Krull dimension of Iwasawa algebras

Konstantin Ardakov

1 Introduction

Let $G$ be a compact $p$-adic Lie group. In the recent years, there has been an increased amount of interest in completed group algebras (Iwasawa algebras)

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

for example, because of their connections with number theory and arithmetic geometry; see the paper by Coates, Schneider and Sujatha ([4]) for more details.

When $G$ is a uniform pro-$p$ group, $\Lambda_G$ is a concrete example of a complete local Noetherian ring (noncommutative, in general) with good homological properties: it is known that $\Lambda_G$ has finite global dimension and is an Auslander regular ring. Thus, $\Lambda_G$ falls into the class of rings studied by Brown, Hajarnavis and MacEacharn in [1]. There they consider various properties of Noetherian rings $R$ of finite global dimension, including the Krull(-Gabriel-Rentschler) dimension $\mathcal{K}(R)$ - a module-theoretic dimension which measures how far $R$ is from being Artinian. They also posed the following question:

**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 $R$?

In this paper, we address the problem of computing $\mathcal{K}(\Lambda_G)$. We establish lower and upper bounds for $\mathcal{K}(\Lambda_G)$ in terms of the Lie algebra $\mathfrak{g} = \mathcal{L}(G)$ of $G$:

**Theorem A.** Let $\lambda(\mathfrak{g})$ 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 $\mathfrak{g}$. Then

$$\lambda(\mathfrak{g}) + 1 \leq \mathcal{K}(\Lambda_G) \leq \dim \mathfrak{g} + 1.$$

For some groups, the two bounds coincide:

**Corollary A.** Let $\tau$ be the solvable radical of $\mathfrak{g}$ and suppose that the semisimple part $\mathfrak{g}/\tau$ of $\mathfrak{g}$ is isomorphic to a direct sum of copies of $\mathfrak{sl}_2(\mathbb{Q}_p)$. Then $\mathcal{K}(\Lambda_G) = \dim \mathfrak{g} + 1.$
We also establish a better upper bound for $K(\Lambda_G)$ when $L(G)$ is simple and split over $\mathbb{Q}_p$:

**Theorem B.** Let $p \geq 5$ and suppose $g \neq \mathfrak{sl}_2(\mathbb{Q}_p)$ is split simple over $\mathbb{Q}_p$ with a Cartan subalgebra $t$ and a Borel subalgebra $b$. Then

$$\dim b + \dim t + 1 \leq K(\Lambda_G) \leq \dim g < \text{gld}(\Lambda_G).$$

The author believes that $\dim b + \dim t + 1$ is the true value of $K(\Lambda_G)$, with $G$ as above. Applying Theorem B to a particular case allows us to obtain a negative answer to the question posed above:

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

$$K(\Lambda_G) = 8 < \text{gld}(\Lambda_G) = 9.$$ 

In addition, we reprove a general result of R. Walker connecting $K(R)$ with $K(R/I)$ for a certain ring $R$ and a suitable ideal $I$:

**Theorem C (Walker, [10]).** Suppose $R$ is right Noetherian and $x$ is a right regular normal element belonging to the Jacobson radical of $R$. If $K(R) < \infty$ then

$$K(R) = K(R/xR) + 1.$$ 

The reader might like to compare this result with the corresponding one on global dimensions; see Theorem 7.3.7 of [7].

We will denote the completed group algebra of $G$ over $\mathbb{F}_p$ by $\Omega_G$:

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

Theorem C applies directly to Iwasawa algebras, since it is easy to see that $\Omega_G \cong \Lambda_G/p\Lambda_G$:

**Corollary C.** $K(\Lambda_G) = K(\Omega_G) + 1$.

The author would like to thank his supervisor, C.J.B. Brookes for many helpful conversations. Financial assistance from the EPSRC is also gratefully acknowledged.

**Notation.** All rings are assumed to be associative and to possess a unit, but are not necessarily commutative. $J(R)$ always denotes the Jacobson radical of the ring $R$. All modules are right modules, unless stated otherwise; $\text{Mod-R}$ denotes the category of all right modules over $R$. The symbol $p$ will always mean a fixed prime.
2 Preliminaries

2.1 Filtrations

We will conform with the definitions and notations used in the book [6] throughout this paper. In this section, we briefly recall the most relevant concepts.

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

Let $M$ be an $R$-module. A filtration on $M$ is a set of additive subgroups of $M$, $FM = \{F_nM : n \in \mathbb{Z}\}$, satisfying $F_nM \subseteq F_{n+1}M$, $F_nM.F_mM \subseteq F_{n+m}M$ for all $n, m \in \mathbb{Z}$ and $\bigcup_{n \in \mathbb{Z}} F_nM = M$. If $M$ has a filtration, $M$ is said to be a filtered $R$-module. The filtration on $M$ is said to be separated if $\bigcap_{n \in \mathbb{Z}} F_nM = 0$.

Let $I$ be a two-sided ideal of $R$. A notable example of a filtration on $R$ is the $I$-adic filtration given by $F_nR$ if $n \leq 0$ and $F_nR = R$ otherwise.

