On characteristic p Verma modules and subalgebras of the hyperalgebra

Vivi Carstensen

Wolfson College
Oxford

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of Oxford

Trinity Term 1994

Abstract

Vivi Carstensen, Wolfson College, Oxford.
A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of Oxford.
Trinity Term 1994.

On characteristic p Verma modules, and subalgebras of the hyperalgebra

Let $\mathcal{G}$ be a finite dimensional semisimple Lie algebra; we study the class of infinite dimensional representations of $\mathcal{G}$ called characteristic p Verma modules.

To obtain information about the structure of the Verma module $Z(\lambda)$ we find primitive weights μ such that a non-zero homomorphism from $Z(\mu)$ to $Z(\lambda)$ exists. For $\lambda + \rho$ dominant, where ρ is the sum of the fundamental roots, there exist only finitely many primitive weights, and they all appear in a convex, bounded area. In the case of $\lambda + \rho$ not dominant, and the characteristic p a good prime, there exist infinitely many primitive weights for the Lie algebra. For $\mathcal{G} = sl_3$ we explicitly present a large, but not necessarily complete, set of primitive weights. A method to obtain the Verma module as the tensor product of Steinberg modules and Frobenius twisted $Z(\lambda_1)$ is given for certain weights, $\lambda = p^n\lambda_1 + (p^n - 1)\rho$. Furthermore, a result about exact sequences of Weyl modules is carried over to Verma modules for sl_2.

Finally, the connection between the subalgebra u_1^- of the hyperalgebra U for a finite dimensional semisimple Lie algebra, and a group algebra KG for some suitable p-group G is studied. No isomorphism exists, when the characteristic of the field is larger than the Coxeter number. However, in the case of $p = 2$ we find $u_1^-(sl_3) \simeq KG$. Furthermore, we determine the centre of $u_n^-(sl_3)$, and we obtain an alternative K-basis of U^-.

Acknowledgements

I would like to thank my supervisor Dr Karin Erdmann for her continuous guidance and encouragement, and docent Henning Haahr Andersen (Aarhus Universitet, Denmark) for his friendly support and many stimulating conversations. I am also grateful to Professor Stephen Donkin (Queen Mary and Westfield College, London) for introducing me to characteristic p Verma modules, and for our fruitful conversations during my visits at Q.M.W.

My fellow graduate students, especially my office-mates, and my flat-mates are to be thanked for making my time in Oxford so enjoyable.

My doctoral research was funded by Aarhus Universitets Forskningsfond and Forsknings Akademiet, Denmark.

Contents

Introduction

Let $\mathcal{G}$ be a finite dimensional semisimple Lie algebra; we study the class of infinite dimensional representations of $\mathcal{G}$ called Verma modules. They were first introduced by Verma in 1968. In the case of characteristic 0 Verma modules, their Loewy structure was completely described by R. Irving [Irving]: they have a rigid Loewy filtration of finite length. Characteristic p Verma modules were first introduced by W. Haboush [Haboush], and a study by M. Mowbray [Mowbray 1], for the Lie algebra of type sl_2, determined a one to one correspondence between, on the one hand, some ordered subsets of the non-negative integers, and, on the other hand, the submodule structure of the Verma module. Already for this, the smallest Lie algebra, the Verma modules are not of finite length.

In our work we focus on Verma modules for arbitrary finite dimensional semisimple Lie algebras over a field K of characteristic p.

In Chapter 1 we present the notation and some preliminary results. To obtain information about the structure of the Verma module $Z(\lambda)$ we find weights μ for which a non-zero homomorphism from $Z(\mu)$ to $Z(\lambda)$ exists. These weights are called primitive. In the study of "highest weight categories" (possible analogues of the category $\mathcal{O}$), Verma modules are the basic "building blocks". In order to understand such categories, it is important to understand homomorphisms between Verma modules. Chapter 2 contains a study of two cases. For $\lambda+\rho$ dominant, where ρ is the sum of the fundamental roots, there exist only finitely many primitive weights, and they all appear in a convex, bounded area (see Theorem 2.1.6). In the proof of this we use translation functors. In the case of $\lambda+\rho$ not dominant, and the characteristic p a good prime for the Lie algebra, infinitely many primitive weights exist (see Theorem 2.3.1). We specialize to $\mathcal{G} = sl_3$ and in Chapter 3 explicitly determine a large, but not necessarily complete, set of primitive weights.

Chapter 4 gives a method to obtain the Verma module as the tensor product of Steinberg modules and Frobenius twisted $Z(\lambda_1)$, for certain weights $\lambda = p^n\lambda_1 + (p^n - 1)\rho$ (see Proposition 4.1.1). Consider Weyl modules $\Delta(n)$ for $G = SL_2(K)$. Let $i, j \in \mathbf{Z}_{\geq 0}$ with $i + j = p - 2$. Then for any $n \geq 1$ there exists a short exact sequence of G-modules

$$0 \to \Delta(j) \otimes \Delta(n-1)^F \to \Delta(pn+i) \to \Delta(i) \otimes \Delta(n)^F \to 0,$$

where F is the Frobenius map. In Proposition 4.2.1 we obtain an analogue of this for Verma modules for sl_2.

Finally, in Chapter 5 we study the algebra structure of u_n^-. In particular, we determine the centre of $u_n^-(sl_3)$ (see Proposition 5.2.3). Moreover, we obtain an alternative K-basis of U^- in Theorem 5.1.6. In [Quillen] Quillen proved that the associated graded algebra of the group algebra of a p-group is isomorphic to the restricted enveloping algebra of a p-Lie algebra. We study a question which is something like a converse: Is the subalgebra u_1^- of the hyperalgebra U of a finite dimensional semisimple Lie algebra isomorphic to a group algebra KG ? Note that if so, then G must be a p-group for dimension reasons. We show, see Theorem 5.4.11, that the answer is usually no, namely whenever p is larger than the Coxeter number. However, for sl_3 and $p = 2$ the answer is yes, see Proposition 5.4.13. We prove, in Theorem 5.5.4, that for G a finite abelian p-group the group algebra KG is isomorphic to $U^{[p]}(\mathrm{Lie}(G))$, and find an example, in Corollary 5.5.7, that the group algebra is not isomorphic to the graded algebra with respect to powers of the augmentation ideal, $\mathrm{gr}(KG)$.

