Thesis

Longer Nilpotent Series for Classical Unipotent Groups

Submitted by

Josh Maglione

Department of Mathematics

In partial fulfullment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Fall 2013

Master's Committee:

Advisor: James Wilson

Alexander Hulpke
Christina Boucher

Abstract

Longer Nilpotent Series for Classical Unipotent Groups

We compute the adjoint series for the unipotent subgroup, U, of the Chevalley group $A_d(\mathbb{Z}_p)$. The adjoint series of U has length $d^2/4 + d/2 + \Theta(1)$, whose factors have order equal to either p or p^2, whereas the lower central series of U has length $d + 1$, whose factors have order equal to $p^{O(d)}$. We provide an algorithm for computing the adjoint series.

Acknowledgements

Thanks to J. B. Wilson and A. Hulpke for helpful feedback and discussion, and to C. Boucher for helpful comments regarding the algorithm. The author appreciates Leif Anderson and Dan Brake for their help in formatting this document.

Table of Contents

CHAPTER I

Introduction

When trying to determine the automorphisms of a group G, one often turns to a characteristic series of G to constrain the possible automorphisms of G. There are a few standard characteristic series for a nilpotent group described in [7], but for p-groups, these descriptions tend to be either verbal or marginal subgroups of G. An important association with a series of G is its Lie algebra, whose bracket is typically given as commutation in G.

Provided certain conditions hold for a series of G, we can form a Lie algebra with respect to that series. When considering automorphisms of a group, the associated Lie algebra of G is a natural object to study, because automorphisms of G induce automorphisms of the Lie algebra. Surveys of more properties and relationships between a group and its associated Lie algebra can be found in [7, Chapter 3] and [6, Section 5.6]. Finding longer characteristic series of G yields (possibly) two immediate benefits: more constraints on the automorphism group and smaller dimensions of each graded component of its associated Lie algebra (provided the series has an associated Lie algebra). Thus, longer characteristic series for G allow us to better understand the automorphisms of G.

We use Wilson's definition of an *adjoint series* in [12] and refine a characteristic series of G starting with the lower central series (while starting with the Leedham-Green series, defined in [4], seems more logical, we will see that it is identical to the lower central series). At the cornerstone of this definition is the associated Lie algebra of the group, and because of this, our description of characteristic subgroups is independent of the group's presentation.

The paper is organized in the following order. First, we recall results established by Wilson in [12] about filters. In section II, we describe the construction of the adjoint series,

and we prove that it is in fact characteristic. In section III, we provide initial results for the classical Chevalley groups in Proposition III.1.7, and we focus our attention on type A to prove the following theorem.

(I.0.1) Theorem. *Let U be the unipotent subgroup of $A_d(\mathbb{Z}_p)$. The adjoint series of U is a characteristic series and whose length is $d^2/4 + d/2 + \Theta(1)$ and whose factors have order at most p^2. Furthermore, the associated Lie algebra, $L(\alpha)$ is $\mathbb{N}^m$-graded, where $m = \lceil \frac{d}{2} \rceil$.*

Note that the adjoint series is as long as could be expected from the results of Weir and Gibbs. We describe characteristic subgroups that are defined for arbitrary p-groups. We then conclude section III by showing that these subgroups correspond to the classifications of Weir [11] and Gibbs [5] of characteristic subgroups unipotent groups of classical type. In this sense, our method offers a description of these characteristic subgroups which is independent of root systems and representations. Finally, in Section IV, we provide an experimental algorithm to compute the adjoint series of a group and we discuss its complexity.

I.1. Notation

We take $\mathbb{N}$ to be all the nonnegative integers, and for a set S, denote the power set of S by 2^S. Let G be a group. For $x, y \in G$, we let $[x, y]$ denote $x^{-1}y^{-1}xy$. In general, we define $[x_1] = x_1$ and $[x_1, x_2, ..., x_n, x_{n+1}] = [[x_1, ..., x_n], x_{n+1}]$. We say a commutator with n entries has *weight* n. If $H, K \leq G$, then $[H, K] = \langle [h, k] : h \in H, k \in K \rangle$. We use the same recursive notation for subgroups of G as we do with elements of G. We let $\mathbb{Z}_p$ denote $\mathbb{Z}/p\mathbb{Z}$ for some prime p. Denote e_i to be the k-tuple with 1 in the i^{th} component and 0 elsewhere.

We adopt the same notation for root systems and Chevalley groups as provided by Carter in [2, Chapters 2 – 4]. That is, we let Φ denote a system of roots. Define an ordering of

the roots so that Φ^+ and Φ^- denote the positive and negative roots respectively. Let Π be the set of fundamental roots of Φ, and let $\{h_r : r \in \Pi\} \cup \{e_s : s \in \Phi\}$ be a Chevalley basis for the Lie algebra $\mathfrak{g}$ over $\mathbb{C}$ for some Cartan decomposition. The Chevalley group of type $\mathfrak{g}$ over $\mathbb{Z}_p$, denoted $\mathfrak{g}(\mathbb{Z}_p)$, is the group of automorphisms of the Lie algebra $\mathfrak{g}_{\mathbb{Z}_p} = \mathfrak{g} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ generated by $x_r(t)$, for all $r \in \Phi$ and for all $t \in \mathbb{Z}_p$, where

$$x_r(t) = \exp(t \text{ ad } e_r).$$

The root subgroup of r is $X_r = \langle x_r(t) : t \in \mathbb{Z}_p \rangle$. The unipotent subgroup of $\mathfrak{g}(\mathbb{Z}_p)$, denoted by U, is conjugate to the group generated by all X_r, for $r \in \Phi^+$.

I.2. Filters

Let M be a commutative monoid. As defined in [12], a *filter* of G is a function $\theta : M \to 2^G$ such that $\theta_m \leq G$ for all $m \in M$, $\theta_0 = G$, and

$$(\forall s, t \in M) \qquad [\theta_s, \theta_t] \leq \theta_{s+t} \leq \theta_s \cap \theta_t.$$

Note that an *N-series* of a group G, as introduced by Lazard [8], is a filter where $M = \mathbb{N}$ and $N_0 = G$. Note that $\theta_m \trianglelefteq G$ for all $m \in M$.

Every filter induces a new filter $\partial\theta : M \to 2^G$ given by

$$(\partial\theta)_m = \prod_{s \in M - \{0\}} \theta_{m+s}.$$

Note that

$$[(\partial\theta)_m, \theta_m] = \prod_{s\in M-\{0\}} [\theta_{m+s}, \theta_m] = \prod_{s\in M-\{0\}} \theta_{2m+s} \leq \prod_{s\in M-\{0\}} \theta_m \cap \theta_{m+s} \leq \theta_m.$$

Therefore, $(\partial\theta)_m \trianglelefteq \theta_m$. Let $L_0 = 0$ and define $L_m = \theta_m/(\partial\theta)_m$ for all $m \in M - \{0\}$. Thus, by [12, Theorem 3.3], the abelian group, $L(\theta) = \bigoplus_{m\in M} L_m$, is a Lie ring with product on the homogeneous components

(I.2.1) $$(\forall x \in \theta_s, \forall y \in \theta_t) \qquad [(\partial\theta)_s x, (\partial\theta)_t y] = (\partial\theta)_{s+t}[x, y].$$

Note that if θ is a filter such that θ produces an N-series of G, then $\partial\theta$ is also an N-series and $(\partial\theta)_m = N_{m+1}$. Therefore, $L(\theta)$ is the Lie ring described by Lazard cf. [8, Theorem 2.1].