The associated graded ring of $R$ is defined to be $gr R = \bigoplus_{n \in \mathbb{Z}} F_nR/F_{n-1}R$. If $x \in R$, the symbol of $x$ in $gr R$ is $\sigma(x) := x + F_{n-1}R \in F_nR/F_{n-1}R$, where $n$ is such that $x \in F_nR \setminus F_{n-1}R$. If $x \in \bigcap_{n \in \mathbb{Z}} F_nR$, define $\sigma(x) = 0$.

The Rees ring of $R$ is defined to be $\tilde{R} = \bigoplus_{n \in \mathbb{Z}} F_nR$, which we view to be a subring of the Laurent polynomial ring $R[t, t^{-1}]$.

The associated graded module and Rees module of a filtered $R$-module $M$ are defined similarly. We say that the filtration $FM$ on $M$ is good if and only if $\tilde{M}$ is a finitely generated $\tilde{R}$-module. Note that a finitely generated $R$-module $M$ always possesses a good filtration, for example the deduced filtration given by $F_nM = M.F_nR$ for $n \in \mathbb{Z}$.

2.2 Iwasawa algebras

By a well-known result of Lazard (see, for example, Theorem 8.36 of [5]), any compact $p$-adic Lie group $G$ has an open normal uniform pro-$p$ subgroup $H$. Since $H$ has finite index in $G$, any open normal subgroup of $H$ contains an open normal subgroup of $G$. Hence

$$\Lambda_H = \lim_{\rightarrow N \in \mathcal{C}} \mathbb{Z}_p[H/N] \quad \text{and} \quad \Lambda_G = \lim_{\rightarrow N \in \mathcal{C}} \mathbb{Z}_p[G/N],$$

where $\mathcal{C} = \{N \triangleleft G : N \subseteq H\}$. It follows that $\Lambda_G$ is a free right and left $\Lambda_H$-module of finite rank (an appropriate transversal for $H$ in $G$ will serve as a basis), so $K(\Lambda_G) = K(\Lambda_H)$ by Corollary 6.5.3 of [7].
Thus restricting ourselves to the class of uniform pro-$p$ groups does not lose any generality and we will assume that $G$ denotes a uniform pro-$p$ group throughout this paper. For more information about these groups, see the excellent book [5].

Following [5], we will write $L_G$ for the $\mathbb{Z}_p$-Lie algebra of $G$ ([5], 4.29) and $\mathcal{L}(G) = g$ for the $\mathbb{Q}_p$-Lie algebra of $G$ ([5], 9.5).

The following properties of $\Lambda G$ and $\Omega G$ are more or less well known:

**Lemma 2.1.** Let $R = \Lambda G$ or $\Omega G$ and let $d = \dim G$. Then:

(i) $R$ is a local right Noetherian ring with maximal ideal $J = \ker(R \twoheadrightarrow \mathbb{F}_p)$.

(ii) $R$ is complete with respect to the $J$-adic filtration.

(iii) $\gr J \Omega_G \cong \mathbb{F}_p[X_1, \ldots, X_d]$.

(iv) $\gl(\Lambda G) = \gl(\Omega G) + 1 = \dim G + 1$.

(v) $J$ satisfies the right (and left) Artin Rees Property.

**Proof.** Proofs of (i),(ii) and (iii) can be found in Chapter 7 of [5]. Part (iv) is established in [2]. By Theorem 2.2 of Chapter II of [6], 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 [7].

Henceforth, $J_G$ will always denote the maximal ideal of $\Omega_G$. We will require the following characterization of Artinian modules of $\Omega_G$:

**Proposition 2.2.** 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 $\Omega_G$-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.** Note that by Theorem 3.6 of [5], $G_n$ is uniform for each $n \geq 1$.

(i) $\Rightarrow$ (ii). As $\Omega_G$ is Noetherian, $M$ has finite length. Also $\Omega_G/J_G$ is the unique simple $\Omega_G$-module, as $\Omega_G$ 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 $G_m = G^{p^{m-1}}$, 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 $\Omega_G$. Hence $\mathbb{F}_p[G/G_m] \cong \Omega_G/J_{G_m} \Omega_G \rightarrow \Omega_G/I = M$. Since $|G : G_m|$ is finite, the result follows.

(iv) $\Rightarrow$ (i). This is clear. \hfill $\square$

### 2.3 Krull dimension

The definitions and basic facts about the Krull(-Gabriel-Rentschler) dimension can be found in Chapter 6 of [7]. Recall that an $R$-module $M$ is said to be $n$-critical if $K(M) = n$ and $K(M/N) < n$ for all nonzero submodules $N$ of $M$; thus 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 $\text{Lat}(R)$ for the lattice of all right ideals of a ring $R$.

**Lemma 2.3.** Let $R$ and $S$ be rings, with $R$ Noetherian of finite Krull dimension. Let $f : \text{Lat}(R) \rightarrow \text{Lat}(S)$ be an increasing function and let $k, n \in \mathbb{N}$, with $K_R(R) \geq n$. Let $X$ and $Y$ be right ideals of $R$ with $Y \subseteq X$ and suppose $K_R(X/Y) + k \leq K_S(f(X)/f(Y))$ whenever $X/Y$ is $n$-critical. Then $K_R(X/Y) + k \leq K_S(f(X)/f(Y))$ whenever $K_R(X/Y) \geq n$.

In particular, $K_R(R) + k \leq K_S(S)$.