Chapter 1

Notation and preliminary results

This chapter contains a presentation of notation and some preliminary results. We assume the reader to be familiar with the basic theory of semisimple Lie algebras as it can be found for example in [Hump].

1.1 The hyperalgebra, U

Let $\mathcal{G}$ be a complex, finite dimensional semisimple Lie algebra. Let $\mathcal{H}$ be a Cartan subalgebra of $\mathcal{G}$, Φ the corresponding root system, $\Delta = \{\alpha_1, \alpha_2, \cdots, \alpha_l\}$ a fundamental system of roots and Φ^+ the set of positive roots, $|\Phi^+| = r$. Let ρ be the sum of the fundamental roots, which is also half the sum of the positive roots.

We view $\mathcal{G}$ as a left $\mathcal{G}$-module via the adjoint representation $\mathrm{Ad} : \mathcal{G} \to \mathrm{End}_{\mathbf{C}}(\mathcal{G})$. The Killing form on $\mathcal{G}$, that is $(x, y) = \mathrm{trace}(\mathrm{Ad}(x)\mathrm{Ad}(y))$, is non-singular and moreover its restriction to $\mathcal{H}$ is non-singular. For each $\lambda \in \mathcal{H}^* = \mathrm{Hom}_{\mathbf{C}}(\mathcal{H}, \mathbf{C})$ there is a unique $t_\lambda \in \mathcal{H}$ such that $(t_\lambda, H) = \lambda(H)$ for all $H \in \mathcal{H}$, and we transfer the bilinear form from $\mathcal{H}$ to $\mathcal{H}^*$ by setting $(\lambda, \mu) = (t_\lambda, t_\mu)$ for $\lambda, \mu \in \mathcal{H}^*$. For $\alpha \in \Phi$, we define $H_\alpha = 2t_\alpha/(t_\alpha, t_\alpha)$, see for example [Hump] 8.3.

We have the *root space decomposition* of $\mathcal{G}$

$$\mathcal{G} = \mathcal{H} \oplus (\oplus_{\alpha \in \mathcal{H}^*} \mathcal{G}_\alpha),$$

where

$$\mathcal{G}_\alpha = \{x \in \mathcal{G} \mid [H, x] = \alpha(H)x \text{ for all } H \in \mathcal{H}\},$$

and each $\mathcal{G}_\alpha$ is one dimensional over $\mathbf{C}$. The set of all non-zero $\alpha \in \mathcal{H}^*$ for which $\mathcal{G}_\alpha \neq 0$ is the root system Φ.

Let $q_{\alpha\beta}$ and $t_{\alpha\beta}$ be the greatest integers such that $-q_{\alpha\beta}\alpha + \beta$ and $t_{\alpha\beta}\alpha + \beta$ are roots, then $-q_{\alpha\beta}\alpha + \beta, -(q_{\alpha\beta} - 1)\alpha + \beta, \cdots, \beta, \cdots, t_{\alpha\beta}\alpha + \beta$ is the α-string of roots through β, see for example [Hump] 8.4.

The bilinear form derived from the Killing form is a symmetric bilinear form on

$$(-,-) : \mathbf{Z}\Phi \times \mathbf{Z}\Phi \to \mathbf{Z}$$

such that

$$(\alpha, \alpha) \neq 0, \; 2(\beta, \alpha)/(\alpha, \alpha) = q_{\alpha\beta} - t_{\alpha\beta},$$

(see for example [Carter] Chapter 3.3). We adopt the notation $\langle \beta, \alpha \rangle = 2(\beta, \alpha)/(\alpha, \alpha)$.

We have a Chevalley Basis for $\mathcal{G}$ (see for example [Hump] 25.2)

$$\{X_\alpha : \alpha \in \Phi\} \cup \{H_{\alpha_i} : i = 1, 2, \cdots, l\},$$

where $X_\alpha \in \mathcal{G}_\alpha$ and $H_{\alpha_i} \in \mathcal{H}$.

For the Chevalley Basis the structure constants lie in $\mathbf{Z}$. More precisely

$$\begin{aligned}
[X_\alpha, X_{-\alpha}] &= H_\alpha \quad \text{for all } \alpha \in \Phi^+ \\
[X_\alpha, X_\beta] &= \begin{cases} \pm(q_{\alpha\beta} + 1)X_{\alpha+\beta} & \text{if} \quad \alpha + \beta \in \Phi \quad \text{for all } \alpha, \beta \in \Phi \\ 0 & \text{if} \quad t = 0 \end{cases} \\
[H_\alpha, H_\beta] &= 0 \quad \text{if } \alpha, \beta \in \Phi^+ \\
[H_\alpha, X_\beta] &= \langle \beta, \alpha \rangle X_\beta \quad \text{for } \alpha \in \Delta, \; \beta \in \Phi.
\end{aligned}$$

Furthermore, for $\gamma \in \Phi^+$, we have that H_γ is a $\mathbf{Z}$-linear combination of H_α for $\alpha \in \Delta$.

Concerning the choice of signs see for example [Samelson] p. 52-54.

Let $\mathbf{Z}_{\geq 0}$ be the non-negative integers, $\mathbf{Z}_{>0}$ the positive integers and $\mathbf{Z}_{<0}$ the negative integers. Let $\mathbf{Z}(n)$ denote the set $\{0, 1, 2, \cdots, n\}$. Let $A = (a_1, a_2, \cdots, a_r) \in \mathbf{Z}^r_{\geq 0}$ and $B = (b_1, b_2, \cdots, b_l) \in \mathbf{Z}^l_{\geq 0}$. For a given ordering of the roots, $\Phi^+ = \{\beta_1, \beta_2, \cdots, \beta_r\}$ and $\Phi^- = \{\gamma_1, \gamma_2, \cdots, \gamma_r\}$, define

$$\hat{e}_A = \prod_{i=1}^{r} X_{\beta_i}^{a_i}/a_i!, \quad \hat{f}_A = \prod_{i=1}^{r} X_{\gamma_i}^{a_i}/a_i!$$

and

$$\hat{h}_B = \prod_{i=1}^{l} \binom{H_{\alpha_i}}{b_i},$$

where

$$\binom{H_{\alpha_i}}{b_i} = H_{\alpha_i}(H_{\alpha_i} - 1) \cdots (H_{\alpha_i} - b_i + 1)/b_i!$$

