is equal to the closure of the centre of $\mathcal{U}(\mathfrak{g})$:*

$$Z(\Pi_{\mathfrak{g}}) = \overline{Z(\mathcal{U}(\mathfrak{g}))}.$$

Of course, one inclusion is obvious. The proof of the other inclusion is given at the end of the chapter. In this section, we will establish some generalities, as well as elucidate the structure of $\overline{Z(\mathcal{U}(\mathfrak{g}))}$.

We will use the language of affine group schemes. For the necessary background on these objects, consult [17] or [29].

Let G be a connected, split semisimple, simply-connected affine group scheme over $\mathbb{Z}$ ([17], II.1.1). Let $\mathcal{R}$ be the root system of G and let Lie(G) be the Lie algebra of G ([17],I.7.7). We will assume G is chosen so that $\mathcal{R} = X$.

If k is any commutative ring, let G_k be k-group scheme obtained from G by base change ([17], I.1.10). Note that $\mathfrak{g}_k :=$ Lie$(G_k) \cong$ Lie$(G) \otimes k$ by formula (1) of [17] II.1.1.

Let K be an algebraically closed field of characteristic p. We will assume the prime p satisfies the following hypotheses:

- (B) p is odd and a good prime for G
- (C) the trace form on Lie(G_K) is non-degenerate.

The primes which are not good for an irreducible root system are

- $p = 2$ for types B_r, C_r and D_r;
- $p = 2$ or 3 for types E_6, E_7, F_4, G_2

- $p = 2, 3$ or 5 for type E_8.

Note that p is a good prime for G if and only if it is a good prime for each irreducible component of $\mathcal{R}$.

Hypothesis (C) excludes the case when $\mathcal{R}$ has an irreducible component of type A_r with $p|r+1$.

See section 2.9 of [2] (or section 6.1 of [18]) for a fuller discussion of these hypotheses. Our hypotheses are the same as those in [2], together with the additional constraint that G be semisimple. Note that hypothesis (A) of [2], namely

- (A) the derived group $\mathcal{D}G$ of G is simply-connected

follows automatically, since $\mathcal{D}G = G$ ([17], II.1.18).

Note also that $\mathfrak{g}_{\mathbb{Z}}$ is the $\mathbb{Z}$-form of the corresponding semisimple complex Lie algebra by the remark made in paragraph 2 of section 9.6 of [18]. In terms of our earlier notation (see Definition 2.8.2), this means that $\mathfrak{g}_k = \mathcal{R}_k$, so that $\mathfrak{g}_{\mathbb{Z}_p}$ is the $\mathbb{Z}_p$-Lie algebra we started off with, namely $\mathfrak{g}$.

Recall ([17], I.2.10) that if M is a G_k-module, then M^{G_k} is the scheme-theoretic submodule of fixed points of G_k, given by

$$M^{G_k} = \{m \in M : g(m \otimes 1) = m \otimes 1 \quad \text{for all} \quad g \in G_k(A), \quad \text{for all} \quad A\}$$

where A can be any (commutative) k-algebra.

Taking fixed points commutes with flat base change:

Lemma 5.2.2. *Let k be a commutative ring, let Y be an affine k-group scheme and let k' be a k-algebra which is flat as a k-module. Let M be a*

Y-module. Then

$$(M \otimes k')^{Y_{k'}} = M^Y \otimes k'.$$

Proof. This is formula (3) of [17], I.2.10. □

The following basic lemma concerning vector spaces will be useful to us in a number of places.

Lemma 5.2.3. *Let $L \subset F$ be a field extension and let $A \subseteq B$ be vector spaces over L. If the natural map $A \otimes_L F \to B \otimes_L F$ is an isomorphism, then $A = B$.*

We have the following description of the centre of $\mathcal{U}(\mathfrak{g}_{\mathbb{Z}_p})$, essentially due to Harish-Chandra:

Proposition 5.2.4. *The centre of $\mathcal{U}(\mathfrak{g})$ is equal to the ring of invariants under the adjoint action of $G_{\mathbb{Z}_p}$ on $\mathcal{U}(\mathfrak{g})$:*

$$Z(\mathcal{U}(\mathfrak{g})) = \mathcal{U}(\mathfrak{g})^{G_{\mathbb{Z}_p}}.$$

Proof. If L is a field of characteristic 0, the image of $G(L)$ in $\mathrm{Aut}(\mathfrak{g}_L)$ under the adjoint representation equals the adjoint Chevalley group of $\mathfrak{g}_L$, $X(L)$. By Lemma 23.2 of [15] (the proof of which does not require L to be algebraically closed), we see that

$$\mathcal{U}(\mathfrak{g}_L)^{G_L} \subseteq \mathcal{U}(\mathfrak{g}_L)^{G(L)} = \mathcal{U}(\mathfrak{g}_L)^{X(L)} = Z(\mathcal{U}(\mathfrak{g}_L)).$$

Let F denote the algebraic closure of L. If $F = L$, the first inclusion above is an equality ([17], Remark I.2.8). Since $\mathcal{U}(\mathfrak{g}_L)^{G_L} \otimes_L F = \mathcal{U}(\mathfrak{g}_F)^{G_F}$

by Lemma 5.2.2 and since $Z(\mathcal{U}(\mathfrak{g}_L)) \otimes_L F \subseteq Z(\mathcal{U}(\mathfrak{g}_F))$, we see that

$$\mathcal{U}(\mathfrak{g}_L)^{G_L} = Z(\mathcal{U}(\mathfrak{g}_L)),$$

using Lemma 5.2.3.

Now let $L = \mathbb{Q}_p$. The result follows after taking intersections with $\mathcal{U}(\mathfrak{g})$ and again using Lemma 5.2.2. □

It turns out that under our hypotheses on p, there is a nice connection between the G-invariants in $\mathcal{U}(\mathfrak{g}_{\mathbb{F}_p})$ and those in $\mathcal{U}(\mathfrak{g}_{\mathbb{Z}_p})$. The next result is due to Jantzen ([18]).

Proposition 5.2.5. *(i) The ring of invariants $\mathcal{U}(\mathfrak{g}_{\mathbb{F}_p})^{G_{\mathbb{F}_p}}$ is isomorphic to a polynomial algebra $\mathbb{F}_p[t_1, \ldots, t_r]$, where r is the rank of $\mathcal{R}$.*

(ii) $\mathcal{U}(\mathfrak{g}_{\mathbb{F}_p})^{G_{\mathbb{F}_p}} \cong \mathcal{U}(\mathfrak{g}_{\mathbb{Z}_p})^{G_{\mathbb{Z}_p}} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$.