**Proof.** This follows from [7], 6.1.17. \hfill $\square$

### 3 Main Results

We now proceed to prove the main theorems stated in the introduction. We prove Theorem C in Section 3.1; the argument is a straightforward induction based on Nakayama’s Lemma and is different to the one used by Walker in [10].

Theorem A is proved in Section 3.2, where we also consider the length function $\lambda(g)$ of a finite dimensional Lie algebra $g$. It is also shown that Corollary A follows from Theorem A.

The remainder of the paper is devoted to proving Theorem B.

#### 3.1 Reduction to $\Omega_G$

Let $R$ be a ring. 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 $m \in M$. 5
The following result summarizes various elementary properties of modules.

**Lemma 3.1.** Let $x$ be a normal element of a ring $R$ and let $B \subseteq A$ be right $R$-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 $K(B/Bx) \leq K(A/Ax)$.

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

The main step comes next.

**Lemma 3.2.** Let $R$ be a right Noetherian ring, $x$ a normal element of $J(R)$. Suppose $M$ is a finitely generated $x$-torsion free $R$-module with finite Krull dimension. Then $K(M/Mx) \geq K(M) - 1$.

**Proof.** Proceed by induction on $K(M) = \beta$. Note that $\beta \geq 1$ since $M$ is $x$-torsion free. Since $x \in J(R)$, the base case $\beta = 1$ 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 also $x$-torsion free by Lemma 3.1(a). Hence, by Lemma 3.1(b), $K(M/Mx) \geq K(N/Nx)$.

Since $M$ is $x$-torsion free and $0 < N \subseteq M$, $N$ is also $x$-torsion free. Hence, by Lemma 3.1(c), $K(N/Nx) = K(N/Nx^n)$ 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 $N/Nx^n \hookrightarrow N/M_{i+1}$ and $K(N/Nx^n) \geq K(N/M_{i+1})$.

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

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

Consider the chain

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

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

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

6
\[
\frac{M_i + Mx}{M_i + 1 + Mx} \cong \frac{M_i}{(M_i + 1 + Mx) \cap M_i} = \frac{M_i}{M_i + 1 + (M_i \cap Mx)}.
\]

Since \(M/M_i\) is \(x\)-torsion free by Lemma 3.1 (a), \(M_i \cap Mx = M_i x\) by Lemma 3.1(b), so every factor of (†) has Krull dimension \(\geq \beta - 2\). Hence \(K(M/Mx) \geq \beta - 1 = K(M) - 1\).

\[\square\]

Proof of Theorem C. Since \(x\) is right regular, \(R\) is \(x\)-torsion free. By Lemma 3.1 (c), the chain \(R > xR > \ldots > x^kR > \ldots\) has infinitely many factors with Krull dimension equal to \(K(R/xR)\), so \(K(R) = K(R/xR)\). The result follows from Lemma 3.2.

\[\square\]

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.

### 3.2 A lower bound for the Krull dimension

**Proposition 3.3.** 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 \(\Omega G\).

(ii) \(K(\Omega_H) < K(\Omega_G)\).

Proof. (i) Since \(\mathbb{F}_p \cong \Omega_H / J_H\) and since \(- \otimes_{\Omega H} \Omega G\) is flat by Lemma 4.5 of [2], we see that \(M \cong \Omega_G / J_H \Omega_G\) as right \(\Omega_G\)-modules.

Suppose \(M\) is Artinian. Then \(J_{G_m} \subseteq J_H \Omega_G\) for some \(m \geq 1\), by Proposition 2.2. 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 \(f : \text{Lat}(\Omega_H) \to \text{Lat}(\Omega_G)\), given by \(I \mapsto I \otimes_{\Omega_H} \Omega_G\). Suppose \(X\) and \(Y\) are right ideals of \(R\) such that \(Y \subseteq X\) and such that \(X/Y\) is simple. Since \(\Omega_H\) 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 \(\Omega_G\) is a flat \(\Omega_H\)-module. As \(M\) is not Artinian by part (i), \(K(f(X)/f(Y)) \geq 1\), so by Lemma 2.3 \(K(\Omega_H) + 1 \leq K(\Omega_G)\), as required.

\[\square\]

Note that the analogous proposition for universal enveloping algebras is false: for example, the Verma module of highest weight zero for \(\mathfrak{g} = sl_2(\mathbb{C})\) is Artinian, and indeed, \(K(\mathcal{U}(\mathfrak{g})) = K(\mathcal{U}(\mathfrak{b})) = 2\), where \(\mathfrak{b}\) is a Borel subalgebra of \(\mathfrak{g}\).

We can now give a proof of the first result stated in the Introduction:
Proof of Theorem A. By Theorem C, it is sufficient to show $\lambda(g) \leq K(\Omega_G) \leq d$, where $d = \text{dim } g$. First, we show that $\lambda(g) \leq K(\Omega_G)$.

Proceed by induction on $\lambda(g)$. Let $0 = g_0 < g_1 < \ldots < g_k = g$ be a chain of maximal length $k = \lambda(g)$ in $g$.

We can find a closed uniform subgroup $H$ of $G$ with Lie algebra $g_{k-1}$. Since $g_{k-1} < g$, $|G:H| = \infty$.

By the inductive hypothesis, $k - 1 = \lambda(g_{k-1}) \leq K(\Omega_H)$. By Proposition 3.3, $K(\Omega_H) < K(\Omega_G)$, so $k = \lambda(g) \leq K(\Omega_G)$.