Furthermore, let $U_{\mathbf{Z}}$ be the Kostant $\mathbf{Z}$-form (see [Kostant]) of the enveloping algebra, that is the subring (with 1) generated by the elements $X_\alpha^a/a!$ for $a \in \mathbf{Z}_{\geq 0}$. We have ([Hump] 26.4)

Theorem 1.1.1 *(Kostant) The elements $\hat{f}_A \hat{h}_B \hat{e}_C$, where $A, C \in \mathbf{Z}^r_{\geq 0}$ and $B \in \mathbf{Z}^l_{\geq 0}$ form a $\mathbf{C}$-basis of the enveloping algebra and a $\mathbf{Z}$-basis of $U_{\mathbf{Z}}$.*

Let K be an algebraically closed field of characteristic $p > 0$. Then

$$U = K \otimes_{\mathbf{Z}} U_{\mathbf{Z}}$$

is the *hyperalgebra* of $\mathcal{G}$ over K.

For $\alpha \in \Phi^+, a \in \mathbf{Z}_{>0}$ let

$$\begin{aligned} H_{\alpha,a} &= 1_K \otimes_{\mathbf{Z}} \binom{H_\alpha}{a}, \text{ where } \binom{H_\alpha}{a} = H_\alpha(H_\alpha - 1) \cdots (H_\alpha - a + 1)/a! \\ X_{\alpha,a} &= 1_K \otimes_{\mathbf{Z}} (X_\alpha)^a/a! \\ X_{-\alpha,a} &= 1_K \otimes_{\mathbf{Z}} (X_{-\alpha})^a/a! \end{aligned}$$

and use the convention

$$H_{\alpha,0} = X_{\alpha,0} = X_{-\alpha,0} = 1,\ H_{\alpha,-a} = X_{\alpha,-a} = X_{-\alpha,-a} = 0.$$

Again with a given ordering of the roots, $\Phi^+ = \{\beta_1, \beta_2, \cdots, \beta_r\}$ and $\Phi^- = \{\gamma_1, \gamma_2, \cdots, \gamma_r\}$, we define

$$e_A = \prod_{i=1}^{r} X_{\beta_i,a_i}, \quad f_A = \prod_{i=1}^{r} X_{\gamma_i,a_i}$$

and

$$h_B = \prod_{i=1}^{l} H_{\alpha_i,b_i},$$

where $A \in \mathbf{Z}^r_{\geq 0}$ and $B \in \mathbf{Z}^l_{\geq 0}$.

Theorem 1.1.2 *The hyperalgebra U has a K-basis, called the* Kostant basis, *consisting of elements of the form*

$$f_A h_B e_C,$$

where $A, C \in \mathbf{Z}^r_{\geq 0}$ and $B \in \mathbf{Z}^l_{\geq 0}$.

Proof: See [Steinberg] Theorem 2, Section 2. □

The hyperalgebra U has a Hopf algebra structure, see [Donkin 2] Chapter 4, with diagonal map $\delta : U \to U \otimes U$ (the tensor product of algebras) such that for $\gamma \in \Phi^+$ and $\alpha \in \Delta$

$$\begin{aligned}
\delta(X_{\gamma,a}) &= \sum_{i=0}^{a} X_{\gamma,i} \otimes X_{\gamma,a-i}, \\
\delta(X_{-\gamma,a}) &= \sum_{i=0}^{a} X_{-\gamma,i} \otimes X_{-\gamma,a-i}, \\
\delta(H_{\alpha,a}) &= \sum_{i=0}^{a} H_{\alpha,i} \otimes H_{\alpha,a-i}.
\end{aligned} \tag{1.1}$$

We introduce various subalgebras of U:

Definition 1.1.3 *Denote by U^+, U^0 and U^- the subalgebras of U generated by*

$$\{X_{\gamma,a}, H_{\alpha,b} : \gamma \in \Phi^+,\ \alpha \in \Delta,\ a, b \in \mathbf{Z}_{\geq 0}\},$$

$$\{H_{\alpha,b} : \alpha \in \Delta,\ b \in \mathbf{Z}_{\geq 0}\},$$

and

$$\{X_{-\gamma,a} : \gamma \in \Phi^+,\ a \in \mathbf{Z}_{\geq 0}\},$$

respectively.

Then $U^0 \subset U^+$ and $U \simeq U^- \otimes_K U^+$ as K-vector space, by Theorem 1.1.2. Note that some books use a different convention for U^+.

Definition 1.1.4 *For each positive integer $n \in \mathbf{Z}_{>0}$, let u_n be the subalgebra of U generated by*

$$\{X_{\gamma,a}, H_{\alpha,b} : \gamma \in \Phi,\ \alpha \in \Delta,\ a, b \in \mathbf{Z}(p^n - 1)\}.$$

This algebra is finite dimensional, and, using Theorem 1.1.2, we get that

$$\{f_A h_B e_C \mid A, C \in \mathbf{Z}(p^n - 1)^r,\ B \in \mathbf{Z}(p^n - 1)^l\} \text{ is a } K\text{-basis of } u_n, \tag{1.2}$$

Moreover $u_n \subset u_{n+1}$ and $U = \cup_{n \geq 1} u_n$. We also define

Definition 1.1.5

$$u_n^- = U^- \cap u_n.$$

This is a subalgebra of u_n, and

$$\{f_A \mid A \in \mathbf{Z}(p^n - 1)^r\} \text{ is a } K - \text{basis of } u_n^-. \tag{1.3}$$

Hence the K-dimension of u_n^- is $|\Phi^+|^{p^n} = r^{p^n}$.

For many purposes it is convenient to work with a finite dimensional subalgebra. The disadvantage with u_n is that the information about weights (see section 1.3 below) is lost. To avoid this, one may use $\hat{u}_n$:

Definition 1.1.6 *The algebra $\hat{u}_n$ is the subalgebra of U generated by*

$$\{X_{\gamma,a}, H_{\alpha,b} : \gamma \in \Phi,\ \alpha \in \Delta,\ a \in \mathbf{Z}(p^n - 1),\ b \in \mathbf{Z}_{\geq 0}\}.$$

Using Theorem 1.1.2, we make the following observation:

$$\{f_A h_B e_C \mid A, C \in \mathbf{Z}(p^n - 1)^r, B \in \mathbf{Z}^l_{\geq 0}\} \text{ is a } K - \text{basis of } \hat{u}_n. \tag{1.4}$$

The above subalgebras are all sub-Hopf algebras, see [Donkin 2] Chapter 5.