Proof. (i) It is shown in section 9.6 of [18] that $\mathcal{U}(\mathfrak{g}_{\mathbb{F}_p})^{G_{\mathbb{F}_p}} \cong \mathcal{U}(\mathfrak{h}_{\mathbb{F}_p})^W$, where $\mathfrak{h}$ is the Lie algebra of a split maximal torus of G and W is the Weyl group of G.

The discussion in section 9.6 of [18] shows that we may apply the Corollary to Theorem 3 of [9] to deduce that $\mathcal{U}(\mathfrak{h}_{\mathbb{F}_p})^W$ is a polynomial algebra in r variables over $\mathbb{F}_p$.

(ii) The final sentence of section 9.6 of [18] says that

$$\mathcal{U}(\mathfrak{g}_K)^{G_K} \cong \mathcal{U}(\mathfrak{g}_{\mathbb{Z}})^{G_{\mathbb{Z}}} \otimes_{\mathbb{Z}} K,$$

where K is an algebraically closed field of characteristic p.

The result easily follows from this, using Lemmas 5.2.2 and 5.2.3. □

We can use this result to describe the algebraic structure of the closure of $Z(\mathcal{U}(\mathfrak{g}))$ in $\Pi_{\mathfrak{g}}$.

Proposition 5.2.6. $\overline{Z(\mathcal{U}(\mathfrak{g}))}$ *is isomorphic to the* p*-adic completion of a polynomial algebra in* r *variables over* $\mathbb{Z}_p$*:*

$$\overline{Z(\mathcal{U}(\mathfrak{g}))} \cong \mathbb{Z}_p[\widehat{c_1, \ldots}, c_r].$$

Proof. Let $R = \mathcal{U}(\mathfrak{g})^{G_{\mathbb{Z}_p}} = Z(\mathcal{U}(\mathfrak{g}))$, by Proposition 5.2.4. Since a p-torsion free $\mathbb{Z}_p$-module is flat (being a direct limit of free modules), tensoring the short exact sequence $0 \to p\mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{F}_p \to 0$ with R shows that $R \otimes_{\mathbb{Z}_p} \mathbb{F}_p \cong R/pR$. Also, the graded ring of R with respect to the p-adic filtration is isomorphic to $(R/pR)[s]$.

It's easy to check that $R \cap p^n\mathcal{U}(\mathfrak{g}) = p^n R$ for all $n \geq 0$; this implies that the subspace filtration on R induced from the p-adic filtration on $\mathcal{U}(\mathfrak{g})$ coincides with the p-adic filtration on R, so $\overline{R}$ is isomorphic to the p-adic completion of R.

By Proposition 5.2.5, $R/pR \cong \mathbb{F}_p[t_1, \ldots, t_r]$. Choose lifts $x_i \in R$ such that $x_i + pR \mapsto t_i$ for each $i = 1, \ldots, r$. The ring homomorphism

$$\mathbb{Z}_p[\widehat{c_1, \ldots}, c_r] \to \overline{R}$$

sending c_i to x_i induces an isomorphism on graded rings, and hence must be an isomorphism. □

Note that if in addition to (B) and (C) we assume that $p > h$, the Coxeter number of G, then the argument used in Proposition 2.1 of [28], together with the Corollary to Theorem 3 of [9] can be used to show that $Z(\mathcal{U}(\mathfrak{g}))$ is itself a polynomial algebra over $\mathbb{Z}_p$ in r variables. In this case, the above result becomes obvious.

5.3 Rings of invariants

In order to prove Theorem 5.2.1, we will require a number of results from the existing literature concerning certain rings of invariants and centres of universal enveloping algebras in characteristic p. These results are collected in this section - none are original, although we weaken the conditions on p for some of them.

For convenience, we will work over an algebraically closed field K of characteristic p.

Until the end of the proof of Corollary 5.4.9, $\mathfrak{g} = \mathfrak{g}_K$ and $G = G_K$.

We know from Proposition 5.2.5 that the ring of invariants $\mathcal{U}(\mathfrak{g})^G$ is isomorphic to a polynomial ring in r variables over K. We will choose the generators of this ring carefully in what follows.

Lemma 5.3.1. *Let G act on the symmetric algebra $\mathcal{S}(\mathfrak{g})$ via the adjoint action on $\mathfrak{g}$. There exist homogeneous invariants $S_1, S_2, \ldots, S_r$ of $\mathcal{S}(\mathfrak{g})$ such that $\mathcal{S}(\mathfrak{g})^G$ is a polynomial algebra on these generators:*

$$\mathcal{S}(\mathfrak{g})^G \cong K[S_1, \ldots, S_r].$$

Proof. See Lemma 3.3 of [2] and the remarks following it. □

In characteristic 0, ”symmetrization” provides an isomorphism of the G-

modules $\mathcal{S}(\mathfrak{g})$ and $\mathcal{U}(\mathfrak{g})$ ([10],2.4.6). There is an analogue to this in characteristic p, due to Friedlander and Parshall (based on the work of Mil'ner).

Theorem 5.3.2. *There exists a filtration-preserving isomorphism*

$$\beta : \mathcal{U}(\mathfrak{g}) \to \mathcal{S}(\mathfrak{g})$$

of G-modules such that $\operatorname{gr}(\beta)$ is the identity map on $\mathcal{S}(\mathfrak{g}) \cong \operatorname{gr}\mathcal{U}(\mathfrak{g})$.

Proof. This is Theorem 1.4 of [12]. The last claim follows by inspecting the proof of Lemma 1.1 and Theorem 1.2 of this paper. □

Clearly, this isomorphism cannot be multiplicative. However we can still infer

Corollary 5.3.3. *There exist elements $T_1, \ldots, T_r$ of $\mathcal{U}(\mathfrak{g})$ whose symbols in $\mathcal{S}(\mathfrak{g})$ are the invariants $S_1, \ldots, S_r$ and such that $\mathcal{U}(\mathfrak{g})^G = K[T_1, \ldots, T_r]$.*

Proof. Set $T_i = \beta^{-1}(S_i)$. Since $\operatorname{gr}(\beta) = 1$, we see that $\operatorname{gr}(\mathcal{U}(\mathfrak{g})^G) = \mathcal{S}(\mathfrak{g})^G$. It follows from Proposition 10 of III.2.9 of [4](p. 180) that the K-algebra generated by $T_1, \ldots, T_r$ is a polynomial algebra, which must equal $\mathcal{U}(\mathfrak{g})^G$. □

We can view $\mathcal{S}(\mathfrak{g})$ as the polynomial algebra on $\mathfrak{g}^*$. The following proposition is crucial to the proof of the results we're interested in (5.3.6, 5.3.7, 5.3.8). See Section 3.2 of [2] for a definition of regularity of $\varphi \in \mathfrak{g}^*$.