By Lemma 2.1, we see that $\Omega_G$ is a complete filtered ring with $\text{gr } \Omega_G \cong \mathbb{F}_p[X_1, \ldots, X_d]$. It follows from Proposition 7.1.2 of Chapter I of [6] and Corollary 6.4.8 of [7] that $K(\Omega_G) \leq K(\text{gr } \Omega_G) = d$, as required.

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

Proposition 3.4. Let $g$ be a finite dimensional Lie algebra over a field $k$.

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

(ii) If $g$ is solvable, $\lambda(g) = \text{dim}_k(g)$.

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

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

Proof. (i) Putting together two chains of maximal length in $h$ and $g/h$ shows that $\lambda(g) \geq \lambda(h) + \lambda(g/h)$. The reverse inequality follows by considering the chains $0 = g_0 \cap h \subseteq \ldots \subseteq g_i \cap h \subseteq \ldots \subseteq h$ and $h \subseteq g_1 + h \subseteq \ldots \subseteq g_i + h \subseteq \ldots \subseteq g$ whenever $0 = g_0 < \ldots < g_i < \ldots < g_n = g$ is a chain of subalgebras of maximal length in $g$.

(ii) This follows directly from (i).

(iii) Let $l = \text{dim } t$. Given a Borel subalgebra $b$, there are exactly $2^l$ parabolic subalgebras containing it, corresponding 1-1 with the subsets of the set of simple roots of $g$. This correspondence preserves inclusions, so we can find a chain of subalgebras of length $l$ starting with $b$. Combining this together with a maximal chain of length $\text{dim } b$ in $b$ gives the result.

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

Proof of Corollary A. This now follows directly from Theorem A and Proposition 3.4.
3.3 An upper bound

The method of proof of Theorem B 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 $K(\mathfrak{U}(g))$ when $g$ is semisimple:

**Theorem 3.5 (Smith).** Let $g$ be a complex semisimple Lie algebra. Let $2r + 1$ be the dimension of the largest Heisenberg Lie algebra contained in $g$. Then $K(\mathfrak{U}(g)) \leq \dim g - r - 1$.

**Proof.** See Corollary 4.3 of [8], bearing in mind the comments contained in section 3.1 of that paper. □

**Definition 3.6.** Let $k$ be a field. The Heisenberg $k$-Lie algebra of dimension $2r + 1$ is defined by the presentation

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

Here $\delta_{ij}$ is the Kronecker delta.

First we establish a useful fact about uniform pro-$p$ groups $H$ with $\mathbb{Q}_p$-Lie algebra isomorphic to a Heisenberg Lie algebra.

**Lemma 3.7.** Let $H$ be a uniform pro-$p$ group such that $L(H)$ is isomorphic to $\mathfrak{h}_{2r+1}$. Let the centre $Z(H)$ of $H$ be topologically generated by $z$. Then there exist $x, y \in H$ and $k \in \mathbb{N}$ such that $[x, y] = z^p k$.

**Proof.** By Theorem 9.10 of [5], we may assume that the group law on $H$ is given by the Campbell-Hausdorff formula on $L(H)$. Let $(,)$ denote the Lie bracket on $L(H) = \mathfrak{h}_{2r+1}$.

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

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

(†)

Now as $\mathbb{Q}_pL_H = \mathfrak{h}_{2r+1}$ there exists $n \in \mathbb{N}$ such that $p^nu_1, p^nv_1 \in L_H$, whence $(p^nu_1, p^nv_1) \in L_H \cap \mathbb{Q}_p \mathbb{Z}_p = \mathbb{Z}_p \mathbb{Z}_p$. Hence $(p^nu_1, p^nv_1) = p^k \lambda z$ for some unit $\lambda \in \mathbb{Z}_p$ and some $k \in \mathbb{N}$, an equation inside $L_H$. We may now take $x = p^nu_1, y = p^nv_1$ and apply (†). □
Next we develop some dimension theory for finitely generated $\Omega_G$-modules, where $G$ is an arbitrary uniform pro-$p$ group. Recall that the $J_G$-adic filtration on $\Omega_G$ gives rise to a polynomial associated graded ring.

**Definition 3.8.** Let $M$ be a finitely generated $\Omega_G$-module, equipped with some good filtration $F M$. The characteristic ideal of $M$ is defined to be

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

The graded dimension of $M$ is defined to be

$$d(M) := \mathcal{K}(\text{gr} \, \Omega_G / J(M)).$$

Lemma 4.1.9 of Chapter III of [6] shows that $J(M)$ and hence $d(M)$ does not depend on the choice of a good filtration for $M$. It is easy to prove that $d(M) = \mathcal{K}(\text{gr} \, M)$ for any good filtration $F M$ on $M$.

Let $\mathfrak{h}$ be a $\mathbb{Q}_p$-Lie subalgebra of $\mathfrak{g}$, the $\mathbb{Q}_p$-Lie algebra of $G$. Let $H = \mathfrak{h} \cap L_G$; since $L_G/H$ injects into $\mathfrak{g}/\mathfrak{h}$ which is torsion-free, we see that $H$ is actually a closed uniform subgroup of $G$, by Theorem 7.15 of [5].