1.2 p-adic integers

Let $\mathbf{Z}_p$ be the ring of p-adic integers,

$$\mathbf{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \mathbf{Z}(p-1) \text{ for all } i\}.$$

Adding and multiplying p-adic integers is very much like the corresponding operations on decimals. The only difference being that the 'carrying' over goes from left to right (as can be seen in Example 1.2.2 below).

Notation 1.2.1 For $a \in \mathbf{Z}_p$ and $i \in \mathbf{Z}_{\geq 0}$, let a_i be the *i'th* entry in the p-adic expansion of a. We use the notation $a = (a_0, a_1, \cdots, a_k, ---)$, when $a_m = a_k$ for all $m \geq k$.

Let $a = \sum_{i \geq 0} a_i p^i$ and $b = \sum_{j \geq 0} b_j p^j$. Recall that c_0 is the value of c mod p, and define $\lceil c_{i+1} \rceil$ inductively as follows $\lceil c_{-1} \rceil = 0$ and $\lceil c_{i+1} \rceil = (c_{i+1} + \lceil c_i \rceil - (c_{i+1} + \lceil c_i \rceil)_0)/p$ (this is the 'carry over'). Then

(1) Let $c = a + b$, and define $\tilde{c}_l = a_l + b_l$. Then $c_l = (\tilde{c}_l + \lceil c_{l-1} \rceil)_0$.

(2) Let $c = ab$, and define $\tilde{c}_l = \sum_{i+j=l} a_i b_j$. Then $c_l = (\tilde{c}_l + \lceil c_{l-1} \rceil)_0$

Example 1.2.2 Let $p = 3$, $a = (1, 2, 0, ---) = 7$ and $b = (2, 1, 1, 0, ---) = 14$, then (1) $(a + b)_0 = 0$, $\lceil (a + b)_0 \rceil = 1$, $(a + b)_1 = 1$, $\lceil (a + b)_1 \rceil = 1$ and $(a + b)_2 = 2$. Therefore $a + b = (0, 1, 2, 0, ---) = 21$.

(2) $(ab)_0 = 2$, $\lceil (ab)_0 \rceil = 0$, $(ab)_1 = (1+4)_0 = 2$, $\lceil (ab)_1 \rceil = 1$, $(ab)_2 = (1+2+1)_0 = 1$, $\lceil (ab)_2 \rceil = 1$, $(ab)_3 = (2+1)_0 = 0$, $\lceil (ab)_3 \rceil = 1$ and $(ab)_4 = 1$. Therefore $ab = (2,2,1,0,1,0,---) = 98$.

We note that the integers are isomorphic to a subring in $\mathbf{Z}_p$. An integer $a \in \mathbf{Z}_{\geq 0}$ is identified with its usual p-adic expansion in $\mathbf{Z}$, that is there exists a k, such that $a = \sum_{i=0}^{k} a_i p^i$, and for all $m \geq k$ we have $a_m = 0$. Moreover, $a \in \mathbf{Z}_{<0}$ is identified with the additive inverse of a in $\mathbf{Z}_p$, that is there exists a k, such that $a_m = p-1$ for all $m \geq k$. For $a \in \mathbf{Z}_p$ and $n \in \mathbf{Z}_{\geq 0}$, we define

$$\binom{a}{n} = a(a-1)\cdots(a-n+1)/n!,$$

$$\binom{a}{a-n} = \binom{a}{n} \text{ and } \binom{a}{0} = 1.$$

Lemma 1.2.3 *Let $a \in \mathbf{Z}_p$ and $n \in \mathbf{Z}_{\geq 0}$, then*

$$\binom{a}{n} \equiv \prod_{r \geq 0} \binom{a_r}{n_r} \pmod{p}. \tag{1.5}$$

and

$$p \not| \binom{a}{n} \Longleftrightarrow \binom{a}{n} \not\equiv 0 \pmod{p} \Longleftrightarrow n_r \leq a_r \textit{ for all } r.$$

Proof: Equation 1.5 is [Haboush] identity 5.1, and the rest follows from this. We note that the product is finite, since $n_r \neq 0$ for at most finitely many r. □

Notation 1.2.4 For $a = \sum_{i \geq 0} a_i p^i \in \mathbf{Z}_p \backslash \{-1\}$, let

$$c_a = \min\{j \mid a_j \neq p-1\} \in \mathbf{Z}_{\geq 0}. \tag{1.6}$$

We write c instead of c_a, if a is clear from the context.

Definition 1.2.5 *Let $a \in \mathbf{Z}_p$, then for all $k \in \mathbf{Z}_{\geq 0}$ we define an integer related to a by*

$$a(k) = \sum_{i=0}^{k} a_i p^i.$$

Lemma 1.2.6 *Let $a = \sum_{i \geq 0} a_i p^i \in \mathbf{Z}_p \backslash \{-1\}$ and $b \in \mathbf{Z}_{>0}$. Then*

$$\binom{a-b+d}{d} \equiv 0 \pmod p \text{ for all } 1 \leq d \leq b \Longleftrightarrow b = 1 + a(k) \text{ for some } k \geq c_a. \tag{1.7}$$

Proof: Assume $b = 1 + a(k)$ for some $k \geq c_a$, then for $1 \leq d \leq b$

$$\binom{a-b+d}{d} = \binom{\sum_{i>k} a_i p^i - 1 + d}{d} \equiv \binom{d-1}{d} \pmod p,$$

which according to Lemma 1.2.3 is equivalent to 0 mod p. Now suppose that

$$\binom{a-b+d}{d} \equiv 0 \pmod p \text{ for all } d \text{ with } 1 \leq d \leq b.$$