Proposition 5.3.4. *Let $\{X_1, \ldots, X_d\}$ be a basis for $\mathfrak{g}$. An element $\varphi \in \mathfrak{g}^*$ is regular if and only if the $r \times d$ Jacobian matrix $(\frac{\partial S_i}{\partial X_j})(\varphi)$ has rank r.*

Proof. When $p \nmid |W|$, this was proved by Veldkamp in [28], Theorem 7.1. The restriction on p was weakened to our current hypotheses (B) and (C) by Brown and Gordon (Corollary 3.4 of [2]). □

By Example 2.9.3, $\mathfrak{g}$ is restricted. The p-structure is given by the following formulae (see, e.g. section 6.1 of [18]):

$$\begin{aligned} h_i^{[p]} &= h_i, \quad 1 \le i \le r \\ e_\alpha^{[p]} &= 0, \quad\ \alpha \in X. \end{aligned}$$

Let G_n denote the n-th Frobenius kernel of G (see [17], I.9). This is an infinitesimal subgroup scheme of G. It is primarily of interest to us because the representation theory of the first Frobenius kernel G_1 is equivalent to the representation theory of $\mathfrak{g}$ as a restricted Lie algebra ([17], I.9.6). The adjoint action of G on $\mathcal{S}(\mathfrak{g})$ and $\mathcal{U}(\mathfrak{g})$ restricts to G_n, so we may consider the appropriate rings of invariants.

Let $\mathbf{S}^\alpha = S_1^{\alpha_1} \dots S_r^{\alpha_r}$ when $\alpha \in \mathbb{N}^r$, and let $\mathbb{N}^r_{p^n} = \{\alpha \in \mathbb{N}^r : \alpha_i < p^n$ for all $i = 1, \dots, r\}$ for each $n \ge 1$.

Theorem 5.3.5. *Let $n \ge 1$ and let $\mathcal{S}(\mathfrak{g})^{p^n}$ denote the subring of $\mathcal{S}(\mathfrak{g})$ generated by p^n-th powers of elements of $\mathfrak{g}$. The ring of invariants $\mathcal{S}(\mathfrak{g})^{G_n}$ is generated as a K-algebra by $\mathcal{S}(\mathfrak{g})^{p^n}$ and $\mathcal{S}(\mathfrak{g})^G$. Moreover, the homogeneous elements $\{\mathbf{S}^\alpha,\ \alpha \in \mathbb{N}^r_{p^n}\}$ are linearly independent over $\mathcal{S}(\mathfrak{g})^{p^n}$.*

Proof. When G is almost simple and $p \nmid |W|$, this follows from Theorem 4.1 of [12]. A careful reading of the proof of that result shows that the condition $p \nmid |W|$ can be weakened to conditions (B) and (C), in the light of Lemma 5.3.1 and Proposition 5.3.4.

The extension to the semisimple case causes no problems. □

When $n = 1$, we obtain

Corollary 5.3.6. *$\mathcal{S}(\mathfrak{g})^{\mathfrak{g}}$ is generated by $\mathcal{S}(\mathfrak{g})^p$ and $\mathcal{S}(\mathfrak{g})^G$.*

We can use the G-isomorphism β between $\mathcal{S}(\mathfrak{g})$ and $\mathcal{U}(\mathfrak{g})$ (see Theorem 5.3.2) to deduce analogous results for $\mathcal{U}(\mathfrak{g})$.

By Proposition 2.9.4, we know that $\mathcal{U}(\mathfrak{g})$ contains a large central subalgebra $\mathcal{O}$, the p-centre.

Theorem 5.3.7. *For each $n \geq 1$, let $\mathcal{O}_n$ denote $\mathcal{O}^{p^{n-1}}$. Then*

(i) The ring of invariants $\mathcal{U}(\mathfrak{g})^{G_n}$ is generated by $\mathcal{O}_n$ and $\mathcal{U}(\mathfrak{g})^G$.

(ii) $\mathcal{U}(\mathfrak{g})^{G_n}$ is a free $\mathcal{O}_n$-module of rank p^{nr}:

$$\mathcal{U}(\mathfrak{g})^{G_n} = \bigoplus_{\alpha \in \mathbb{N}^r_{p^n}} \mathcal{O}_n \mathbf{T}^\alpha.$$

Proof. In the case when $p \nmid |W|$ and G is almost simple, this is Corollary 4.3 of [12], which is deduced directly from Theorem 4.1 of [12], using the map β. In view of the comments made in the proof of Theorem 5.3.5, the result follows *mutatis mutandis.* □

By specializing to the case $n = 1$ we obtain a description $Z(\mathcal{U}(\mathfrak{g}))$.

Corollary 5.3.8. *Let $Z = Z(\mathcal{U}(\mathfrak{g}))$. Then:*

(i) Z is generated as a K-algebra by $\mathcal{U}(\mathfrak{g})^G$ and $\mathcal{O}$.

(ii) Z is a free $\mathcal{O}$-module of rank p^r:

$$Z = \bigoplus_{\alpha \in \mathbb{N}_p^r} \mathcal{O}\mathbf{T}^\alpha.$$

Note that this result also follows from Theorem 3.5 of [2]. We will denote $\mathcal{U}(\mathfrak{g})^{G_n}$ by $\mathcal{O}_n[\mathbf{T}]$ in what follows.

5.4 Proof of Theorem 5.2.1

Let $\overline{\mathbb{Z}_p}$ denote the maximal unramified extension of $\mathbb{Z}_p$. This is a complete local discrete valuation ring with maximal ideal $p\overline{\mathbb{Z}_p}$ and residue field $K = \overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$.

Let $R = \mathcal{U}(\mathfrak{g}_{\overline{\mathbb{Z}_p}})$. Clearly, $R/pR \cong \mathcal{U}(\mathfrak{g})$ where $\mathfrak{g} = \mathfrak{g}_K$ is the K-Lie algebra considered in the previous section.

Let $Y_n = \{y \in R : [y, R] \subseteq p^n R\}$ for $n \in \mathbb{N}$, the inverse image in R of the centre of $R/p^n R$. Note that $Y_0 = R$.

Let $\pi : R \to R/pR$ denote the natural projection. Let $Z_n = \pi(Y_n)$; it's clear that $Z_1 = Z(\mathcal{U}(\mathfrak{g}))$ and that $p^{n-l}Y_l \subseteq Y_n$ for any $l = 0, \ldots, n$.

We will sometimes write $\bar{y}$ for $\pi(y)$ when $y \in R$.