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

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

**Proposition 3.9.** 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 isolated uniform subgroup of $G$ with Lie algebra $\mathfrak{h}_3$.

Let $Z = Z(H) = \langle z \rangle$, say. Let $M$ be a finitely generated $\Omega_G$-module such that $d(M) \leq 1$. Then $\sigma(z - 1) \in J(M)$.

**Proof.** Let $A$ be a uniform subgroup of $G$ with torsion-free $L_G/L_A$. Using Theorem 7.23(ii) of [5] it is easy to check that the subspace filtration on $\Omega_A$ induced from the $J_G$-adic filtration on $\Omega_G$ coincides with the $J_A$-adic filtration.

It follows that the Rees ring $\Omega_A$ of $\Omega_A$ embeds into $\widehat{\Omega_G}$ and that $\Omega_A \cap t \widehat{\Omega_G} = t \Omega_A$, so this embedding induces a natural embedding of graded rings

$$\text{gr} \, \Omega_A = \Omega_A / t \Omega_A \hookrightarrow \widehat{\Omega_G} / t \widehat{\Omega_G} = \text{gr} \, \Omega_G.$$

It’s easy to see that $L_H/L_Z$ is torsion-free. Since $L_G/L_H$ is torsion-free by assumption on $H$, $L_G/L_Z$ is also torsion-free so the above discussion applies to both $Z$ and $H$.

Now, equip $M$ with a good filtration $F M$ and consider the Rees module $\widehat{\Omega_G} M$. This is an $\Omega_H$-module, so we can view it as an $\Omega_H$-module by restriction.
Let $S = \tilde{\Omega}_Z - t\tilde{\Omega}_Z$. This is a central multiplicatively closed subset of the domain $\tilde{\Omega}_H$, so we may form the localisations $\tilde{\Omega}_Z S^{-1} \hookrightarrow \tilde{\Omega}_H S^{-1}$ and the localised $\tilde{\Omega}_H S^{-1}$-module $\tilde{M} S^{-1}$.

Let $R = \lim_{\leftarrow} \tilde{\Omega}_Z S^{-1}/t^n\tilde{\Omega}_Z S^{-1}$ and let $N = \lim_{\rightarrow} \tilde{M} S^{-1}/t^n\tilde{M} S^{-1}$.

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

Now, consider the $t$-adic filtration on $R$. It’s easy to see that $R/tR = \tilde{\Omega}_Z S^{-1}/t\tilde{\Omega}_Z S^{-1} \cong \text{gr} \Omega_Z\tilde{\Omega}_Z^{-1}$, where $\tilde{\Omega}_Z = \text{gr} \Omega_Z - \{0\}$. Thus $R/tR \cong k$, the field of fractions of $\text{gr} \Omega_Z$.

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

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

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 $N/tN \cong t^n N/t^{n+1} N \cong \text{gr} M\tilde{\Omega}_Z^{-1}$. Hence

$$\text{gr}_t N = \bigoplus_{n=0}^{\infty} \frac{t^n N}{t^{n+1} N} \cong (\text{gr} M\tilde{\Omega}_Z^{-1}) \otimes_k k[s].$$

Now, because $d(M) \leq 1$, $\text{gr} M\tilde{\Omega}_Z^{-1}$ is finite dimensional over $k$. It follows that $\text{gr}_t N$ is a finitely generated $\text{gr}_t R$-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 5.7 of Chapter I of [6], $N$ is finitely generated over $R$.

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

Hence $R$ is a commutative PID 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 $h_3$, so by Lemma 3.7 we can find elements $x, y \in H$ such that $[x, y] = z^{p^k}$ for some $k \geq 1$.

Hence $\rho(x) \rho(y) = \rho(\rho(z)^{p^k} = z^{p^k} I$. Taking determinants yields $z^{kn} = 1$.

Since $Z = \mathbb{F}_p \cong \mathbb{Z}_p$, this is only possible if $n = 0$.

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

The above result 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 $M$. When $g$ is itself a Heisenberg Lie algebra, a stronger result has been proved by Wadsley ([9], Theorem B):

**Theorem 3.10.** Let $G$ be a uniform pro-$p$ group with $\mathbb{Q}_p$-Lie algebra $h_{2r+1}$ and let $M$ be a finitely generated $\Omega G$-module. If $d(M) \leq r$, then $\text{Ann}_{\Omega G} (M) \cap \Omega Z \neq 0$, where $Z = Z(G)$.

We are tempted to conjecture that the following generalization of Proposition 3.9 holds:

**Conjecture.** Let $G$ be a uniform pro-$p$ group with $\mathbb{Q}_p$-Lie algebra $g$ such that $h_{2r+1} \subseteq g$. Let $H$ be the isolated uniform subgroup of $G$ with Lie algebra $h_{2r+1}$ and let $Z = Z(H) = \langle z \rangle$, say. Let $M$ be a finitely generated $\Omega G$-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 [8] 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 $K(\Omega G)$ from $\dim g - 1$ to $\dim g - r$, when $G$ is as in Theorem B.

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 $\text{Aut}(G)$ 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 $\text{Inn}(G)$ is trivial, so we see that $G/G_2$ is naturally an $\mathbb{F}_p[\text{Out}(G)]$-module.