Then by Lemma 1.2.3 we get that for any such d there exists an r with

$$d_r > (a-b+d)_r. \tag{1.8}$$

Assume $b = \sum_{i=0}^{l} b_i p^i$, where $b_l \neq 0$. If $d = 1 = p^0$ then (1.8) gives $1 = d_0 > (a-b+1)_0$. This means $(a-b)_0 = p-1$. Similarly, by considering $d = p^j$ we get

$$(a-b)_j = p-1 \quad \text{for} \quad 0 \leq j \leq l. \tag{1.9}$$

For $d = b$ equation (1.8) gives that there exists an $r \leq l$ such that $b_r > a_r$. This together with (1.9) yields the existence of an $r \leq l$ such that

$$a_0 = a_1 = \cdots = a_{r-1} = p-1, \quad b_0 = b_1 = \cdots = b_{r-1} = 0,$$

$$b_r = a_r + 1, \quad a_r \neq p-1. \tag{1.10}$$

Therefore $b = 1 + a(l)$ for $l \geq r = c_a$. $\square$

1.3 U-modules

Let X be the set of weights, that is the set of K-algebra homomorphisms from the subalgebra U^0 of U to K. In [Haboush] Example 2.12 it is shown that there is a bijection Ψ from $\mathbf{Z}_p^l$ to X, where $\mathbf{Z}_p^l$ is the cartesian product of l copies of the p-adic integers, $\mathbf{Z}_p$, such that if $(a_1, a_2, \cdots, a_l) \in \mathbf{Z}_p^l$, $\alpha_i \in \Delta$, and $n \in \mathbf{Z}_{>0}$, then

$$\Psi(a_1, a_2, \cdots, a_l)(H_{\alpha_i,n}) = \binom{a_i}{n} 1_K.$$

Remark 1.3.1 Let us make a few comments about this in the case $\mathcal{G} = sl_2$. We set $H_{\alpha,n} = H_n$. We have that $U_{\mathbf{Z}}^0$ is generated by $\{\binom{H}{n} \mid n \in \mathbf{Z}_{\geq 0}\}$ subject to the relations

$$\binom{H}{r}\binom{H}{s} = \sum_{i=0}^{r}(r+s-i)!/[(r-i)!(s-i)!i!]\binom{H}{r+s-i},$$

see [Jantzen] p. 117.

Define a map λ from $U_{\mathbf{Z}}^0$ to $\mathbf{Z}$ by

$$\lambda(\binom{H}{s}) = \binom{a}{s},$$

and linear extension. We check that this is a $\mathbf{Z}$-algebra homomorphism. We need it to satisfies

$$\lambda(\binom{H}{r}\binom{H}{s}) = \lambda(\binom{H}{r})\lambda(\binom{H}{s}) \quad \text{for all } 1 \leq r \leq s.$$

We get

$$\begin{aligned}
\lambda(\binom{H}{r}\binom{H}{s}) &= \lambda(\sum_{i=0}^{r}(r+s-i)!/[(r-i)!(s-i)!i!]\binom{H}{r+s-i}) \\
&= \sum_{i=0}^{r}(r+s-i)!/[(r-i)!(s-i)!i!]\lambda(\binom{H}{r+s-i})
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{r}(r+s-i)!/[(r-i)!(s-i)!i!]\binom{a}{r+s-i} \\
&= \sum_{i=0}^{r}(r+s-i)!/[(r-i)!(s-i)!i!]\binom{a}{s}(a-s)!s!/[(a-s-r+i)!(r+s-i)!] \\
&= \binom{a}{s}\sum_{i=0}^{r}\binom{a-s}{r-i}\binom{s}{i} \\
&= \binom{a}{s}\binom{a}{r} \quad \text{see Remark 1.3.3 below} \\
&= \lambda(\binom{H}{r})\lambda(\binom{H}{s}).
\end{aligned}
$$

By base change this homomorphism gives us a homomorphism, call it λ, from $U^0 = K \otimes_{\mathbf{Z}} U^0_{\mathbf{Z}}$ to K.

The set of weights X is by definition the algebra homomorphisms from U^0 to K, and the statement is that X can be identified with $\mathbf{Z}_p$. The correspondence is given such that we to each $a = \sum_{i\geq 0} a_i p^i \in \mathbf{Z}_p$ relate the homomorphism λ from U^0 to K.

We have an inclusion $\Phi \subseteq X$, if we set $\beta(H_{\alpha,n}) = \binom{\langle\beta,\alpha\rangle}{n}$ for $\beta \in \Phi$ and $n \geq 1$. Now, $\langle \beta, \alpha \rangle \in \mathbf{Z}$, which allows us to identify $\mathbf{Z}\Phi$ with a subgroup of $X_{\mathbf{Z}} = \Psi(\mathbf{Z}^l)$; and the usual bilinear form on $\mathbf{Z}\Phi$ defines $(-,-)$ and $\langle -,- \rangle$ on $X_{\mathbf{Z}}$.

Extend the map $\langle -,- \rangle$ to X in the first variable such that

$$\lambda = \Psi(\langle \lambda, \alpha_1 \rangle, \langle \lambda, \alpha_2 \rangle, \cdots, \langle \lambda, \alpha_l \rangle),$$

for $\lambda \in X$, $\Delta = \{\alpha_1, \alpha_2, \cdots, \alpha_l\}$. For $\gamma \in \Delta$ we use the notation $\lambda_\gamma = \langle \lambda, \gamma \rangle$. We will sometimes omit the Ψ and simply write

$$\lambda = (\langle \lambda, \alpha_1 \rangle, \langle \lambda, \alpha_2 \rangle, \cdots, \langle \lambda, \alpha_l \rangle) = (\lambda_{\alpha_1}, \lambda_{\alpha_2}, \cdots, \lambda_{\alpha_l}).$$

We have a natural partial order on X: for $\lambda, \mu \in X$ write $\lambda \leq \mu$ if $\mu - \lambda = \sum_{\alpha\in\Phi^+} m_\alpha \alpha$ for some $m_\alpha \in \mathbf{Z}_{\geq 0}$.