Suppose $\mathcal{S}$ generates M. Let $\mathcal{G} = \mathcal{G}(M, \mathcal{S})$ be the (directed) Cayley graph whose vertices are M and whose labeled edge set is $\{m \xrightarrow{s} n : m + s = n, s \in \mathcal{S}\}$. Furthermore, let $\mathcal{G}_m^n$ denote the set of all paths, t, from vertex m to vertex n in $\mathcal{G}$. We write a path t as a sequence of edge labels the path traverses. That is, for each $s_i \in \mathcal{S}$, $t = (s_1, ..., s_k)$ where $m + s_1 + \cdots + s_k = n$. For simplicity, we write $[\pi_t]$ to denote $[\pi_{s_1}, ..., \pi_{s_k}]$, for $t = (s_1, ..., s_k)$. Given a function $\pi : \mathcal{S} \to 2^G$, define a new function $\bar{\pi} : M \to 2^G$ by

(I.2.2) $$(\forall m \in M) \qquad \bar{\pi}_m = \prod_{t\in\mathcal{G}_0^m} [\pi_t].$$

We regard a function π as generating a filter, $\bar{\pi}$, provided M and π satisfy some conditions. For our purposes, $M = \mathbb{N}^k$ for some integer k, and such an M satisfies all the required

conditions (a conical monoid with decomposition). Define $\prec$ on M so that

(I.2.3) if $m \prec n$, then there exists $c \in M$ such that $m + c = n$,

for all $m, n \in M$. Thus, if $m \prec n$ implies $\pi_m \geq \pi_n$ and π maps into the normal subgroups of G, then $\bar{\pi} : \mathbb{N}^k \to 2^G$, as defined in (I.2.2), is a filter. Note that $\bar{\pi}$ is a series, provided the image of π is totally ordered with $\leq$ [12, Theorem 3.11]. For a more detailed exposition of filters and their properties see [12, Section 3].

CHAPTER II

Constructing the Lex-Least Stable Adjoint Series

To produce the stable lex-least adjoint refinement, which we call the *adjoint series* (or α-*series*), we iterate the below process until the series stabilizes. This construction is first done by Wilson in [12, Section 4], and is done with arbitrary commutative monoids. However, for our purposes, we only need to be concerned with the monoid $\mathbb{N}^k$.

Let θ be a filter from $\mathbb{N}$ into the subgroups of G, and set $\alpha_n^{(1)} = \theta_n$ for all $n \in \mathbb{N}$. In our construction, we use the lower central series of G, which is only defined on $\mathbb{Z}^+$, as a filter. This construction allows for the opportunity to record operators at the top of the filter, θ_0, even though we take θ_0 to be G. We define the $\alpha^{(1)}$-series to be the filter $\alpha^{(1)} : \mathbb{N} \to 2^G$, and in general, the $\alpha^{(k)}$-series is the filter $\alpha^{(k)} : \mathbb{N}^k \to 2^G$.

As established in Section I.2, if $n \in \mathbb{N}^k$, then $L_n^{(k)} = \alpha_n^{(k)}/\alpha_{n+e_k}^{(k)}$ is the homogenous component of the Lie algebra $L(\alpha^{(k)})$. Thus, to obtain the $\alpha^{(k+1)}$-series from the $\alpha^{(k)}$-series for $k \geq 1$, we first construct a biadditive map (bimap) on the graded component $L_{e_1}^{(k)}$. Define $\circ : L_{e_1}^{(k)} \times L_{e_1}^{(k)} \to L_{2e_1}^{(k)}$ where

$$\textbf{(II.0.4)} \qquad \left(\forall x, y \in \alpha_{e_1}^{(k)}\right) \qquad \alpha_{e_1+e_k}^{(k)} x \circ \alpha_{e_1+e_k}^{(k)} y = \alpha_{2e_1+e_k}^{(k)}[x, y].$$

We see that $\circ$ is indeed a bimap since each homogeneous component is abelain. Given a bimap $\diamond : U \times V \to W$, define the *ring of adjoints* to be

$$\mathrm{Adj}\,(\diamond) = \{(f, g) \in \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}} : uf \diamond v = u \diamond gv, \forall u \in U, \forall v \in V\}.$$

See [14, Section 2] for further details on adjoints.

Let J be the Jacobson radical of $\mathrm{Adj}\,(\circ)$, and let $J^0 = \mathrm{Adj}\,(\circ)$. Recursively define $J^{i+1} = J^i J$ for all $i \in \mathbb{N}$. Note that $\alpha^{(k)}_{e_i} = G$ for all $i = 1, 2, ..., k$. Therefore, the first place to (possibly) insert a new subgroup is between $\alpha^{(k)}_{e_1}$ and $\alpha^{(k)}_{e_1+e_k}$. To this end, let $n \in \mathbb{N}$, define τ_n so that $\alpha^{(k)}_{e_1} \geq \tau_n \geq \alpha^{(k)}_{e_1+e_k}$ and

(II.0.5) $$\tau_n / \alpha^{(k)}_{e_1+e_k} = L^{(k)}_{e_1} J^n.$$

For $n = (n_1, ..., n_{k+1})$, define

(II.0.6) $$\pi_n = \begin{cases} \alpha^{(k)}_{(n_1,...,n_k)} & \text{if } (n_1, ..., n_k) \neq e_1, \\ \tau_{n_{k+1}} & \text{if } (n_1, ..., n_k) = e_1. \end{cases}$$

We note that π is a function from $\mathbb{N}^{k+1}$ into the normal subgroups of G (which is totally ordered with respect to $\leq$), but is not necessarily a filter of G.

Now we seek to determine the filter that π generates. To this end, define

(II.0.7) $$\mathcal{S}_t = \{e_1, e_1 + e_i : 2 \leq i \leq t\} \cup \{(0, n_2, ..., n_t) : n_i \in \mathbb{N}\},$$

so that $\mathcal{S}_{k+1}$ generates $\mathbb{N}^{k+1}$, and hence, we define $\alpha^{(k+1)}_n = \bar{\pi}_n$, as in (I.2.2), which gives us the $\alpha^{(k+1)}$-series of G.

Before proceeding to specific groups, we wish to prove that the adjoint series is a characteristic series. To this end, define the *pseudo-isometries* of $\circ$, as in (II.0.4), as

$$\Psi\,\mathrm{Isom}\,(\circ) = \left\{(h, \hat{h}) \in \mathrm{Aut}\left(L^{(k)}_{e_1}\right) \times \mathrm{Aut}\left(L^{(k)}_{2e_1}\right) : xh \circ hy = (x \circ y)\hat{h}\right\}.$$

(II.0.8) Lemma. $\Psi\,\mathrm{Isom}\,(\circ)$ *acts on* $\mathrm{Adj}\,(\circ)$ *by*

$$(f,g)^{(h,\hat{h})} = (h^{-1}fh, hgh^{-1}) \in \mathrm{Adj}\,(\circ)\,,$$

for $(f,g) \in \mathrm{Adj}\,(\circ)$ *and* $(h,\hat{h}) \in \Psi\,\mathrm{Isom}\,(\circ)$. *Furthermore, this action is faithful.*

Proof: Let $x, y \in L_{e_1}^{(k)}$. It follows that $\Psi\,\mathrm{Isom}\,(\circ)$ acts on $\mathrm{Adj}\,(\circ)$ as

$$xh^{-1}fh \circ y = (xh^{-1}f \circ h^{-1}y)\hat{h} = (xh^{-1} \circ gh^{-1}y)\hat{h} = x \circ hgh^{-1}y.$$

It follows that this action is faithful because h and $\hat{h}$ are automorphisms cf. [13, Proposition 4.16]. □

(II.0.9) Proposition. If the initial filter, $\theta : \mathbb{N} \to 2^G$, is a characteristic series, then the adjoint series of G is a characteristic series.

Proof: Note that $\mathrm{Aut}\,(G)$ maps into $\Psi\,\mathrm{Isom}\,(\circ)$ cf. [13, Proposition 3.8]. Therefore, by Lemma II.0.8, $\mathrm{Aut}\,(G)$ acts on $\mathrm{Adj}\,(\circ)$ by conjugation. Furthermore, since J is the intersection of all maximal ideals in $\mathrm{Adj}\,(\circ)$, it follows that the action of $\mathrm{Aut}\,(G)$ fixes J. Thus, J^i is fixed by the action of $\mathrm{Aut}\,(G)$ for every $i \in \mathbb{Z}^+$. Therefore, $L_{e_1}^{(k)}J^n$ is characteristic, and hence, π_n is characteristic for $n \in \mathbb{N}^{k+1}$, provided $\alpha_{(n_1,\ldots,n_k)}^{(k)}$ is characteristic. Since θ_m is characteristic for $m \in \mathbb{N}$, it follows by induction that each term in the $\alpha^{(k+1)}$-series is characteristic. □

CHAPTER III

The Stable Adjoint Refinement of Classical Unipotent Groups

III.1. The Chevalley Groups

In this section we aim to characterize the adjoint series of the unipotent subgroups of Classical Chevalley groups. Indeed, the group of upper unitriangular mactrices ($\mathrm{U}_n(\mathbb{Z}_p)$) is the unipotent subgroup of the Chevalley group $A_{n-1}(\mathbb{Z}_p)$. While this generality may seem unnecessary for an understood matrix group, our intention is to compute the adjoint series of all classical Chevalley groups. This generality allows us to display the computation in a more concise manner. Note that commutation is the backbone of the adjoint series; while computing matrix commutators is not too difficult, computing root subgroup commutators is much more straightforward, thanks to the work of Chevalley [3].