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

**Lemma 3.11.** The map $\phi : G/G_2 \rightarrow J/J^2$ given by $\phi(gG_2) = \sigma(g - 1) = g - 1 + J^2$ is an isomorphism of $\mathbb{F}_p[\text{Out}(G)]$-modules.
Proof. It is easy to check that \( \varphi \) is an \( F_p \)-linear map preserving the \( \text{Out}(G) \)-structure.

Now \( \{g_1 G_2, \ldots, g_d G_2\} \) is a basis for \( G/G_2 \), if \( \{g_1, \ldots, g_d\} \) is a topological generating set for \( G \). By Theorem 7.24 of [5], \( \{X_1, \ldots, X_d\} \) is a basis for \( J/J^2 \), where \( X_i = \sigma(g_i - 1) = \varphi(g_i G_2) \). The result follows.

**Theorem 3.12.** Let \( G, H, z \) be as in Proposition 3.9. Suppose \( z G_2 \) generates the \( F_p[\text{Out}(G)] \)-module \( G/G_2 \). Then

(i) \( \Omega_G \) has no finitely generated modules \( M \) with \( d(M) = 1 \)

(ii) \( K(\Omega_G) \leq \dim g - 1 \).

**Proof.** Let \( M \) be a finitely generated \( \Omega_G \)-module with \( d(M) \leq 1 \). By Lemma 3.11, \( G/G_2 \cong J/J^2 \) as \( F_p[\text{Out}(G)] \)-modules. Because \( z G_2 \) generates \( G/G_2 \),

\[ \varphi(z G_2) = \sigma(z - 1) \in J/J^2 \text{ generates } J/J^2. \]

In other words, \( F_p \cdot \{\sigma(z - 1)^\alpha : \alpha \in \text{Out}(G)\} \subseteq J/J^2 \).

Let \( \theta \in \text{Aut}(G) \). By Proposition 3.9 applied to \( H^\theta, \sigma(z^\theta - 1) = \sigma(z - 1)^\theta \in J(M) \), where \( ^\theta : \text{Aut}(G) \rightarrow \text{Out}(G) \) is the natural surjection.

Hence \( J/J^2 = F_p \cdot \{\sigma(z - 1)^\alpha : \alpha \in \text{Out}(G)\} \subseteq J(M) \). This forces

\[ (X_1, \ldots, X_d) \subseteq J(M) \subseteq F_p[X_1, \ldots, X_d] = \text{gr } \Omega_G, \]

whence \( d(M) = 0 \) and part (i) follows.

Consider the increasing map \( \text{gr} : \text{Lat}(\Omega_G) \rightarrow \text{Lat}(\text{gr } \Omega_G) \), where we endow each right ideal of \( \Omega_G \) with the subspace filtration from the \( J_G \)-adic filtration on \( G \). If \( X, Y \leq \Omega_G \) are such that \( M = X/Y \) is 1-critical, then \( K(\text{gr } M) = K(\text{gr } X/\text{gr } Y) \geq 1 \), giving \( M \) the subquotient filtration from \( \Omega_G \).

Now, by Proposition 1.2.3 of Chapter II of [6], this subquotient filtration is good, since \( \Omega_G \) is a complete filtered ring with Noetherian \( \text{gr } \Omega_G \). Hence \( K(\text{gr } M) = d(M) \geq 1 \) by the remarks following Definition 3.8. By part (i), \( K(\text{gr } X/\text{gr } Y) \geq 2 \) so part (ii) follows from Lemma 2.3.

We will use this result to deduce Theorem B.

### 3.4 Chevalley groups over \( \mathbb{Z}_p \)

We recall some facts from the theory of Chevalley groups:

Let \( X \in \{A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2\} \) be an indecomposable root system and let \( R \) be a commutative ring. Let \( \mathcal{B} = \{h_r : r \in \Pi\} \cup \{e_r : r \in X\} \) be the Chevalley basis for the \( R \)-Lie algebra \( X_R \).
Let \( X(R) = \langle x_r(t) : r \in X, t \in R \rangle \subseteq \text{Aut}(X_R) \) be the adjoint Chevalley group over \( R \). Here \( x_r(t) \in \text{Aut}(X_R) \) is given by

\[
x_r(t).e_r = e_r \\
x_r(t).e_{-r} = e_{-r} + t h_r - t^2 e_r \\
x_r(t).h_s = h_s - A_{sr} t e_r \\
x_r(t).e_s = \sum_{i=0}^{b} M_{r,s,i} t^i e_{ir+s}
\]

where \( s \in X \) is a root linearly independent from \( r, a \in \mathbb{N} \) is the largest integer such that \( s - ar \in X \), \( b \in \mathbb{N} \) is the largest integer such that \( s + br \in X \), \( A_{sr} = \frac{2(s,r)}{(r,r)} \) and \( M_{r,s,i} = \pm \binom{a+i}{i} \).