For a U^0-module V and $\lambda \in X$, we write

$$V_\lambda = \{v \in V \mid hv = \lambda(h)v \quad \text{for all } h \in U^0\},$$

or equivalently

$$V_\lambda = \{v \in V \mid H_{\alpha,a}v = \binom{\langle \lambda, \alpha \rangle}{a} v \quad \text{for all } \alpha \in \Delta, a \in \mathbf{Z}_{>0}\}.$$

The space V_λ is called the *λ-weight space* of V, and $0 \neq v \in V$ is called a *weight vector* of weight λ if $v \in V_\lambda$. An element $\lambda \in X$ is called a *weight* of V if $V_\lambda \neq 0$. We say that the weight λ of V has *multiplicity* m if $\dim V = m$. We call λ a *maximal weight* of V if also $V_\mu = 0$ for all $\mu > \lambda$. In this case any $0 \neq v \in V_\lambda$ is a *maximal weight vector.* If there is a unique maximal weight of V, we call it the *highest weight* of V, and a non-zero vector in V of this weight is a *highest weight vector.*

A weight vector $v \in V_\lambda$ is called *primitive* if $X_{\alpha,n}v = 0$ for all $\alpha \in \Phi^+$, $n \in \mathbf{Z}_{>0}$. We say that λ is a *primitive weight* of the module V if there exists a primitive weight vector $v \in V$ of weight λ. Note that this is a stronger condition than the one found in the literature (for example [Kac]), where the existence of a submodule U of V such that $v \notin U$, and $X_{\alpha,n}v \in U$ for all $\alpha \in \Phi^+$, $n \in \mathbf{Z}_{>0}$ is sufficient. For α_i a simple root, we call a weight vector v an *α_i-primitive weight vector* if $X_{\alpha_i,n}v = 0$ for all $n \in \mathbf{Z}_{>0}$.

Define the *dominant weights* to be $X^+ = \Psi((\mathbf{Z}_{\geq 0})^l)$, the *integral weights* to be $X_\mathbf{Z} = \Psi(\mathbf{Z}^l)$, and let $X_n = \Psi((\{0,1,2,\cdots,p^n-1\})^l) = \Psi(\mathbf{Z}(p^n-1)^l)$ for $n \in \mathbf{Z}_{>0}$. We note that $X_\mathbf{Z}$ is an abelian group, and hence a $\mathbf{Z}$-module. From (1.1) we get:

Lemma 1.3.2 *Let v and w be weight vectors in the U-modules V and W, respectively. Assume $\gamma \in \Phi$ and $\eta \in \Delta$, then the action of U on $V \otimes W$ satisfies*

$$X_{\gamma,a}(v \otimes w) = \sum_{i=0}^{a} X_{\gamma,i}v \otimes X_{\gamma,a-i}w,$$

and

$$H_{\eta,a}(v \otimes w) = \sum_{i=0}^{a} H_{\eta,i} v \otimes H_{\eta,a-i} w.$$

Remark 1.3.3 We notice that if the weight vectors are of weight $v \in V_\lambda$ and $w \in W_\mu$, respectively, then $v \otimes w$ has weight $\lambda + \mu$. This follows using Pascal's formula, $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$, to obtain the following by induction on b

$$\begin{aligned}
\binom{a+b}{l} &= \binom{a+b-1}{l} + \binom{a+b-1}{l-1} \\
&= \sum_{i=0}^{l} \binom{a}{i}\binom{b-1}{l-i} + \sum_{i=0}^{l-1} \binom{a}{i}\binom{b-1}{l-1-i} \\
&= \sum_{i=0}^{l-1} \binom{a}{i}(\binom{b}{l-i} + \binom{b-1}{l-1-i}) + \binom{a}{l} \\
&= \sum_{i=0}^{l} \binom{a}{i}\binom{b}{l-i}.
\end{aligned} \tag{1.11}$$

Lemma 1.3.4 *Let $\alpha \in \Phi^+$ and $\beta \in \Phi$. In $U_{\mathbf{Z}}$ we have*

$$(H_\alpha - n\langle \beta, \alpha \rangle)(X_\beta^n / n!) = (X_\beta^n / n!) H_\alpha.$$

Proof: We prove by induction on n that in the enveloping algebra

$$(H_\alpha - n\langle \beta, \alpha \rangle)(X_\beta)^n = (X_\beta)^n H_\alpha.$$

Our result follows from this. For $n = 1$ we have (section 1.1) $[H_\alpha, X_\beta] = \langle \beta, \alpha \rangle X_\beta$, and the induction step is

$$\begin{aligned}
(H_\alpha - (n-1+1)\langle \beta, \alpha \rangle)(X_\beta)^n &= (X_\beta)^{n-1} H_\alpha X_\beta - \langle \beta, \alpha \rangle (X_\beta)^n \\
&= (X_\beta)^{n-1}(X_\beta H_\alpha + \langle \beta, \alpha \rangle X_\beta) - \langle \beta, \alpha \rangle (X_\beta)^n \\
&= (X_\beta)^n H_\alpha. \ \square
\end{aligned}$$

From [Donkin 2] Chapter 4 we know

Corollary 1.3.5 *Let $\beta \in \Phi$ and $n \in \mathbf{Z}_{\geq 0}$. Assume v is a weight vector of weight λ in a module for a subalgebra of U containing U^0 and $X_{\beta,n}$, then $X_{\beta,n}v$ is a weight vector of weight $\lambda + n\beta$.*

Observation 1.3.6 Let us consider U^-, which has a K-basis spanned by f_A, as a U^0-module via the adjoint representation. Recall that for a given ordering of the roots, $\Phi^- = \{\gamma_1, \gamma_2, \cdots, \gamma_r\}$, we defined $f_A = \prod_{i=1}^r X_{\gamma_i,a_i}$, where $a_i \in \mathbf{Z}_{\geq 0}$. Then $U^- = \oplus_\lambda U_\lambda^-$, where the weight space

$$U_\lambda^- = \{f_A \in U^- \mid [H_{\alpha,a}, f_A] = \binom{\langle \lambda, \alpha \rangle}{a} f_A \quad \text{for all } \alpha \in \Delta\}$$

has a K-basis

$$\mathrm{span}_K\{f_A \in U^- \mid \sum_{i=1}^r a_i\gamma_i = \lambda\}.$$

We notice that the weights λ occurring fulfil $\lambda < 0$, and that each weight space has dimension equal to the cardinality of the set $\{A = (a_1, a_2, \cdots, a_r) \in \mathbf{Z}_{\geq 0}^r \mid \lambda = \sum_i a_i\gamma_i\}$. This is finite.