Our goal will be to prove the following

Theorem 5.4.1. $Z_n = \mathcal{O}_n[\mathbf{T}]$.

We start with some computational results. The first one is an analogue of Lemma 5 of [21].

Lemma 5.4.2. *Let A be a commutative $\mathbb{F}_p$-algebra, $D \in Der A, y \in A$. Then*

$$D^{p-1}(y^{p-1}Dy) = y^{p-1}D^p y - (Dy)^p.$$

Proof. By the Leibniz formula, we have

$$\begin{aligned}
&D^{p-1}(y^{p-1}Dy) - y^{p-1}D^p y = \\
&= \sum_{\substack{0 \le j_1, \dots, j_p < p \\ j_1+j_2+\dots+j_p=p-1}} \frac{(p-1)!}{j_1! \dots j_p!} \, D^{j_1}yD^{j_2}y \dots D^{j_p+1}y \quad - \quad y^{p-1}D^p y \\
&= \sum_{\substack{0 \le j_1, \dots, j_{p-1} < p \\ 1 \le j_p < p \\ j_1+j_2+\dots+j_p=p}} \frac{(p-1)!}{j_1! \dots j_p!} \, j_p \, D^{j_1}yD^{j_2}y \dots D^{j_p}y \\
&= \sum_{s \in S} \frac{(p-1)!}{0!^{s_0}1!^{s_1} \dots (p-1)!^{s_{p-1}}} (D^0 y)^{s_0} \cdots (D^{p-1}y)^{s_{p-1}} \sum_{j \in M(s)} j_p
\end{aligned}$$

since A is commutative. Here $S = \{s = (s_0, \dots, s_{p-1}) \in \mathbb{N}^p : \sum_{i=0}^{p-1} s_i = \sum_{i=0}^{p-1} i s_i = p\}$ and for $s \in S$,

$$M(s) = \{j = (j_1, \dots, j_p) \in \mathbb{N}^p : |\{k | j_k = i\}| = s_i \quad \forall i = 0, \dots, p-1\}.$$

If $s \in S$, let $\lambda_s = \sum_{j \in M(s)} j_p$. By symmetry, $\lambda_s = \sum_{j \in M(s)} j_k$ for any $k = 1, \dots, p$, whence

$$\lambda_s = \frac{1}{p} \sum_{j \in M(s)} (j_1 + \dots + j_p) = |M(s)| = \frac{p!}{s_0! \dots s_{p-1}!}.$$

Hence $\lambda_s = 0 \bmod p$, unless $s = (0, p, 0, \ldots, 0)$ when $\lambda_s = 1$. It follows that

$$\begin{aligned} D^{p-1}(y^{p-1}Dy) &= y^{p-1}D^p y + \frac{(p-1)!}{0!^0 1!^p \ldots (p-1)!^0}(Dy)^p \\ &= y^{p-1}D^p y - (Dy)^p, \end{aligned}$$

as required. □

Lemma 5.4.3. *Let A be a ring, $a, b \in A, k \in \mathbb{N}$. Then*

$$[a, b^k] = \sum_{i=0}^{k-1} b^i [a, b] b^{k-1-i}.$$

Proof. This follows from an easy induction argument, using the fact that $x \mapsto [a, x]$ is a derivation of R to itself. □

Lemma 5.4.4. *Let A be a ring, $a, b \in A$ such that $[b, A] \subseteq pA$. Suppose $[a, b] = pc$ for some $c \in A$. Then*

$$[a, b^{p^n}] = p^{n+1} c b^{p^n - 1} \mod p^{n+2} A.$$

Proof. Proceed by induction on n, the case $n = 0$ being clear.

Let $n \geq 1$ and assume $[a, b^{p^{n-1}}] = p^n c b^{p^{n-1}-1} + p^{n+1} d$ for some $d \in A$. By Lemma 5.4.3, we have

$$\begin{aligned} [a, b^{p^n}] &= \sum_{i=0}^{p-1} b^{p^{n-1} i} [a, b^{p^{n-1}}] b^{p^{n-1}(p-1-i)} \\ &= p^n \sum_{i=0}^{p-1} c b^{p^n - p^{n-1}} + p^n \sum_{i=0}^{p-1} [b^{p^{n-1} i}, c] b^{p^{n-1}(p-i)-1} + p^{n+1} u \end{aligned}$$

where $u = \sum_{i=0}^{p-1} b^{p^{n-1}i} d b^{p^{n-1}(p-1-i)}$. Now, using Lemma 5.4.3 again,

$$\begin{aligned}
[b^{p^{n-1}i}, c] &= \sum_{j=0}^{i-1} b^{p^{n-1}j}[b^{p^{n-1}}, c] b^{p^{n-1}(i-j-1)} \\
&\equiv \sum_{j=0}^{i-1} [b^{p^{n-1}}, c] b^{p^{n-1}(i-1)} \equiv i[b^{p^{n-1}}, c] b^{p^{n-1}(i-1)} \mod p^2 A
\end{aligned}$$

since $[b, [b, A]] \subseteq p^2 A$. Hence,

$$\begin{aligned}
[a, b^{p^n}] &\equiv p^{n+1} c b^{p^n - 1} + p^n (\sum_{i=0}^{p-1} i)[b^{p^{n-1}}, c] b^{p^{n-1}(p-1)-1} + p^{n+1} u \\
&\equiv p^{n+1} c b^{p^{n-1}} \mod p^{n+2} A
\end{aligned}$$

since $u \equiv p d b^{p^{n-1}(p-1)} \equiv 0 \mod pA$ and since we're assuming p to be odd. □

Note that Lemma 5.4.4 shows that $Y_1^{p^{n-1}} \subseteq Y_n$ for all $n \geq 1$. Moreover, we now have enough information to prove one of the inclusions in Theorem 5.4.1:

Proposition 5.4.5. $\mathcal{O}_n[\mathbf{T}] \subseteq Z_n$.

Proof. It's sufficient to prove that $\mathcal{O}_n \subseteq Z_n$ and $T_i \in Z_n$ for all $1 \leq i \leq r$. Proposition 5.2.5(ii) shows that

$$\mathcal{U}(\mathfrak{g})^{G_K} = \mathcal{U}(\mathfrak{g}_{\mathbb{Z}_p})^{G_{\mathbb{Z}_p}} \otimes_{\mathbb{Z}_p} K.$$

Hence, there exist $C_1, \ldots, C_r \in \mathcal{U}(\mathfrak{g}_{\mathbb{Z}_p})^{G_{\mathbb{Z}_p}}$ such that $T_i = C_i \otimes 1 = \pi(C_i)$ (see the proof of Proposition 5.2.6). The C_i's are central elements of R by Theorem 5.2.4 and hence lie in all the Y_n's. It follows that $T_i \in Z_n$ for all i

and n. Also, $\mathcal{O}_n = \mathcal{O}^{p^{n-1}} \subseteq \pi(Y_1)^{p^{n-1}} \subseteq \pi(Y_n) = Z_n$, by the above remark and Corollary 5.3.8. The result follows. □

We will fix the central elements $C_1, \dots, C_r \in R$ in what follows.