Let U be a unipotent subgroup of the Chevalley group $\mathfrak{g}(\mathbb{Z}_p)$, which is unique up to conjugation. Let γ_k denote the k^{th} term in the lower central series of U (the γ-series), where we let $\gamma_0 = U$. For $n \in \mathbb{N}$, define $\alpha_n^{(1)} = \gamma_n$. Define the map $\circ$ as in (II.0.4).

Let $\{h_r : r \in \Pi\} \cup \{e_s : s \in \Phi\}$ be a Chevalley basis for $\mathfrak{g}$ over $\mathbb{C}$ so that

$$\begin{aligned}
[h_r, h_s] &= 0, \\
[h_r e_s] &= \frac{2(r,s)}{(r,r)} e_s, \\
[e_r, e_{-r}] &= h_r, \\
[e_r, e_s] &= \pm\,(v+1) e_{r+s} \qquad (0 \text{ if } r+s \notin \Phi),
\end{aligned}$$

where v is defined to be the largest nonnegative integer such that $s - vr \in \Phi$. As in [2, Theorem 5.2.2], let $r, s \in \Phi^+$ and $t, u \in \mathbb{Z}_p$, then

(III.1.1) $$[x_s(u), x_r(t)] = \prod_{i,j>0} x_{ir+js}(C_{ijrs}(-t)^i u^j)$$

where the product is taken in increasing order of $i + j$. The constants C_{ijrs} are given by

$$C_{i1rs} = \pm\binom{v+i}{i} \qquad \text{and} \qquad C_{1jrs} = \mp(-1)^j\binom{v+j}{j},$$

where v is the largest nonnegative integer such that $s - vr \in \Phi$. Although we have not described C_{ijrs} for general i and j, we observe that it is impossible for both i and j to be greater than 1, with $\mathfrak{g}$ of type A, B, C, or D; this fact can be seen in (III.1.5) and in Proposition III.1.7. From (III.1.1) we note that the set of all X_r generate U, for $r \in \Pi$. Hence, $U = \langle X_r : r \in \Pi \rangle$.

Note that for every $r \in \Phi^+$, we can write

(III.1.2) $$r = p_{i_1} + \cdots + p_{i_k},$$

for (not necessarily distinct) $p_{i_j} \in \Pi$. Thus, we may talk about the *height* of each (positive) root r denoted $h(r)$ which is the sum of the coefficients of r when written as in (III.1.2). Let U_m denote the subgroup generated by all X_r such that $h(r) \geq m$. As we will see, these subgroups almost always coincide with the lower central series of $U \leq \mathfrak{g}(\mathbb{Z}_p)$.

(III.1.3) Lemma (Gibbs [5]; Levchuk [9]). *Let $\mathfrak{g}(\mathbb{Z}_p)$ be a Chevalley group of rank d and of type A, B, C or D. It follows that if $p \geq 3$ or if $\mathfrak{g}$ is of type A or D, then $\gamma_m = U_m = \langle X_r : h(r) \geq m \rangle$.*

(III.1.4) Remark. Levchuk describes how the lower central series of U is related to the series

$$U = U_1 > U_2 > \cdots > U_\ell = 1$$

in [9], and finds that $\gamma_m \neq U_m$ for some integers m when $p = 2$ for C_d and B_d. Since our aim is to provide examples of the usefulness of the adjoint series, we avoid the troubles of working in characteristic 2 in C_d or B_d. Thus, throughout the paper, if $\mathfrak{g}$ is of type B_d or C_d, then we assume $p \geq 3$. It follows then that $L_i^{(1)} = U_i/U_{i+1}$.

We recognize that for $A_d(\mathbb{Z}_p)$, the description of U_i is more approachable as a matrix rather than root subgroups. However, the Chevalley commutator formula, (III.1.1), gives us a universal way to compare the bimaps of these unipotent groups. We will see that the Chevalley formula allows us to easily show that all the bimaps are the same (for types A, B, C, and D).

Note that $x_r(t_1)x_r(t_2) = x_r(t_1 + t_2)$, so $(x_r(t))^p = x_r(0) = 1$. Hence, $L_i^{(1)}$ is elementary abelian (thus the lower central series is identical to the Leedham-Green series). Since there are exactly d fundamental roots, $L_1^{(1)} \cong \mathbb{Z}_p^d$ as vector spaces. Furthermore, since there are exactly $d-1$ positive roots with height 2, $L_2^{(1)} \cong \mathbb{Z}_p^{d-1}$ as vector spaces. Therefore, $\circ$ may be regarded as a $\mathbb{Z}_p$-bilinear map, $\circ : \mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^{d-1}$.

We wish to construct the structure constants matrix (Gram matrix) of $\circ$, denoted by M. We denote the fundamental roots, p_i, to be consistent with the Dynkin diagram for $\mathfrak{g}$. That is, p_1 is connected to p_2, p_2 is connected to both p_1 and p_3, etc. The Dynkin diagrams for types A, B, C, and D are given in Figure III.1. Pick an ordering of Π so that $p_i \prec p_j$ provided $i < j$. For constants C_{ijrs} as in (III.1.1), the parity is determined solely by *extra*

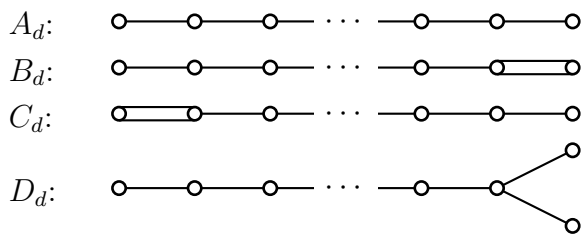

FIGURE III.1. The classical Dynkin diagrams.

special pairs (r, s) as in [2, pg. 58] (as we will see in (III.1.5), these are exactly the non-commuting pairs). For simplicity, if (r, s) is extra special, we let $[e_r, e_s] = -(v+1)e_{r+s}$, where v is defined to be the largest nonnegative integer such that $s - vr \in \Phi$. Thus, for $\mathfrak{g}$ of type A_d,

$$\textbf{(III.1.5)} \qquad [x_{p_i}(s), x_{p_j}(t)] = \begin{cases} x_{p_i+p_j}(st) & \text{if } (p_i, p_j) \text{ is extra special,} \\ x_{p_i+p_j}(-st) & \text{if } (p_j, p_i) \text{ is extra special,} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, $[X_{p_i}, X_{p_j}] = X_{p_i+p_j}$, provided $p_i + p_j \in \Phi^+$.

Define $\varphi_1 : L_1 \to \mathbb{Z}_p^d$ given by $\varphi_1(\gamma_2 x_{p_i}(t)) = te_i$, and define $\varphi_2 : L_2 \to \mathbb{Z}_p^{d-1}$ given by $\varphi_2(\gamma_3 x_{p_i+p_j}(t)) = te_{j-1}$, provided $i < j$. Note that both φ_1 and φ_2 are vector space isomorphisms. Define the structure of constants matrix M so that $\varphi_2([X_{p_i}, X_{p_j}]) = e_i M e_j^{\mathrm{T}}$. Thus, by (III.1.5),

$$\textbf{(III.1.6)} \qquad M = \begin{bmatrix} 0 & e_1 & 0 & \cdots & 0 \\ -e_1 & 0 & e_2 & & \vdots \\ 0 & -e_2 & 0 & \ddots & \\ \vdots & & \ddots & \ddots & e_{d-1} \\ 0 & \cdots & & -e_{d-1} & 0 \end{bmatrix}.$$

(III.1.7) Proposition. Let M be the matrix described in (III.1.6). Let M' be the matrix representation of $\circ$ (as in (II.0.4)) for U the unipotent subgroup of $\mathfrak{g}(\mathbb{Z}_p)$, where $\mathfrak{g}$ is of type B, C, or D with rank d. It follows that $M' = M$ for each $\mathfrak{g}$ of type B, C, or D.