Definition 1.3.7 *A U^0-module V is called* admissible *if it satisfies the following conditions:*

(1) $V = \oplus_{\lambda \in X} V_\lambda$;

(2) $\dim V_\lambda < \infty$ for all $\lambda \in X$;

(3) the set of weights of V is bounded above, that is there exist finitely many elements $\mu_1, \cdots, \mu_n \in X$, such that for each weight λ of V, we have $\lambda \leq \mu_i$ for some $1 \leq i \leq n$.

Example 1.3.8 According to Observation 1.3.6 above U^- is admissible.

We call a U or U^+-module admissible if it is admissible as a U^0-module. Notice that submodules, factor modules and finite direct sums of admissible modules are admissible. One can define (see [Donkin 2], Chapter 5) a K-algebra map F, called the Frobenius map, from U to U, such that $F(X_{\alpha,a}) = F(H_{\alpha,a}) = 0$ if $a \notin p\mathbf{Z}$, $F(X_{\alpha,pb}) = X_{\alpha,b}$ and

$F(H_{\alpha,pb}) = H_{\alpha,b}$ for $b \in \mathbf{Z}_{\geq 0}$. For M an admissible U-module, we define M^F to be the U-module which has the same vector space structure as M, and the following action

$$u.m = F(u)m \quad u \in U, m \in M,$$

The action is often called *twisted.*

Definition 1.3.9 *A U-module V is a* module of highest weight *if, for some $\lambda \in X$, there exists an element $0 \neq v \in V_\lambda$, such that $e_A v^+ = 0$ for all $A \in \mathbf{Z}^r_{\geq 0}, A \neq 0$, and $V = Uv^+$.*

For each $\lambda \in X$, let K_λ be the one-dimensional U^+-module Kv (see [Donkin 2] Chapter 4) whose action is given by

$$H_{\alpha,a}v = \lambda(H_{\alpha,a})v \text{ for all } \alpha \in \Delta, a \in \mathbf{Z}_{>0},$$
$$X_{\gamma,a}v = 0 \text{ for all } \gamma \in \Phi^+, a \in \mathbf{Z}_{>0}.$$

Definition 1.3.10 *The Verma module with highest weight $\lambda \in X$ is*

$$Z(\lambda) = U \otimes_{U^+} K_\lambda.$$

This is a module for the hyperalgebra via left multiplication on U.

Since $\hat{u}_n^+$ is a subalgebra of U^+, the one-dimensional U^+-module K_λ is a $\hat{u}_n^+$-module by restriction.

Definition 1.3.11 *The $\hat{u}_n$-Verma module with highest weight λ is*

$$\hat{Z}_n(\lambda) = \hat{u}_n \otimes_{\hat{u}_n^+} K_\lambda.$$

From Theorem 1.1.2 it follows that multiplication $U^- \otimes U^+ \longrightarrow U$ is an isomorphism of left U^--modules, in particular, $Z(\lambda)$ is a free U^--module, generated by $v^+ = 1 \otimes v$, where

$0 \neq v \in K_\lambda$. We find that

$$\{f_A v^+ \mid A \in \mathbf{Z}^r_{\geq 0}\} \text{ is a } K-\text{basis of } Z(\lambda). \tag{1.12}$$

Likewise by (1.3) we see that

$$\{f_A v^+ \mid A \in \mathbf{Z}(p^n-1)^r\} \text{ is a } K-\text{basis of } \hat{Z}_n(\lambda). \tag{1.13}$$

Since $Z(\lambda)$ is a free U^--module of rank 1 generated by $v^+ \in Z(\lambda)_\lambda$, the weight space $(Z(\lambda))_{\lambda-\mu}$ has the same dimension as the weight space $U^-_{-\mu}$ for $\mu \in X$. Therefore, by Observation 1.3.6, the multiplicity of $\lambda - \mu$ as a weight of $Z(\lambda)$ is the cardinality of $\{A = (a_1, a_2, \cdots, a_r) \in \mathbf{Z}^r_{\geq 0} \mid -\mu = \sum_i a_i\gamma_i\}$. This set is finite. Also, $Z(\lambda)$ is a direct sum of weight spaces, and the weights are bounded above by λ, and we get that $Z(\lambda)$ is admissible.

Proposition 1.3.12 *Let V be a U-module of highest weight.*

(1) V is admissible, V has a unique highest weight λ and $\dim V_\lambda = 1$.

(2) V has a unique proper maximal submodule.

(3) V is a homomorphic image of $Z(\lambda)$.

Proof: See [Donkin 2] Chapter 4. □

Remark 1.3.13 We have a similar result for $\hat{u}_n$-modules.

From Proposition 1.3.12 or the definition of $Z(\eta)$ we get

Lemma 1.3.14 *Let M be an admissible U-module and let $0 \neq w \in M_\eta$. Then w is a primitive weight vector if and only if there exists a U-homomorphism $Z(\eta) \to M$ taking a highest weight vector v of $Z(\eta)$ to w.*

Remark 1.3.15 We have a similar result for $\hat{u}_n$-modules.

For $\lambda \in X$, let $M(\lambda)$ denote the unique maximal submodule of $Z(\lambda)$, and let $L(\lambda) = Z(\lambda)/M(\lambda)$. Hence $L(\lambda)$ is simple.

Proposition 1.3.16 *A complete set of inequivalent irreducible admissible U-modules is $\{L(\lambda) \mid \lambda \in X\}$.*

Proof: See [Donkin 2] Chapter 4. □

Similarly we get (see [Donkin 2], Chapter 5):

Proposition 1.3.17 *Let $r \in \mathbf{Z}_{>0}$ and $\lambda \in X$, then $\hat{Z}_r(\lambda)$ has a unique maximal submodule $\hat{M}_r(\lambda)$. Defining $\hat{L}_r(\lambda) = \hat{Z}_r(\lambda)/\hat{M}_r(\lambda)$, it follows that $\{\hat{L}_r(\lambda) \mid \lambda \in X\}$ is a complete set of inequivalent irreducible $\hat{u}_r$-modules.*

Remark 1.3.18 It can be shown that there exists a functor ψ from the category of finite dimensional G_nT-modules to the category of finite dimensional $\hat{u}_n$-modules with integral weights,

$$\psi : G_nT - \text{modules} \to \hat{u}_n - \text{modules},$$

such that, for λ an integral weight, we have $\hat{Z}_n(\lambda)$ in the image of ψ. This means that any result from [Jantzen] about finite dimensional G_nT-modules carry over to $\hat{Z}_n(\lambda)$ for λ integral.