For $n \in \mathbb{N}$ and $x \in Z_1$, define $\overline{\mathbb{Z}_p}$-linear maps

$$\begin{aligned} D_x^{(n)} : Y_n &\to Z_1 \\ y &\mapsto \pi(z) \end{aligned}$$

where $[\tilde{x}, y] = p^n z$ for any $\tilde{x} \in \pi^{-1}(x) \subseteq Y_1$.

If $u \in R$, $[u, p^n z] = -[\tilde{x}, [y, u]] - [y, [u, \tilde{x}]] \in [\tilde{x}, p^n R] + [y, pR] \subseteq p^{n+1}R$, so $[\bar{u}, \bar{z}] = 0$ for all $\bar{u} \in R/pR$. It follows that $\pi(z) \in Z_1$.

Since $[pR, Y_n] \subseteq p^{n+1}R$, we see that $\pi(z)$ only depends on x and not on $\tilde{x}$, meaning that $D_x^{(n)}$ is well-defined. We think of $D_x^{(n)}$ as "$\mathrm{ad}(x)/p^n \mod p$".

Lemma 5.4.6. *The maps $D_x^{(n)}$ satisfy the following relations:*

(i) $D_x^{(0)} = 0$

(ii) $D_x^{(n)}(p^{n-l}y) = D_x^{(l)}(y)$ *for all* $y \in Y_l, l = 0, \dots, n$

(iii) $D_x^{(n)}(C_i y) = T_i D_x^{(n)}(y)$ *for all* $y \in Y_n, i = 1, \dots, r$

(iv) $D_x^{(n)}(y^{p^{n-1}}) = \bar{y}^{p^{n-1}-1} D_x^{(1)}(y)$ *for all* $y \in Y_1$.

Proof. Parts (i),(ii) and (iii) follow immediately from the definitions, noting that $\pi([\tilde{x}, R]) = 0$ and that C_i is central in R. Part (iv) follows directly from Lemma 5.4.4. □

We concentrate on the maps $D_x^{(1)}$. Since $D_x^{(1)}(pR) = 0$ by the above, we may define maps

$$\begin{array}{rcl} P_x^{(1)} : Z_1 & \to & Z_1 \\ \bar{y} & \mapsto & D_x^{(1)}(y) \end{array}$$

As shown in section 1 of [21], these are *Poisson derivations* of the centre Z_1 of $\mathcal{U}(\mathfrak{g})$. This means that if we set $\{a, b\} = P_a^{(1)}(b)$ for $a, b \in Z_1$, then $\{,\}$ is a *Poisson bracket* on Z_1. Recall that a Poisson bracket on a K-algebra A is a K-linear Lie bracket $\{,\} : A \times A \to A$ which is also a biderivation: $\{ab, c\} = a\{b, c\} + \{a, c\}b$ for all $a, b, c \in A$.

Recall the semilinear map $\varphi : \mathfrak{g} \to \mathcal{O}$ given by $\varphi(x) = x^p - x^{[p]}$; see Proposition 2.9.4. We have the following connection between the Lie structure on $\mathfrak{g}$ and the Poisson bracket on Z_1:

Theorem 5.4.7. *For all $a, b \in \mathfrak{g}$, $\{\varphi(a), \varphi(b)\} = \varphi([a, b])$.*

Proof. This is the content of Corollary 1 of [21], where everything is done over $\mathbb{F}_p$. The result extends easily to K, using the semilinearity of φ. □

Since $\mathcal{O}$ is generated by $\varphi(\mathfrak{g})$ as a K-algebra, we see that $\{\mathcal{O}, \mathcal{O}\} \subseteq \mathcal{O}$. We can transfer the Poisson structure to $\mathcal{O}_n$.

For $n \in \mathbb{N}$ and $x \in Z_1$, define a K-linear map $P_x^{(n)} : \mathcal{O}_n \to \mathcal{O}_n$ by setting $P_x^{(n)}(y^{p^{n-1}}) = P_x^{(1)}(y)^{p^{n-1}}$. Since $\mathcal{O}_n[\mathbf{T}]$ is a free $\mathcal{O}_n$-module by Theorem 5.3.7(ii), we can extend $P_x^{(n)}$ to the whole of $\mathcal{O}_n[\mathbf{T}]$ by insisting that $P_x^{(n)}(T_i y) = T_i P_x^{(n)}(y)$ for $y \in \mathcal{O}_n$ and $i = 1, \ldots, r$.

The next proposition essentially says that

$$(\mathcal{U}(\mathfrak{g})^{G_n})^{\mathfrak{g}^{(n)}} = (\mathcal{U}(\mathfrak{g})^{G_n})^{\frac{G_{n+1}}{G_n}} = \mathcal{U}(\mathfrak{g})^{G_{n+1}}.$$

Proposition 5.4.8. *For all $n \geq 1$,*

$$\bigcap_{x \in \varphi(\mathfrak{g})} \ker P_x^{(n)} = \mathcal{O}_{n+1}[\mathbf{T}].$$

Proof. Let $x \in Z_1$. Since $P_x^{(1)}$ is a derivation of the $\mathbb{F}_p$-algebra $\mathcal{O}$, $P_x^{(1)}(y^p) = 0$ for all $y \in \mathcal{O}$. Since $P_x^{(1)}$ is $\mathbf{T}$-linear, it follows that

$$\mathcal{O}_{n+1}[\mathbf{T}] \subseteq \bigcap_{x \in \varphi(\mathfrak{g})} \ker P_x^{(n)}.$$

Let $\mathfrak{g}^{(1)}$ denote the Frobenius twist of $\mathfrak{g}$. As a set and a $\mathbb{F}_p$-Lie algebra, $\mathfrak{g}^{(1)} = \mathfrak{g}$, but K acts on $\mathfrak{g}^{(1)}$ via $a.x = a^{1/p}x$ for $a \in K, x \in \mathfrak{g}$.