Proof: First let $\mathfrak{g}$ be of type B. Then for $i, j = 1, ..., d-1$, $[x_{p_i}(s), x_{p_j}(t)]$ is described by (III.1.5). Furthermore,

$$[x_{p_{d-1}}(s), x_{p_d}(t)] = x_{p_{d-1}+p_d}(st)x_{p_{d-1}+2p_d}(-st^2) \equiv x_{p_{d-1}+p_d}(st) \pmod{\gamma_3}.$$

It follows that for $i, j = 1, ..., d$, $[x_{p_i}(s), x_{p_j}(t)]$ is described by (III.1.5). Thus, the matrix representation of $\circ$ of $U \leq B_d(\mathbb{Z}_p)$ is equal to M as in (III.1.6). A similar argument is applied to $C_d(\mathbb{Z}_p)$ (the only difference with $\mathfrak{g}$ of type C, is that $p_{d-1} + 2p_d$ is not a root, but instead $2p_{d-1} + p_d$ is a root).

Now suppose $\mathfrak{g}$ is of type D. Then for $i, j = 1, ..., d-1$, $[x_{p_i}(s), x_{p_j}(t)]$ is given by (III.1.5). However,

$$[x_{p_{d-2}}(s), x_{p_d}(t)] = x_{p_{d-2}+p_d}(st).$$

Therefore, since $\varphi_2([x_{p_{d-2}}(s), x_{p_d}(t)]) = ste_{d-1}$, it follows that the matrix representation of $\circ$ of $U \leq D_d(\mathbb{Z}_p)$ is given by (III.1.6). $\square$

(III.1.8) Corollary. *Let $L = L(\gamma)$, the Lie algebra associated to the lower central series of U of type either A, B, C, or D. Then L/L^3 are all isomorphic.*

Define $M_i \in \mathrm{M}_d(\mathbb{Z}_p)$ to be the matrix with 1 in the $i, (i+1)$ entry, -1 in the $(i+1), i$ entry, and 0 elsewhere. Therefore, $M = \sum_{i=1}^{d-1} e_i M_i$.

(III.1.9) Lemma. $\mathrm{Adj}\,(M_1) = \left\{ \left(\begin{bmatrix} w & x & * \\ y & z & * \\ 0 & 0 & * \end{bmatrix}, \begin{bmatrix} z & -x & * \\ -y & w & * \\ 0 & 0 & * \end{bmatrix} \right) : w, x, y, z \in \mathbb{Z}_p \right\}$

Proof: $(F, G) \in \mathrm{Adj}\,(M_1)$ if, and only if, $FM_1 = M_1 G^{\mathrm{T}}$. □

Note that we can obtain M_i from M_1 by applying a permutation. Applying such a permutation also permutes the adjoint ring, and therefore

(III.1.10) $$\mathrm{Adj}\,(M_i) = \left\{ \left(\begin{bmatrix} * & 0 & 0 & * \\ * & w & x & * \\ * & y & z & * \\ * & 0 & 0 & * \end{bmatrix}, \begin{bmatrix} * & 0 & 0 & * \\ * & z & -x & * \\ * & -y & w & * \\ * & 0 & 0 & * \end{bmatrix} \right) : w, x, y, z \in \mathbb{Z}_p \right\}.$$

Observe that $\mathrm{Adj}\,(M) = \mathrm{Adj}\left(\sum_{i=1}^{d-1} e_i M_i\right) = \bigcap_{i=1}^{d-1} \mathrm{Adj}\,(M_i)$. As i and j vary, we see from (III.1.10) that $F_{ij} = G_{ij} = 0$ for $i \neq j$ except when (i, j) equals $(2, 1)$ or $(d-1, d)$. Note that in this case, $F_{ij} = -G_{ij}$. Also, $F_{ii} = F_{(i+2)(i+2)} = G_{(i+1)(i+1)}$ for all i. Furthermore, all matrices (F, G) of this form are an adjoint for M. Therefore, this characterizes $\mathrm{Adj}\,(M)$.

Now, we wish to characterize the Jacobson radical of $\mathrm{Adj}\,(M)$, but the structure of it is much easier seen in a different basis. To this end, let $H = \langle H_i : H_i = X_{p_{2i}} \rangle$ and $K = \langle K_i : K_i = X_{p_{2i-1}} \rangle$. For $s = \left\lfloor \frac{d}{2} \right\rfloor$ and $t = \left\lceil \frac{d}{2} \right\rceil$, let $\mathcal{B}_1 = \{H_1, H_2, ..., H_s, K_1, K_2, ..., K_t\}$. Note that $\mathcal{B}_1$ is an ordered basis for L_1 and $[H_i, H_j] = 0$ and $[K_i, K_j] = 0$, for all i and j. Thus, the permutation associated with the change of basis permutes $\mathrm{Adj}\,(M)$. And hence,

if d is even, then

(III.1.11) $$\mathrm{Adj}\,(M) = \left\{ \left(\begin{bmatrix} wI_s & xE_{11} \\ yE_{ss} & zI_s \end{bmatrix}, \begin{bmatrix} zI_s & -xE_{11} \\ -yE_{ss} & wI_s \end{bmatrix} \right) : w, x, y, z \in \mathbb{Z}_p \right\}.$$

However, if d is odd, then

(III.1.12)
$$\mathrm{Adj}\,(M) = \left\{ \left(\begin{bmatrix} wI_s & xE_{11} + yE_{st} \\ 0_{ts} & zI_t \end{bmatrix}, \begin{bmatrix} zI_s & -xE_{11} - yE_{st} \\ 0_{ts} & wI_t \end{bmatrix} \right) : w, x, y, z \in \mathbb{Z}_p \right\}.$$

Note that E_{ij} is the matrix with a 1 in the i, j entry and 0 elsewhere, whose dimension is given by the context.

(III.1.13) Lemma. *Let* $s = \left\lfloor \frac{d}{2} \right\rfloor$ *and* $t = \left\lceil \frac{d}{2} \right\rceil$. *For* $\mathrm{Adj}\,(M)$ *as in* (III.1.11) *and* (III.1.12), *let* J *be the Jacobson radical of* $\mathrm{Adj}\,(M)$. *It follows that for even* d,

$$J = \left\{ \left(\begin{bmatrix} 0_s & xE_{11} \\ yE_{ss} & 0_s \end{bmatrix}, \begin{bmatrix} 0_s & -xE_{11} \\ -yE_{ss} & 0_s \end{bmatrix} \right) : x, y \in \mathbb{Z}_p \right\},$$

and for odd d,

$$J = \left\{ \left(\begin{bmatrix} 0_s & xE_{11} + yE_{st} \\ 0_{ts} & 0_t \end{bmatrix}, \begin{bmatrix} 0_s & -xE_{11} - yE_{st} \\ 0_{ts} & 0_t \end{bmatrix} \right) : x, y \in \mathbb{Z}_p \right\}.$$

Proof: For d even, note that

$$I_1 = \left\{ \left(\begin{bmatrix} wI_s & xE_{11} \\ yE_{ss} & 0_s \end{bmatrix}, \begin{bmatrix} 0_s & -xE_{11} \\ -yE_{ss} & wI_s \end{bmatrix} \right) : x, y \in \mathbb{Z}_p \right\}$$

and

$$I_2 = \left\{ \left(\begin{bmatrix} 0_s & xE_{11} \\ yE_{ss} & zI_s \end{bmatrix}, \begin{bmatrix} zI_s & -xE_{11} \\ -yE_{ss} & 0_s \end{bmatrix} \right) : x, y \in \mathbb{Z}_p \right\}$$

are maximal ideals of $\mathrm{Adj}\,(M)$. Thus, $J \subseteq I_1 \cap I_2$. Since $\mathrm{Adj}\,(M)$ is Artinian, $J(\mathrm{Adj}\,(M)) = nil(\mathrm{Adj}\,(M))$. Note that $I_1 \cap I_2$ is nilpotent, and hence $I_1 \cap I_2 \subseteq J$. A similar argument is applied when d is odd. Therefore, the lemma follows. □

It will be useful to see how the permutation, associated with the change in basis from $\mathcal{B}_1$ to the standard basis, permutes J. If $s = \left\lfloor \frac{d}{2} \right\rfloor$ and $t = \left\lceil \frac{d}{2} \right\rceil$, then

(III.1.14)
$$J = \left\{ \left(\begin{bmatrix} xE_{21} & 0_{st} \\ 0_{ts} & yE_{(t-1)t} \end{bmatrix}, \begin{bmatrix} -xE_{21} & 0_{st} \\ 0_{ts} & -yE_{(t-1)t} \end{bmatrix} \right) : x, y \in \mathbb{Z}_p \right\}.$$

Note that in (III.1.14), the shape of J does not drastically change based on the parity of d.