Let \( R^* \) denote the group of units of \( R \). When \( t \in R^* \) and \( r \in X \), define

\[
n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t) \quad \text{and} \quad h_r(t) = n_r(t)n_r(-1).
\]

The actions of \( h_r(t) \) and \( n_r = n_r(1) \) on \( X_R \) are as follows:

\[
\begin{align*}
h_r(t).h_s &= h_s, \quad s \in \Pi \\
h_r(t).e_s &= t^{A_{sr}} e_s, \quad s \in X \\
n_r.h_s &= h_{w_r(s)} \\
n_r.e_s &= \eta_r e_{w_r(s)}
\end{align*}
\]

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

The Steinberg relations hold in \( X(R) \):

\[
\begin{align*}
h_r(t_1)h_r(t_2) &= h_r(t_1 t_2), & t_1, t_2 & \in R^*, r \in X \\
x_r(t)x_s(u)x_r(t)^{-1} &= x_s(u), & t, u, s & \in R, r, s \in X \\
h_s(u)x_r(t)h_s(u)^{-1} &= x_r(u^{A_{sr} t}), & t & \in R^*, u \in R^*, r, s \in X.
\end{align*}
\]

Here \( C_{ijrs} \) are certain integers such that \( C_{11rs} = M_{r,s,i} \).

For more details on the above, see [3].

Now, consider the \( \mathbb{Z}_p \)-Lie algebra \( X_{\mathbb{Z}_p} \). Since \([pX_{\mathbb{Z}_p}, pX_{\mathbb{Z}_p}] = p^2[X_{\mathbb{Z}_p}, X_{\mathbb{Z}_p}] \subseteq p^p X_{\mathbb{Z}_p} \), we see that \( pX_{\mathbb{Z}_p} \) is a powerful \( \mathbb{Z}_p \)-Lie algebra. Let \( Y = (pX_{\mathbb{Z}_p}, \ast) \) be the uniform pro-\( p \) group constructed from \( pX_{\mathbb{Z}_p} \) using the Campbell-Hausdorff formula.

We have a group homomorphism \( \text{Ad} : Y \to GL(pX_{\mathbb{Z}_p}) \) given by \( \text{Ad}(g)(u) = g u g^{-1} \). It is shown in Exercise 9.10 of [5] that

\[
\text{Ad} = \exp \circ \text{ad}
\]

where \( \exp : \mathfrak{gl}(pX_{\mathbb{Z}_p}) \to GL(pX_{\mathbb{Z}_p}) \) is the exponential map.

It’s clear that \( \ker \text{Ad} = Z(Y) \). Since the Lie algebra \( X_{\mathbb{Q}_p} \) of \( Y \) is simple, it’s easy to see that \( L(Z(Y)) = Z(L(Y)) = 0 \); hence \( \ker \text{Ad} = 1 \) and \( \text{Ad} \) is an injection.
Lemma 3.13. Let $N = \text{Ad}(Y)$ and $G = X(Z_p)$. Then $N \trianglelefteq G$.

Proof. First we show that $N \subseteq G$. It’s clear that the $\mathbb{Z}_p$-linear action of $N$ on $pX_{Z_p}$ extends naturally to a $\mathbb{Z}_p$-linear action of $N$ on $X_{Z_p}$. Now, direct computation shows that

$$\text{Ad}(te_r) = x_r(t), \quad t \in p\mathbb{Z}_p, r \in X$$

and

$$\text{Ad}(th_r) = h_r(\exp(t)), \quad t \in p\mathbb{Z}_p, r \in \Pi.$$ 

Hence $\text{Ad}(pu\mathbb{Z}_p) \subseteq G$ for all $u \in B$. The set $p\mathcal{B}$ is a $\mathbb{Z}_p$-basis for $pX_{Z_p}$ and hence a topological generating set for $Y$ by Theorem 9.8 of [5]. By Proposition 3.7 of [5], $Y$ is equal to the product of the procyclic subgroups $pu\mathbb{Z}_p$ as $u$ ranges over $B$. Hence $N \subseteq G$.

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

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

and

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

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

Hence $N \trianglelefteq G$, as required. \hfill \Box

Theorem 3.14. Let $G, N$ be as in Lemma 3.13. There exists a commutative diagram of group homomorphisms:

$$
\begin{array}{cccc}
G & \overset{\alpha}{\longrightarrow} & X(F_p) & \overset{\iota}{\longrightarrow} & \text{Aut}(X_{F_p}) \\
\beta \downarrow & & & \downarrow \phi^* \\
\text{Aut}(N) & \overset{\pi}{\longrightarrow} & \text{Out}(N) & \overset{\gamma}{\longrightarrow} & \text{Aut}(N/N_2)
\end{array}
$$

Proof. We begin by defining all the relevant maps. Any automorphism $f$ of $X_{Z_p}$ must fix $pX_{Z_p}$ and hence induces an automorphism $\alpha(f)$ of $X_{F_p} \cong X_{Z_p}/pX_{Z_p}$. It’s clear from the definition of the Chevalley groups that $\alpha(x_r(t)) = x_r(\bar{t})$ where $\bar{t} : \mathbb{Z}_p \to F_p$ is reduction mod $p$ and that $\alpha$ is a surjection.

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

We have observed in the remarks preceding Lemma 3.11 that $\text{Out}(N)$ acts naturally on $N/N_2$; we denote this action by $\gamma$. By Lemma 3.13 $N$ is normal in $G$, and we denote the conjugation action of $G$ on $N$ by $\beta$. 

15
Finally, \( \iota \) is the natural injection of \( X(F_p) \) into \( \text{Aut}(X_{E_p}) \) and \( \pi \) is the natural projection of \( \text{Aut}(N) \) onto \( \text{Out}(N) \).