Now, consider the maps $P^{(1)} : \mathfrak{g}^{(1)} \to \mathrm{End}_K(\mathcal{O})$ given by $P^{(1)}(x) = P^{(1)}_{\varphi(x)}$ and $\mathrm{ad}^{(1)} : \mathfrak{g}^{(1)} \to \mathrm{End}_K(\mathcal{S}(\mathfrak{g})^p)$ given by $\mathrm{ad}^{(1)}(x)(y^p) = [x, y]^p$, where $y \in \mathfrak{g}$. It can be easily checked using Theorem 5.4.7 and the fact that $\{,\}$ is a Poisson bracket that $P^{(1)}$ and $\mathrm{ad}^{(1)}$ are K-linear representations of $\mathfrak{g}^{(1)}$.

The semilinear map $\varphi : \mathfrak{g} \to \mathcal{O}$ gives rise to a natural K-algebra isomorphism

$$\psi : S(\mathfrak{g})^p \to \mathcal{O}$$

given on generators by $\psi(x^p) = \varphi(x)$ for all $x \in \mathfrak{g}$. It follows from the definitions and Theorem 5.4.7 that $P^{(1)}(x) \circ \psi = \psi \circ \mathrm{ad}^{(1)}(x)$ for all $x \in \mathfrak{g}^{(1)}$, so ψ is an isomorphism of $\mathfrak{g}^{(1)}$-modules. We can naturally identify $\mathcal{S}(\mathfrak{g}^{(1)})$

with $\mathcal{S}(\mathfrak{g})^p$, whence

$$\bigcap_{x\in\varphi(\mathfrak{g})} \ker P_x^{(1)}|_{\mathcal{O}} = \psi(\mathcal{S}(\mathfrak{g}^{(1)})^{\mathfrak{g}^{(1)}}).$$

Now, by Corollary 5.3.6, we see that

$$\mathcal{S}(\mathfrak{g}^{(1)})^{\mathfrak{g}^{(1)}} = (\mathcal{S}(\mathfrak{g})^{\mathfrak{g}})^p \subseteq < \mathcal{S}(\mathfrak{g}^{(1)})^p, \mathcal{S}(\mathfrak{g}^{(1)})^G > .$$

It can be shown that ψ is an isomorphism of G-modules, using the fact that the adjoint action of G on $\mathfrak{g}$ preserves the p-structure on $\mathfrak{g}$. Hence,

$$\bigcap_{x\in\varphi(\mathfrak{g})} \ker P_x^{(1)}|_{\mathcal{O}} \quad \subseteq \quad < \mathcal{O}^p, \mathcal{O}^G > .$$

Using Theorem 5.3.7, we obtain

$$\bigcap_{x\in\varphi(\mathfrak{g})} \ker P_x^{(n)} = \bigoplus_{\alpha\in\mathbb{N}^r_{p^n}} (\bigcap_{x\in\varphi(\mathfrak{g})} \ker P_x^{(n)}|_{\mathcal{O}_n})\mathbf{T}^\alpha \subseteq < \mathcal{O}_{n+1}, \mathcal{U}(\mathfrak{g})^G >= \mathcal{O}_{n+1}[\mathbf{T}],$$

as required. □

We can now give a proof of the main result of this section.

Proof of Theorem 5.4.1. We will prove by induction on n that the following statements hold:

(1) $Z_n = \mathcal{O}_n[\mathbf{T}]$.

(2) Let $x \in \varphi(\mathfrak{g})$ and let $1 \leq k \leq n$. Let $x^{[p]}$ denote $\varphi(\varphi^{-1}(x)^{[p]})$. There exist $\overline{\mathbb{Z}_p}$-linear maps $E_x^{(k,n)} : Y_n \to Z_1$ satisfying:

   (a) $E_x^{(1,n)} = D_x^{(n)}$

   (b) $E_x^{(k,n)}(p^{n-l}y) = E_x^{(k,l)}(y)$ for all $y \in Y_l$, $1 \leq k \leq l \leq n$

   (c) $E_x^{(k,n)}(y^{p^{n-1}}) = (\bar{y}^{p^{n-k}-1} D_x^{(1)}(y))^{p^{k-1}}$ for all $y \in Y_1$, $1 \leq k \leq n$

   (d) $E_x^{(k,n)}(C_i y) = T_i E_x^{(k,n)}(y)$ for all $y \in Y_n$, $1 \leq i \leq r$, $1 \leq k \leq n$

   (e) $\mathrm{Im} E_x^{(k,n)} \subseteq Z_k$, $1 \leq k \leq n$

   (f) $E_x^{(k,n)} = E_{x^{[p]}}^{(k-1,n)} - (P_x^{(k-1)})^{p-1} \circ E_x^{(k-1,n)}, 2 \leq k \leq n$

   (g) $E_x^{(n,n)}(y) = P_x^{(n)}(\bar{y})$ for all $y \in Y_n$.

Of these properties, (a) and (f) are the most important ones - they are the ones actually used to *define* the $E_x^{(k,n)}$. The remaining properties are listed in this order so that the definition in (f) makes sense.

The idea is that the information contained in the maps $D_x^{(n)}$, $x \in \varphi(\mathfrak{g})$ completely determines the derivations $P_x^{(n)}$, as seen from (a), (f) and (g).

When $n = 1$, (1) has been established in Corollary 5.3.8, whereas all parts of (2) follow by setting $E_x^{(1,1)} = D_x^{(1)}$ and using Lemma 5.4.6.

Let $y \in Y_n$ and $x \in \varphi(\mathfrak{g})$. Choose a lift $\tilde{x} \in R$ for x; we see that $[\tilde{x}, y] = p^n z = p^{n-1}(pz)$ for some $z \in R$. Hence $D_x^{(n-1)}(y) = E_x^{(1,n-1)}(y) = 0$.

Using (2)(a) and (f) inductively, we see that $E_x^{(k,n-1)}(y) = 0$ for all $k = 1, \ldots, n-1$. It follows from (2)(g) that $E_x^{(n-1,n-1)}(y) = P_x^{(n-1)}(\bar{y}) = 0$ for all $x \in \varphi(\mathfrak{g})$, so

$$\bar{y} \in \bigcap_{x \in \varphi(\mathfrak{g})} \ker P_x^{(n-1)} = \mathcal{O}_n[\mathbf{T}],$$

using Proposition 5.4.8. This proves (1), in view of Proposition 5.4.5.

Next, we construct $E_x^{(k,n)} : Y_n \to Z_1$ by induction on k, showing that each $E_x^{(k,n)}$ satisfies conditions (a) to (g).

Define $E_x^{(1,n)} = D_x^{(n)}$, so that (a) is satisfied automatically. Properties (b),(c) and (d) follow directly from Lemma 5.4.6 and the remaining ones are true trivially.