III.2. Preliminary Construction for the Adjoint Series of the Unipotent Subgroups of $A_d(\mathbb{Z}_p)$.

We have already done most of the work for the $\alpha^{(2)}$-series in section III.1. For $n \in \mathbb{N}$ and J as in Lemma III.1.13, define τ_n so that $\gamma_1 \geq \tau_n \geq \gamma_2$ and $\tau_n/\gamma_2 = L_1 J^n$. Note that $J^2 = 0$, so that $\tau_k = \tau_{k+1} = \gamma_2$, for $k \geq 2$. For $(m, n) \in \mathbb{N}^2$, define $\pi_{(m,n)}$ as in (II.0.6). Thus, $\pi_{(1,0)} = \gamma_1$ and

(III.2.1)
$$\pi_{(1,1)} = \tau_1 = \langle X_{p_1}, X_{p_d}, \gamma_2 \rangle.$$

For $m \neq 1$, $\pi_{(m,n)} = \gamma_m$, for all $n \in \mathbb{N}$. Recall from (II.0.7) that $\mathcal{S}_2 = \{e_1, e_2, e_1 + e_2, n \cdot e_2 : n \in \mathbb{Z}^+\}$, and that $\mathcal{G}_0^{(m,n)}$ is the set of all paths from 0 to the vertex (m, n). Thus,

(III.2.2) $$\alpha^{(2)}_{(m,n)} = \prod_{t \in \mathcal{G}_0^{(m,n)}} [\pi_t]\,.$$

Before we start working towards the adjoint series of these groups, we state a lemma which will facilitate computations.

(III.2.3) Lemma. *Let π and π' be subgroups of U containing root subgroups of height one. If $X_r \leq [\pi, \pi']$, with $h(r) = 2$, then $r = p_i + p_j$, where $X_{p_i} \leq \pi$ and $X_{p_j} \leq \pi'$ for some i and j.*

Of course we extend Lemma III.2.3 by induction to work on commutators of weight n. Indeed, the majority of the computation is considering the possible contributions (of fundamental roots) for each entry in the commutator. Before we prove the following lemma, we seek to simplify notation slightly. Let

$$X_{ij} = X_{p_i + p_{i+1} + \cdots + p_{i+j-1}},$$

so that $X_{23} = X_{p_2+p_3+p_4}$.

(III.2.4) Lemma. *Let U be the unipotent subgroup of $A_d(\mathbb{Z}_p)$. For all m and $n \in \mathbb{N}$,*

$$\alpha^{(2)}_{(m,n)} = \begin{cases} \langle X_{1m}, X_{(d-m+1)m}, \gamma_{m+1} \rangle & \text{if } 1 \leq m \leq d \text{ and } n = 1, \\ \gamma_k & \text{otherwise,} \end{cases}$$

for some $k \in \mathbb{N}$.

Proof: From (II.0.6) and (III.2.2), we deduce that $\alpha^{(2)}_{(0,n)} = U$ and $\alpha^{(2)}_{(n,0)} = \gamma_n$ for all $n \in \mathbb{N}$. Furthermore, $\alpha^{(2)}_{(d+1,n)} = 1$ for all $n \in \mathbb{N}$ since every commutator has weight at least $d+1$. Since

$$\alpha^{(2)}_{(m,n)} \geq \left[\pi_{(1,0)}, ..., \pi_{(1,0)}, \pi_{(0,n)}\right] = \gamma_{m+1},$$

we need only look at the commutators of weight m to determine $\alpha^{(2)}_{(m,n)}$. Note that every label in a given path $t \in \mathcal{G}_0^{(m,n)}$ corresponds either to $\pi_{(1,1)}$, given in (III.2.1), or to $\pi_{(1,0)} = \pi_{(0,k)} = \gamma_1$, for all $k \in \mathbb{N}$. Because of this, every commutator of weight m will have entries equal to γ_1 or $\pi_{(1,1)}$.

Suppose $1 \leq m \leq d$ and $n = 1$. If $m = 1$, then by (III.2.1), we are done, so suppose $m \geq 2$. Thus, $\alpha^{(2)}_{(m,1)}$ has commutators of weight m equal to either

(III.2.5) $$[\gamma_{m-1}, \pi_{(1,1)}], \qquad [\gamma_k, \pi_{(1,1)}, \gamma_1, ..., \gamma_1], \qquad \text{or} \qquad [\pi_{(1,1)}, \gamma_1, ..., \gamma_1],$$

for some $1 \leq k \leq m-2$. Since each commutator contains exactly one entry equal to $\pi_{(1,1)}$ and since $U \leq A_d(\mathbb{Z}_p)$, it follows from (III.1.1) that all commutators in (III.2.5) are equal. Hence, $\alpha^{(2)}_{(m,1)} = [\gamma_{m-1}, \pi_{(1,1)}]$.

Suppose $1 \leq m \leq d$ and $2 \leq n$. Then each commutator of weight m will contain at least two entries equal to $\pi_{(1,1)}$. Therefore, if $X_r \leq \alpha^{(2)}_{(m,n)}$ with $h(r) = m$, then r must contain p_1 and p_d as summands. This is impossible for $m \leq d-1$. Thus, if $m \leq d-1$, $\alpha^{(2)}_{(m,n)} = \gamma_{m+1}$. However, if $m = d$ and $n = 2$, then $X_r = X_{1d} = \gamma_d$ with $h(r) = d$; thus, $\alpha^{(2)}_{(d,2)} = \gamma_d$. If $n \geq 3$, then every commutator of weight m must contain at least three entries equal to $\pi_{(1,1)}$. Hence, if $X_r \in \alpha^{(2)}_{(m,n)}$ with $n \geq 3$ and $h(r) = m$, r must contain three summands equal to either p_1 or p_d, which is impossible in a root system of type A. Thus, $\alpha^{(2)}_{(m,n)} = \gamma_{m+1}$ for $n \geq 3$. Hence, the statement of the lemma follows. $\square$

(III.2.6) Example. $G = A_5(\mathbb{Z}_p)$.

The $\alpha^{(2)}$-series of U is

$$U > \begin{bmatrix} 1 & * & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & * \\ & & & & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & * \\ & & & & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & * & * & * \\ & 1 & . & * & * \\ & & 1 & . & * \\ & & & 1 & * \\ & & & & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ & 1 & . & . & * \\ & & 1 & . & * \\ & & & 1 & . \\ & & & & 1 \end{bmatrix}$$
$$> \begin{bmatrix} 1 & . & . & * & * \\ & 1 & . & . & * \\ & & 1 & . & * \\ & & & 1 & . \\ & & & & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ & 1 & . & . & * \\ & & 1 & . & . \\ & & & 1 & . \\ & & & & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & . & * \\ & 1 & . & . & . \\ & & 1 & . & . \\ & & & 1 & . \\ & & & & 1 \end{bmatrix} > 1.$$

(III.2.7) Corollary. *Let U be the unipotent subgroup of $A_d(\mathbb{Z}_p)$. The $\alpha^{(2)}$-series of U includes $d-2$ subgroups not included in the lower centeral sereis of U.*

Proof: By Lemma III.2.4, $\alpha^{(2)}_{(d-1,1)} = \gamma_{d-1}$ and $\alpha^{(2)}_{(d,1)} = \gamma_d$. Suppose that $m \leq d-2$. In this case, each $\alpha^{(2)}_{(m,1)}$ contains at most two root subgroups which are not contained in γ_{m+1}. Thus, $\gamma_m > \alpha^{(2)}_{(m,1)} > \gamma_{m+1}$, provided $1 \leq m \leq d-2$. Hence, the $\alpha^{(2)}$-series has added $d-2$ more characteristic subgroups to the lower central series. □

The length of the $\alpha^{(2)}$-series of U is $2d-1$. Thus, after just one iteration, we have nearly doubled the length of the lower central series of U.