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

\[
\varphi^* \iota \alpha(x_r(t))(\text{Ad}(pe_s)N_2) = \varphi^*(x_r(\overline{t}))(\text{Ad}(pe_s)N_2) = \varphi(x_r(\overline{t})(e_s)) = \varphi(\sum_{i=0}^{b} M_{r,s,i} t^i e_{ir+s}) = \prod_{i=0}^{b} \text{Ad}(pM_{r,s,i} t^i)N_2 = \prod_{i=0}^{b} x_{ir+s}(pM_{r,s,i} t^i)N_2, (\dagger)
\]

using the definition of the action of \( x_r(\overline{t}) \) on \( X_{E_p} \). On the other hand,

\[
\gamma \pi \beta(x_r(t))(\text{Ad}(pe_s)N_2) = x_r(t)x_s(p)x_r(-t)N_2 = x_s(p) \prod_{i,j>0} x_{ir+js}(C_{ijr}t^ip^j)N_2,
\]

using the Steinberg relations.

Since \( x_\alpha(p^2) \in N_2 \) for any \( \alpha \in X \), we see that all the terms in the above product with \( j > 1 \) vanish, and the remaining expression is equal to the result of (\dagger), since \( C_{i1r}s = M_{r,s,i} \).

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

The above theorem shows that the action of \( \text{Out}(N) \) on \( N/N_2 \) which was of interest in the preceding section is linked to the natural action of \( X(F_p) \) on \( X_{E_p} \).

Since \( \alpha \) is surjective, we see that if \( c_r \) generates \( X_{E_p} \) as an \( F_p[X(F_p)] \)-module, then \( \text{Ad}(pe_r)N_2 \) generates \( N/N_2 \) as an \( F_p[\text{Out}(N)] \)-module. We drop the bars in the following proposition.

**Proposition 3.15.** Suppose \( p \geq 5 \) and let \( R = F_p[X(F_p)] \). Then \( X_{E_p} = R.e_r \) for any \( r \in X \).

**Proof.** This is probably well known and is purely a matter of computation. 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 [3], we can choose \(w \in W\) such that \(w(r) \in \Pi\). Hence \(n_w.h_r = h_{w(r)} \in R.e_r\).

Let \(\alpha, \beta\) be adjacent fundamental roots. Then \(n_{\alpha}.h_{\beta} = h_{\alpha}(\beta) = h_{\beta} - A_{\beta\alpha}h_{\alpha}\) where \(A_{\beta\alpha} = -1, -2\) or \(-3\). The condition on \(p\) implies that if \(h_{\beta} \in R.e_r\) then \(h_{\alpha} \in R.e_r\) also.

Since \(X\) is indecomposable, \(h_{\alpha} \subseteq R.e_r\) for any \(\alpha \in \Pi\). Since the fundamental coroots span the Cartan subalgebra, \(h_{s} \in R.e_r\) 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 \(X_{F_{p}}\), the result follows. \(\Box\)

The condition on \(p\) in the above proposition can be relaxed somewhat - it might even be the case that it can be dropped altogether. Since this is a small detail of no interest to us, we restrict ourselves to the case \(p \geq 5\).

We can finally provide a proof of our main result.

**Proof of Theorem B.** In view of Theorem C and Lemma 2.1, it is sufficient to prove that

\[
\dim \mathfrak{b} + \dim \mathfrak{t} \leq K(\Omega G) \leq \dim \mathfrak{g} - 1.
\]

Note that the lower bound on \(K(\Omega G)\) follows from Proposition 3.4 and Theorem A.

Let \(X\) be the root system of \(\mathfrak{g}\); thus \(\mathfrak{g} = X_{Q_{p}}\). 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 \(h_{3}\) with centre \(Q_{p}e_{r+s}\).

Let \(N\) be the uniform pro-\(p\) group appearing in the statement of Theorem 3.14. By construction, \(\mathfrak{g}\) is the Lie algebra of \(N\). By Proposition 3.15 and the remarks preceding it, we see that \(Ad(p_{r+s})N_{2} \in N/N_{2}\) generates the \(F_{p}[Out(N)]\)-module \(N/N_{2}\). Hence \(K(\Omega N) \leq \dim \mathfrak{g} - 1\) by Theorem 3.12.

Since the Lie algebra of \(G\) is \(\mathfrak{g} = Q_{p}L_{G} = Q_{p}L_{N}\), we see that \(N \cap G\) is an open subgroup of both \(N\) and \(G\), whence \(K(\Omega G) = K(\Omega N) \leq \dim \mathfrak{g} - 1\), as required. \(\Box\)

**Proof of Corollary B.** It is readily seen that \(G\) is a uniform pro-\(p\) group with \(Q_{p}\)-Lie algebra \(\mathfrak{sl}(Q_{p})\) which is split simple over \(Q_{p}\). We have observed in Lemma 2.1 that \(\Lambda_{G}\) is a local right Noetherian ring whose Jacobson radical satisfies the right Artin Rees Property, and that \(\operatorname{gld}(\Lambda_{G}) = \dim \mathfrak{g} + 1 = 9\).
If \( b \) and \( t \) denote the Borel and Cartan subalgebras of \( g \), then \( \dim b = 5 \) and \( \dim t = 2 \). The result follows from Theorems B and C.

References