Let $2 \leq k \leq n$ and $x \in \varphi(\mathfrak{g})$. Assume that for each $j = 1, \ldots, k-1$, $E_x^{(j,n)}$ has been defined. Since $\mathrm{Im} E_x^{(k-1,n)} \subseteq Z_k = \mathcal{O}_k[\mathbf{T}]$ by (e) and (1), we may define

$$E_x^{(k,n)} := E_{x^{[p]}}^{(k-1,n)} - (P_x^{(k-1)})^{p-1} \circ E_x^{(k-1,n)} : Y_n \to Z_1.$$

It's clear that $E_x^{(k,n)}$ is $\overline{\mathbb{Z}_p}$-linear. We check that $E_x^{(k,n)}$ satisfies (b), (c) and (d).

Let $k \leq l \leq n$ and let $y \in Y_l$. Then, using (b) and (f) inductively,

$$\begin{aligned} E_x^{(k,n)}(p^{n-l}y) &= E_{x^{[p]}}^{(k-1,n)}(p^{n-l}y) - (P_x^{(k-1)})^{p-1}(E_x^{(k-1,n)}(p^{n-l}y)) \\ &= E_{x^{[p]}}^{(k-1,l)}(y) - (P_x^{(k-1)})^{p-1}(E_x^{(k-1,l)}(y)) \\ &= E_x^{(k,l)}(y), \end{aligned}$$

which shows that (b) holds.

Next, let $y \in Y_1$. Writing $a = \bar{y}, D' = P_{x^{[p]}}^{(1)}, D = P_x^{(1)}$ and using (c) and (f) inductively, we see that

$$\begin{aligned} E_x^{(k,n)}(y^{p^{n-1}}) &= E_{x^{[p]}}^{(k-1,n)}(y^{p^{n-1}}) - (P_x^{(k-1)})^{p-1}(E_x^{(k-1,n)}(y^{p^{n-1}})) \\ &= (a^{p^{n-k+1}-1}D'a)^{p^{k-2}} - (P_x^{(k-1)})^{p-1}((a^{p^{n-k+1}-1}Da)^{p^{k-2}}) \\ &= (a^{p^{n-k+1}-1}D'a - D^{p-1}(a^{p^{n-k+1}-1}Da))^{p^{k-2}} \end{aligned}$$

Now, D is a derivation of Z_1, so $D(u^p) = 0$ for all $u \in Z_1$. Hence, by Proposition 5.4.2,

$$\begin{aligned} D^{p-1}(a^{p^{n-k+1}-1}Da) &= a^{p^{n-k+1}-p}D^{p-1}(a^{p-1}Da) \\ &= a^{p^{n-k+1}-p}(a^{p-1}D^pa - (Da)^p) \\ &= a^{p^{n-k+1}-1}D^pa - (a^{p^{n-k}-1}Da)^p. \end{aligned}$$

Since $\mathfrak{g}$ is restricted, $\operatorname{ad} u^{[p]} = (\operatorname{ad} u)^p$ for all $u \in \mathfrak{g}$. Extending this equality of derivations on $\mathfrak{g}$ to $\mathcal{S}(\mathfrak{g})$, we see that $\operatorname{ad}^{(1)} u^{[p]} = (\operatorname{ad}^{(1)} u)^p$, as derivations of $\mathcal{S}(\mathfrak{g}^{(1)})$ (see the proof of Proposition 5.4.8 for the relevant notation). In view of the isomorphism ψ, we have $P_{x^{[p]}}^{(1)} = (P_x^{(1)})^p$ for all $x \in \varphi(\mathfrak{g})$. Therefore,

$$\begin{aligned} E_x^{(k,n)}(y^{p^{n-1}}) &= (a^{p^{n-k+1}-1}(D'a - D^pa) + (a^{p^{n-k}-1}Da)^p)^{p^{k-2}} \\ &= (a^{p^{n-k}-1}Da)^{p^{k-1}} = (\bar{y}^{p^{n-k}-1}D_x^{(1)}(y))^{p^{k-1}}, \end{aligned}$$

proving (c).

An argument similar to the proof of (b) shows that (d) holds: use (d) and (f) inductively, noting that $P_x^{(k-1)}$ is $\mathbf{T}$-linear.

We can now prove (e). Let $y \in Y_n$, so that $\bar{y} \in \mathcal{O}_n[\mathbf{T}]$, by (1). Choosing appropriate lifts, we may write

$$y = \sum_{\alpha \in \mathbb{N}^r_{p^n}} v_\alpha^{p^{n-1}} \mathbf{C}^\alpha + pw$$

for some $w \in R$ and $v_\alpha \in Y_1$. Here $\mathbf{C}^\alpha = C_1^{\alpha_1} \dots C_r^{\alpha_r}$.

As $Y_1^{p^{n-1}} C_i \subseteq Y_n$ for all i, we see that $pw \in Y_n$, whence $w \in Y_{n-1}$. Suppose $k \leq n-1$. Then $E_x^{(k,n)}(pw) = E_x^{(k,n-1)}(w) \in Z_k$ by (b). If $k = n$,

$$\begin{aligned} E_x^{(n,n)}(pw) &= E_{x^{[p]}}^{(n-1,n)}(pw) - (P_x^{(n-1)})^{p-1}(E_x^{(n-1,n)}(pw)) \\ &= E_{x^{[p]}}^{(n-1,n-1)}(w) - (P_x^{(n-1)})^{p-1}(E_x^{(n-1,n-1)}(w)) \\ &= P_{x^{[p]}}^{(n-1)}(w) - (P_x^{(n-1)})^p(w) = 0 \in Z_k \end{aligned}$$

using (g) and the fact that $P_{x^{[p]}}^{(n-1)} = (P_x^{(n-1)})^p$. Now,

$$E_x^{(k,n)}(v_\alpha^{p^{n-1}} \mathbf{C}^\alpha) = (\overline{v_\alpha}^{p^{n-k}-1} D_x^{(1)} v_\alpha)^{p^{k-1}} \mathbf{T}^\alpha \in \mathcal{O}_k[\mathbf{T}] = Z_k,$$

by (c),(d) and (1). Part (e) follows.

Finally, (f) holds by definition, whereas (g) follows from (c) and the above computation of $E_x^{(n,n)}(y)$. □

Corollary 5.4.9. $\bigcap_{n=1}^\infty Z_n = \mathcal{U}(\mathfrak{g})^G = K[\mathbf{T}]$.

Proof. By Proposition 5.4.5, $K[\mathbf{T}] \subseteq Z_n$ for all $n \geq 1$.