III.3. Constructing the Adjoint Series of the Unipotent Subgroup of $A_d(\mathbb{Z}_p)$.

Now we wish to generalize the process of computing the $\alpha^{(2)}$ terms (from the terms of the lower central series). Computing the next iteration, the $\alpha^{(k+1)}$-series of $A_d(\mathbb{Z}_p)$, is equivalent to computing the $\alpha^{(2)}$-series of $A_{d'}(\mathbb{Z}_p)$, for some $d' < d$. The next lemma begins to establish this fact and determines exactly the value of d'.

(III.3.1) Proposition. Suppose U is the unipotent subgroup of $A_d(\mathbb{Z}_p)$, and

$$\alpha^{(k)}_{e_1} = \gamma_1, \qquad \alpha^{(k)}_{e_1+e_k} = \left\langle X_{(k-1)1}, X_{(d-k+2)1}, \alpha^{(k-1)}_{e_1+e_{k-1}} \right\rangle,$$
$$\alpha^{(k)}_{2e_1} = \gamma_2, \qquad \alpha^{(k)}_{2e_1+e_k} = \left\langle X_{(k-1)2}, X_{(d-k+1)2}, \alpha^{(k-1)}_{2e_1+e_{k-1}} \right\rangle,$$

for some $k \geq 2$. It follows that M, the matrix representation of $\circ$ given in (II.0.4), is described in (III.1.6) and is a $d-2(k-1)$ by $d-2(k-1)$ matrix over $\mathbb{Z}_p^{d-2k+1}$.

Proof: Let V be the unipotent subgroup of $A_{d-2(k-1)}(\mathbb{Z}_p)$, with fundamental roots labeled $p_k, p_{k+1}, ..., p_{d-k+1}$. By assumption,

$$\alpha_{e_1}^{(k)}/\alpha_{e_1+e_k}^{(k)} = \langle X_{i1} : k \leq i \leq d-k+1 \rangle = \gamma_1(V)/\gamma_2(V),$$

$$\alpha_{2e_1}^{(k)}/\alpha_{2e_1+e_k}^{(k)} = \langle X_{i2} : k \leq i \leq d-k \rangle = \gamma_2(V)/\gamma_3(V).$$

Thus, commutation in $\alpha_{e_1}^{(k)}/\alpha_{e_1+e_k}^{(k)}$ is equivalent to commutation in $\gamma_1(U)/\gamma_2(U)$ with fundamental roots $p_1, ..., p_{k-1}$ and $p_{d-k+2}, ..., p_d$ removed. Hence, we may regard $\circ$ as a $\mathbb{Z}_p$-bilinear map from $\gamma_1(V)/\gamma_2(V) \times \gamma_1(V)/\gamma_2(V)$ to $\gamma_2(V)/\gamma_3(V)$. Thus, we have the same M except that we have removed $e_1, ..., e_{k-1}$ and $e_{d-k+1}, ..., e_{d-1}$, and the statement follows. $\square$

(III.3.2) Corollary. *Let U be the unipotent subgroup of $A_d(\mathbb{Z}_p)$. For all $1 \leq m \leq d$,*

(III.3.3)
$$\alpha_{me_1+e_{k+1}}^{(k+1)} = \left\langle X_{km}, X_{(d-k-m+2)m}, \alpha_{me_1+e_k}^{(k)} \right\rangle.$$

Furthermore, the $\alpha^{(k)}$-series of U is the adjoint series for $k = \lceil \frac{d}{2} \rceil$, and this is the smallest such k.

Proof: For $k = 1$, (III.3.3) holds. Suppose (III.3.3) holds for $k \geq 1$. Proposition III.3.1 tells us exactly the structure of M. Let V be the unipotent subgroup of $A_{d-2(k-1)}(\mathbb{Z}_p)$, with fundamental roots labeled $p_k, p_{k+1}, ..., p_{d-k+1}$. Let $\beta_{(m,n)}^{(2)}$ be the (m,n) term of the $\alpha^{(2)}$-series of V. Thus, the new subgroup between $\alpha_{me_1}^{(k)}$ and $\alpha_{me_1+e_k}^{(k)}$ is determined by $\beta_{(m,1)}^{(2)}$. By Lemma

III.2.4,

$$\beta^{(2)}_{(m,1)} = \left\langle X_{km}, X_{(d-k-m+2)m}, \gamma_{m+1}(V) \right\rangle .$$

Therefore,

$$\alpha^{(k+1)}_{me_1+e_{k+1}} = \left\langle X_{km}, X_{(d-k-m+2)m}, \alpha^{(k)}_{me_1+e_k} \right\rangle .$$

From Proposition III.3.1 we get that the $\alpha^{(k+1)}$-series of U is equal to the $\alpha^{(k)}$-series of U when $k = \left\lceil \frac{d}{2} \right\rceil$ because M has trivial Jacobson radical. □

(III.3.4) Remark. Note that the subgroup described in Corollary III.3.2 is the only subgroup obtained between $\alpha^{(k)}_{me_1} = \gamma_m$ and $\alpha^{(k)}_{me_1+e_k}$. This is completely determined by the Jacobson radical of the adjoint algebra, and by the fact that there is at most one subgroup between γ_m and γ_{m+1} in Lemma III.2.4.

All that is left to do is show that if $\alpha^{(k+1)}_n$ is a subgroup not included in the $\alpha^{(k)}$-series, then it must be the subgroup described in Corollary III.3.2. For the following lemma, we use the fact that automorphisms of $\mathbb{Z}_p$ induce automorphisms of $\mathfrak{g}(\mathbb{Z}_p)$. Indeed, if $\tau \in \mathrm{Aut}\,(\mathbb{Z}_p)$, then the map $\varphi : \mathfrak{g}(\mathbb{Z}_p) \to \mathfrak{g}(\mathbb{Z}_p)$ given by $x_r(t)\varphi = x_r(\tau(t))$ is an automorphism of $\mathfrak{g}(\mathbb{Z}_p)$ cf. [2, pg. 200].

(III.3.5) Lemma. *Let U be the unipotent subgroup of $A_d(\mathbb{Z}_p)$, and let $n = (n_1, ..., n_{k+1}) \in \mathbb{N}^{k+1}$. If $n_{k+1} \geq 2$, then $\alpha^{(k+1)}_n = \alpha^{(k)}_m$ for some $m \in \mathbb{N}^k$.*

Proof: This is certainly true for $k = 1$ (Lemma III.2.4), so suppose this holds for $k \geq 1$. If $n_{k+1} \geq 2$, then $n_1e_1 + e_{k+1} \prec n$ ($\prec$ defined in (I.2.3) on page 5). Therefore, $\alpha^{(k+1)}_n \leq \alpha^{(k+1)}_{n_1e_1+e_{k+1}}$. From Corollary III.3.2, $\alpha^{(k+1)}_n < \alpha^{(k+1)}_{n_1e_1+e_{k+1}}$.

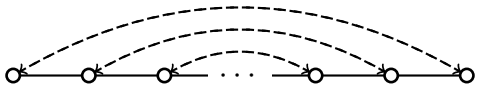

FIGURE III.2. The nontrivial graph automorphism of A_d.

Suppose that $\alpha_n^{(k+1)} \neq \alpha_m^{(k)}$ for all $m \in \mathbb{N}^k$. Thus, it is strictly between $\alpha_{n_1e_1+e_c}^{(c)}$ and $\alpha_{n_1e_1+e_{c-1}}^{(c-1)}$, for $2 \leq c \leq k$ because $\gamma_{n_1+1} < \alpha_n^{(k+1)} < \alpha_{n_1e_1+e_{k+1}}^{(k+1)}$. By Proposition II.0.9, $\alpha_n^{(k+1)}$ is characteristic, so if $x_r(t) \in \alpha_n^{(k+1)}$, then $X_r \leq \alpha_n^{(k+1)}$ because field automorphisms induce group automorphisms. Note that $\alpha_n^{(k+1)}$ must then contain exactly one root subgroup not contained in $\alpha_{n_1e_1+e_{c-1}}^{(c-1)}$ since $\alpha_{n_1e_1+e_c}^{(c)}/\alpha_{n_1e_1+e_{c-1}}^{(c-1)} \leq p^2$; call this root subgroup X_r, for some $r \in \Phi^+$. However, X_r must be held invariant or mapped to another root subgroup by the automorphisms induced by the graph automorphisms of the Dynkin diagram.

For $A_d(\mathbb{Z}_p)$, the Dynkin diagram has an automorphism group isomorphic to $\mathbb{Z}_2$ as seen in Figure III.2. Note under our assumptions, $\alpha_n^{(k+1)} = \left\langle X_r, \alpha_{n_1e_1+e_{c-1}}^{(c-1)} \right\rangle$. Since $\alpha_{n_1e_1+e_{c-1}}^{(c-1)}$ is characteristic, X_r must be held invariant by graph automorphisms. It follows that

$$r = p_{(d+1)/2-i} + \cdots + p_{(d+1)/2} + \cdots + p_{(d+1)/2+i},$$

if d is odd or

$$r = p_{d/2-i} + \cdots + p_{d/2} + p_{d/2+1} + \cdots + p_{d/2+1+i},$$

if d is even. However, from Corollary (III.3.2), this is impossible. Thus, the lemma follows.

□

(III.3.6) Proposition. Let U be the unipotent subgroup of $A_d(\mathbb{Z}_p)$, and let $k \geq 1$. If $n = (n_1, ..., n_{k+1}) \in \mathbb{N}^{k+1}$, then

$$\alpha_n^{(k+1)} = \begin{cases} \left\langle X_{kn_1}, X_{(d-k-n_1+2)n_1}, \alpha^{(k)}_{n_1e_1+e_k} \right\rangle & \text{if } n = n_1e_1 + e_{k+1}, \\ \alpha_m^{(k)} & \text{otherwise,} \end{cases}$$

for some $m \in \mathbb{N}^k$.

Proof: If $n_1 = 0$, then $\alpha_n^{(k+1)} \geq [\pi_n] = U$. Furthermore, if $n_1 \geq d+1$, then every commutator of $\alpha_n^{(k+1)}$ has weight at least $d+1$. Hence, $\alpha_n^{(k+1)} = 1$ in this case. Now suppose $1 \leq n_1 \leq d$. We will classify each case based on the value of n_{k+1}.

Assume that $n_{k+1} = 0$, and let $\mathcal{G} = \mathcal{G}(\mathbb{N}^{k+1}, \mathcal{S}_{k+1})$. If $t \in \mathcal{G}_0^n$, then the edges that the path t traverses are in the subgraph $\mathcal{G}(\mathbb{N}^k \times \{0\}, \mathcal{S}_k) \cong \mathcal{G}(\mathbb{N}^k, \mathcal{S}_k)$. It follows that $\alpha_n^{(k+1)} = \alpha^{(k)}_{(n_1,...,n_k)}$. Suppose $n_{k+1} \geq 2$; by Lemma III.3.5, $\alpha_n^{(k+1)} = \alpha_m^{(k)}$ for some $m \in \mathbb{N}^k$.

Finally, suppose that $n_{k+1} = 1$. If $n = n_1e_1 + e_{k+1}$, then by Corollary III.3.2,

$$\alpha_n^{(k+1)} = \left\langle X_{kn_1}, X_{(d-k-n_1+2)n_1}, \alpha^{(k)}_{n_1e_1+e_k} \right\rangle.$$

Therefore, suppose $n \neq n_1e_1 + e_{k+1}$. Replace every $\pi_{e_1+e_{k+1}}$ with π_{e_1} in every commutator of weight n_1 contained in $\alpha_n^{(k+1)}$. Since $n_{k+1} = 1$, every commutator of weight n_1 must contain exactly one $\pi_{e_1+e_{k+1}}$, so that

$$\alpha_n^{(k+1)} = \prod [\cdots, \pi_{e_1+e_{k+1}}, \cdots]\gamma_{n_1+1} \leq \prod [\cdots, \pi_{e_1}, \cdots]\gamma_{n_1+1} = \alpha^{(k+1)}_{(n_1,...,n_k,0)}.$$

Therefore, $\alpha_n^{(k+1)} \leq \alpha^{(k)}_{(n_1,...,n_k)}$. Since $n \neq n_1e_1+e_{k+1}$, it follows that $\alpha^{(k)}_{(n_1,...,n_k)} < \alpha^{(k+1)}_{n_1e_1+e_{k+1}}$, so $\alpha_n^{(k+1)} < \alpha^{(k+1)}_{n_1e_1+e_{k+1}}$. Apply a similar argument to $\alpha_n^{(k+1)}$ as in the proof of Lemma III.3.5 to

show that $\alpha_n^{(k+1)} = \alpha_m^{(k)}$ for some $m \in \mathbb{N}^k$ since $\alpha_n^{(k+1)}$ is characteristic. Hence, the statement of the proposition follows. $\square$

Now we are ready to prove Theorem I.0.1.

Proof of Theorem I.0.1: Note when constructing the $\alpha^{(k+1)}$-series from the $\alpha^{(k)}$-series, by Proposition III.3.6, we will get new subgroups if, and only if, $\alpha_{e_1+e_k}^{(k+1)}$ is a new subgroup. From Corollary III.3.2, $\alpha_{e_1+e_k}^{(k+1)}$ will be a new subgroup if, and only if, $k \leq \left\lceil \frac{d}{2} \right\rceil - 1$. From Corollary III.2.7, the i^{th} iteration adds $\ell - 3$ new subgroups, where ℓ is the length of the γ-series of V, the unipotent subgroup of $A_{d-2(i-1)}(\mathbb{Z}_p)$. Note that the γ-series of U has exactly $d+1$ subgroups. If $k = \left\lceil \frac{d}{2} \right\rceil$, then the length of the adjoint series is $d + 1 + \sum_{i=2}^{k}(d - 2i + 2)$. Furthermore,

$$\frac{d^2 + 2d + 4}{4} \leq d + 1 + \sum_{i=2}^{k}(d - 2i + 2) \leq \frac{d^2 + 2d + 5}{4}.$$

Also note that by Proposition III.3.6, the order of α_n/α_{n+e_m} is at most 2. Provided $d \geq 4$, then $\alpha_{e_1+e_2}/\alpha_{2e_1}$ has order p^2, by (III.2.1). However, if $V \leq A_3(\mathbb{Z}_p)$, then $\beta_{(1,0)}^{(2)}/\beta_{(1,1)}^{(2)}$ has order p. Therefore, there exists factors of the α-series with order p and p^2. $\square$

(III.3.7) Example. $G = A_4(\mathbb{Z}_p)$.

U has the following γ-series:

$$U > \begin{bmatrix} 1 & . & * & * & * \\ . & 1 & . & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & . & * \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > 1.$$

The α-series of U increases the length of the γ-series by two:

$$U > \begin{bmatrix} 1 & * & * & * & * \\ . & 1 & . & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & * \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & * & * & * \\ . & 1 & . & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & * & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & . & * \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > 1.$$

(III.3.8) Example. $G = A_5(\mathbb{Z}_p)$.

The γ-series of U is

$$U > \begin{bmatrix} 1 & . & * & * & * \\ . & 1 & . & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & . & * \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > 1.$$

The α-series of U, adds 4 more terms to the series, yielding

$$U > \begin{bmatrix} 1 & * & * & * & * \\ . & 1 & * & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & * \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & * & * & * & * \\ . & 1 & * & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & * \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & * & * & * \\ . & 1 & . & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & * \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & * & * & * \\ . & 1 & . & * & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix}$$

$$> \begin{bmatrix} 1 & . & . & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & * \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & * & * \\ . & 1 & . & . & * \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > \begin{bmatrix} 1 & . & . & . & * \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix} > 1.$$

Note that each term of the α-series for $U \leq A_d(\mathbb{Z}_p)$ fits the description of Weir and Gibbs' characteristic subgroups of $U_{d+1}(\mathbb{Z}_p)$.