Let $x \in \bigcap_{n=1}^\infty Z_n$. Choose n such that $p^n > \deg(x)$. By Theorems 5.4.1 and 5.3.7,

$$x \in \mathcal{O}_n[\mathbf{T}] = \bigoplus_{\alpha \in \mathbb{N}^r_{p^n}} \mathcal{O}_n \mathbf{T}^\alpha,$$

so we may write $x = \sum_{\alpha \in \mathbb{N}^r_{p^n}} x_\alpha$, where $x_\alpha \in \mathcal{O}_n \mathbf{T}^\alpha$. Let $k = \max \deg(x_\alpha)$; clearly $\deg(x) \leq k$.

If $\deg(x) < k$, some nontrivial sum of symbols of the x_α would have to be zero in $\operatorname{gr} \mathcal{U}(\mathfrak{g})$. Since $\operatorname{gr} \mathcal{O}_n = \mathcal{S}(\mathfrak{g})^{p^n}$ and since $\sigma(\mathbf{T}^\alpha) = \mathbf{S}^\alpha$, this is impossible by Theorem 5.3.5.

Hence $\deg(x_\alpha) \leq \deg(x) < p^n$ for each $\alpha \in \mathbb{N}^r_{p^n}$. This forces $x_\alpha \in K\mathbf{T}^\alpha$, whence $x \in K[\mathbf{T}]$, as required. □

We can at last deduce the main result. Let $\mathfrak{g} = \mathfrak{g}_{\mathbb{Z}_p}$, $G = G_{\mathbb{Z}}$.

Proof of Theorem 5.2.1. By Proposition 5.2.4, we know $\overline{\mathcal{U}(\mathfrak{g})^{G_{\mathbb{Z}_p}}} \subseteq Z(\Pi_{\mathfrak{g}})$, and that it is sufficient to prove the reverse inclusion.

Taking graded rings with respect to the p-adic filtration, we see that it is sufficient to prove that $\mathcal{U}(\mathfrak{g}_{\mathbb{F}_p})^{G_{\mathbb{F}_p}} = \pi(Z(\Pi_{\mathfrak{g}}))$, in view of Proposition 5.2.5.

If $x \in Z(\Pi_{\mathfrak{g}})$, then $\pi(x) \otimes 1 \in Z_n$ for all $n \geq 1$, so $\pi(Z(\Pi_{\mathfrak{g}})) \otimes_{\mathbb{F}_p} K \subseteq \bigcap_{n=1}^\infty Z_n = \mathcal{U}(\mathfrak{g}_K)^{G_K}$ by the above Corollary.

By Lemmas 5.2.2 and 5.2.3, $\pi(Z(\Pi_{\mathfrak{g}})) \subseteq \mathcal{U}(\mathfrak{g}_{\mathbb{F}_p})^{G_{\mathbb{F}_p}}$ and the other inclusion is clear. □

Bibliography

[1] K.A. Brown, C.R. Hajarnavis, A.B. MacEacharn, *Noetherian rings of finite global dimension*, Proc. London Math. Soc. (3) **44** (1982), no.2, 349-371

[2] K.A. Brown, I. Gordon, *The ramification of centres: Lie algebras in positive characteristic and quantised enveloping algebras*, Proc. London Math. Soc. (3) **84** (2002), no.1, 147-178

[3] K.A. Brown, R.B. Warfield, Jr, *The Influence of Ideal Structure on Representation Theory*, J. Algebra **116** (1988), 294-315

[4] N. Bourbaki, *Commutative Algebra*, Translated from French. Hermann (1972)

[5] A. Brumer, *Pseudocompact Algebras, Profinite Groups and Class Formations*, Bull. Amer. Math. Soc. **72** (1966), 321-324

[6] J. Coates, P. Schneider, R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), no. 1, 73-108

[7] R. Carter, *Simple groups of Lie type*, J. Wiley, London (1989)

[8] J. Clark, *Auslander-Gorenstein rings for beginners*, International Symposium on Ring Theory (Kyongju, 1999), 95-115

[9] M. Demazure, *Invariants symétriques entiers des groupes de Weyl et torsion*, Invent. Math., **21** (1973), 287-301

[10] J. Dixmier, *Enveloping Algebras*, Graduate Studies in Mathematics **11**, (1996)

[11] J.D.Dixon, M.P.F. Du Sautoy, A.Mann, D.Segal, *Analytic pro-p groups*, 2nd edition, CUP (1999)

[12] E.M. Friedlander, B.J. Parshall, *Rational actions associated to the adjoint representation*, Ann. Scient. Ec. Norm. Sup. (4) **20** (1987), 215-226

[13] M. Harris, *The annihilators of p-adic induced modules*, J. Algebra **67** (1980), no. 1, 68-71

[14] *Structure of central torsion Iwasawa modules*, Bull. Soc. Math. France **130** (2002), no. 4, 507-535

[15] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics **9**, Springer (1980)

[16] L. Huishi and F. van Oystaeyen, *Zariskian filtrations*, K-monographs in mathematics, vol.2 (1996)

[17] J. C. Jantzen, *Representations of Algebraic Groups*, Pure and Applied Mathematics; v. 131. (1987)

[18] J. C. Jantzen, *Representations of Lie Algebras in prime characteristic, Notes by Iain Gordon*, Representation theories and algebraic geometry (Montreal, PQ, 1997), 185-235, Kluwer Acad. Publ., Dordrecht (1998)

[19] N. Jacobson, *Lie Algebras*, Interscience Publishers, New York (1962)

[20] A. Joseph, *The minimal orbit in a simple Lie algebra and its associated maximal ideal*, Ann. Scient. Ec. Norm. Sup. **9** (1976), 1-30

[21] V. Kac, A. Radul, *Poisson structure for restricted Lie algebras*, The Gelfand Mathematical Seminars, 1996-1999, 77-84

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

[23] J.C.McConnell, J.C. Robson, *Noncommutative Noetherian rings*, J. Wiley, London (1987)

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

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

[26] S.P. Smith, *Krull dimension of factor rings of the enveloping algebra of a semi-simple Lie algebra*, Math. Proc. Camb. Phil. Soc. **93** (1983), 459-466

[27] S.P. Smith, *Krull dimension of the enveloping algebra of $\mathfrak{sl}(2,\mathbb{C})$*, J. Algebra **71** (1981), no. 1, 189-194

[28] F.D. Veldkamp, *The center of the universal enveloping algebra of a Lie algebra in characteristic p*, Ann. Scient. Ec. Norm. Sup. (4) **5** (1972), 217-240

[29] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Graduate Texts in Mathematics **66**, Springer (1979)

[30] S.J. Wadsley, *Finite presentation of solvable pro-p groups*, to appear

[31] R. Walker, *Local rings and normalizing sets of elements*, Proc. Lond. Math. Soc. **24** (1972), 27-45.