CHAPTER IV

An algorithm to compute adjoint filters

The goal of this section is to provide an algorithm for experimentation. The process of refining a characteristic series to the adjoint series requires repetition of two vital steps: obtaining new subgroups and generating a filter. Thus, we provide algorithms which can be repeatedly used to obtain the stable adjoint refinement of Section III.

(IV.0.9) Proposition. There exists a polynomial-time algorithm that obtains the new subgroups for adjoint series refinement process.

Proof: We first describe such an algorithm. Given a filter $\alpha^{(k)}$, obtain the adjoint ring of $\circ : L_{e_1}^{(k)} \times L_{e_1}^{(k)} \to L_{2e_1}^{(k)}$ as described in (II.0.4). Then compute its Jacobson radical, J. Finally compute all subgroups $\tau_n = \left\langle L_{e_1}^{(k)} J^n, \alpha_{e_1+e_k}^{(k)} \right\rangle$.

In [1], Brooksbank and Wilson provide a deterministic algorithm that computes the adjoint ring of $\circ$ in $O(d^6 \log^2 p)$ basic operations. Rónyai provides a method for computing the Jacobson radical in polynomial time in [10], and computing τ_n is in polynomial time as well since $L_{e_1}^{(k)} J^n$ is matrix multiplication. □

Now all that is left is to discuss how to generate a filter given a function $\pi : \mathcal{S}_k \to 2^G$, where $\mathcal{S}_k$ is the generating set for $\mathbb{N}^k$ given in (II.0.7). Recall that $\mathcal{G}$ is the Cayley graph $\mathcal{G}(\mathbb{N}^k, \mathcal{S}_k)$, and $\mathcal{G}_0^n$ is the set of paths from vertex 0 to vertex n in $\mathcal{G}$. Then the filter $\bar{\pi}$ generated by π is given by

$$(\forall n \in \mathbb{N}^k) \qquad \bar{\pi}_n = \prod_{t \in \mathcal{G}_0^n} [\pi_t].$$

However, it is not necessary to look at all of $\mathcal{G}_0^n$, for $n = (n_1, ..., n_k) \in \mathbb{N}^k$. Instead, we need only $t \in \mathcal{G}_0^n$, where t is a path of length n_1. To obtain all paths of length n_1, we first observe that we only need to find one path of length n_1.

(IV.0.10) Lemma. *If $t = (t_1, ..., t_{n_1})$ and $s = (s_1, ..., s_{n_1})$ are paths of length n_1 from vertices 0 to n in $\mathcal{G}(\mathbb{N}^k, \mathcal{S}_k)$, then $(t_1, ...t_{n_1}) = (s_{1^\sigma}, ..., s_{n_1^\sigma})$, for some $\sigma \in Sym(n_1)$.*

Proof: Note that since t is a path of length n_1, we have that for all $i \in \{1, ..., n_1\}$, $t_i \neq (0, m_2, ..., m_k)$, where $m_j \in \mathbb{N}$. We prove this by induction on k. It will be useful to (naturally) embed $\mathcal{G}$ into $\mathbb{R}^k$. First, suppose $k = 2$. Then t is a labeled Delannoy path. Since t must contain a maximal amount of labels of the form $\pi_{e_1+e_i}$, it follows that every path from 0 to n has the same labels as t up to rearrangements. In fact, every possible rearrangement of labels of t gives a path of length n_1. □

Therefore, we apply a greedy algorithm to compute one path of length n_1. From that, we take all possible rearrangements, so we have paths of length n_1.

(IV.0.11) Proposition. Given $\pi : \mathcal{S}_k \to 2^G$, there exists an algorithm which computes the generated filter $\bar{\pi} : \mathbb{N}^k \to 2^G$.

Proof: The algorithm runs as follows. For each $n \in \mathbb{N}^k$, with $n_1 \leq c$, where c is the class of G, and $\sum_{i=2}^k n_i \leq n_1$, use a greedy algorithm to obtain all paths of length n_1 from 0 to n in $\mathcal{G}$. Then compute the commutator subgroup of all the labels of each path, and take the product of all such paths together with γ_{n_1+1}.

When the algorithm terminates, the output is indeed the filter $\bar{\pi} : \mathbb{N}^k \to 2^G$. To this end, if $n_1 > c$, then we set $\pi_n = 1$ since $\gamma_c \geq \pi_n$. Recall,

$$\mathcal{S}_k = \{e_1, e_1 + e_i : 2 \leq i \leq k\} \cup \{(0, n_2, ..., n_k) : n_i \in \mathbb{N}\}.$$

If $n_1 \leq c$ but $\sum_{i=2}^{k} n_i > n_1$, then there are no paths of length n_1 from 0 to n in $\mathcal{G}$. Thus, $\pi_n = \gamma_{n_1+1}$. There are a finite number of $n \in \mathbb{N}^k$ with $n_1 \leq c$ and $\sum_{i=2}^{k} n_i \leq n_1$, so the algorithm terminates. □

The initial use of this algorithm was to form and test conjectures. Although it is far from optimal, we believe that the algorithm can be more efficient if we do not look at all paths of length n_1. Indeed, in the proofs in Section III we only used a few key paths. Other examples (Chevalley groups of type B, C, and D) also suggest that it may be enough to look at a subset of all paths of length n_1.

CHAPTER V

Closing Remarks

For the Chevalley group of type A, we see that the length adjoint series of the unipotent subgroup is $d^2/4+d/2+\Theta(1)$ with respect to the rank, d. We have strong evidence that shows that the length of the adjoint series of the unipotent subgroups for types B, C, and D is close to the length for type A. That is, the length of the adjoint series of the unipotent subgroup of the Chevalley groups of type B, C, and D seem to be equal to $\Theta(d^2)$. Furthermore, the orders of almost all the factors is either p or p^2 in these groups.

Although the respective bimaps are the same, this is not enough to say that the structure of the adjoint series is the same. Indeed, evidence indicates that the adjoint series for types B, C, and D seem to be slightly different from type A. However, this does not come as a surprise because we took advantage of the root system structure of type A and of the automorphism group of the Dynkin diagram of type A.

Bibliography

1. Peter A. Brooksbank and James B. Wilson. Intersecting two classical groups. *J. Algebra*, 353:286–297, 2012.
2. Roger W. Carter. *Simple groups of Lie type*. John Wiley & Sons, London-New York-Sydney, 1972. Pure and Applied Mathematics, Vol. 28.
3. C. Chevalley. Sur certains groupes simples. *Tôhoku Math. J. (2)*, 7:14–66, 1955.
4. Bettina Eick. *Charakterisierung und Konstruktion von Frattinigruppen mit Anwendungen in der Konstruktion endlicher Gruppen*. Verlag der Augustinus-Buchh, 1996. Thesis (Ph.D.) – RWTH Aachen University.
5. John A. Gibbs. Automorphisms of certain unipotent groups. *J. Algebra*, 14:203–228, 1970.
6. Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.
7. Evgenii I. Khukhro. *Nilpotent groups and their automorphisms*, volume 8 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1993.
8. Michel Lazard. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. Ecole Norm. Sup. (3)*, 71:101–190, 1954.
9. V. M. Levchuk. Automorphisms of unipotent subgroups of Chevalley groups. *Algebra i Logika*, 29(3):315–338, 381–382, 1990.
10. Lajos Rónyai. Computing the structure of finite algebras. *J. Symbolic Comput.*, 9(3):355–373, 1990.
11. A. J. Weir. Sylow p-subgroups of the general linear group over finite fields of characteristic p. *Proc. Amer. Math. Soc.*, 6:454–464, 1955.

12. James B. Wilson. More characteristic subgroups, lie rings, and isomorphism tests for p-groups (in press). *J. Group Theory*. doi: 0.1515/jgt-2013-0026.

13. James B. Wilson. Decomposing p-groups via Jordan algebras. *J. Algebra*, 322(8):2642–2679, 2009.

14. James B. Wilson. Division, adjoints, and dualities of bilinear maps. *Comm. Algebra*, 41(11):3989–4008, 2013.