Let V be an admissible U-module ($\hat{u}_n$-module) and m a finite ascending filtration

$$0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_k = V.$$

For $\lambda \in X$, denote by

$$[V : L(\lambda)]_m \quad ([V : \hat{L}_n(\lambda)]_m)$$

the number of integers i such that $1 \leq i \leq k$ and V_i/V_{i-1} is isomorphic to $L(\lambda)$ as a U-module ($\hat{L}_n(\lambda)$ as a $\hat{u}_n$-module). Note that by additivity of weight space dimensions on short exact sequences, $[V : L(\lambda)]_m \quad ([V : \hat{L}_n(\lambda)]_m)$ is bounded above by $\dim V_\lambda$.

Definition 1.3.19 *Let V be an admissible U-module ($\hat{u}_n$-module) and $L(\lambda)$ ($\hat{L}_n(\lambda)$) a simple module. Then the* composition multiplicity

$$[V : L(\lambda)] \quad ([V : \hat{L}_n(\lambda)]),$$

is the maximum value of $[V : L(\lambda)]_m \quad ([V : \hat{L}_n(\lambda)]_m)$ as m ranges over all finite filtrations of V.

We refer to [Mowbray 2] Chapter 2 for further information about the composition multiplicities.

1.4 The Weyl group

Let W be the *Weyl group* which is the finite group generated by the set of simple reflections, $\{s_\alpha \mid \alpha \in \Delta\}$, where $s_\alpha : X_{\mathbf{Z}} \to X_{\mathbf{Z}}$ for $\alpha \in \Phi^+$ is given by

$$s_\alpha(\lambda) = \lambda - \langle \lambda, \alpha \rangle \alpha.$$

Let W_p be the group generated by the set

$$\{s_{\alpha,i} \mid \alpha \in \Delta, i \in \mathbf{Z}\},$$

where

$$s_{\alpha,i}(\lambda) = \lambda - \langle \lambda, \alpha \rangle \alpha + ip\alpha.$$

Extend the W-action $\mathbf{Z}_p$-linearly to X. Adding the p-translations we get a W_p-action on X. If $\lambda \in X, w \in W$, then let $w.\lambda = w(\lambda + \rho) - \rho$.
We define $H_\alpha = \{x \in X_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{R} \mid \langle x + \rho, \alpha \rangle = 0\}$ for $\alpha \in \Phi$ to be the α-*wall* in $X_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{R}$.

The reflection group W_p acting on $X_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{R}$ defines a system of *facets*. A facet for W_p

is a non-empty set of the form

$$F = \{x \in X_{\mathbf{Z}} \otimes_Z \mathbf{R} \mid \langle x+\rho, \alpha \rangle = n_\alpha p \quad \text{for} \quad \alpha \in \Phi_0^+(F),$$
$$(n_\alpha - 1)p < \langle x+\rho, \alpha \rangle < n_\alpha p \quad \text{for} \quad \alpha \in \Phi_1^+(F)\},$$

for integers $n_\alpha \in \mathbf{Z}$ and a disjoint decomposition $\Phi^+ = \Phi_0^+(F) \dot\cup \Phi_1^+(F)$. Then the *closure* $\bar{F}$ of F is equal to

$$\bar{F} = \{x \in X_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{R} \mid \langle x+\rho, \alpha \rangle = n_\alpha p \quad \text{for} \quad \alpha \in \Phi_0^+(F),$$
$$(n_\alpha - 1)p \leq \langle x+\rho, \alpha \rangle \leq n_\alpha p \quad \text{for} \quad \alpha \in \Phi_1^+(F)\}.$$

We call

$$\hat{F} = \{x \in X_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{R} \mid \langle x+\rho, \alpha \rangle = n_\alpha p \quad \text{for} \quad \alpha \in \Phi_0^+(F),$$
$$(n_\alpha - 1)p < \langle x+\rho, \alpha \rangle \leq n_\alpha p \quad \text{for} \quad \alpha \in \Phi_1^+(F)\},$$

the *upper closure* of F. We call a facet F an *alcove* if $\Phi_0^+(F) = \emptyset$.

Definition 1.4.1 *For $\lambda + \rho \in X^+$, let $A.(\lambda)$ be the set of weights η such that*

$$\eta \in A.(\lambda) \text{ if and only if } \eta \in W_p.\lambda \text{ and } w.\eta \leq \lambda \quad \text{for all } w \in W.$$

This will be used in Chapter 2.

Definition 1.4.2 *Let*

$$\bar{C}_{\mathbf{Z}} = \{\lambda \in X_{\mathbf{Z}} \mid 0 \leq \langle \lambda+\rho, \beta \rangle \leq p \quad \text{for all } \beta \in \Phi^+\}, \tag{1.14}$$

and

$$C = \{\lambda \in X_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{R} \mid 0 < \langle \lambda+\rho, \beta \rangle < p \quad \text{for all } \beta \in \Phi^+\}. \tag{1.15}$$

The stabilizer *is*

$$\mathrm{Stab}_{W_p}(\lambda) = \{w \in W_p \mid w.\lambda = \lambda\}. \tag{1.16}$$

The set C is called the *fundamental chamber*, and with the dot action we have a unique element in $\bar{C}$, the closure of C, in each W_p orbit. We note that the stabilizer of a weight λ is the set of reflections in W_p which keeps λ fixed, that is the reflections corresponding to the walls on which λ lies.

Example 1.4.3 Suppose $\lambda \in C \cap X_{\mathbf{Z}}$. Then

$$\mathrm{Stab}_{W_p}(\lambda) = \{1\},$$

since assume that λ is stabilized by $w \in W_p \setminus \{1\}$, then λ lies on the w wall. This is not possible, since by assumption λ is not on any wall.

Definition 1.4.4 *Let $\Sigma(C')$ be the set of all reflections with respect to any wall F of the alcove C', and let*

$$\Sigma^0(\lambda, C') = \{s \in \Sigma(C') \mid s.\lambda = \lambda\}. \tag{1.17}$$

1.5 The translation functor T_λ^μ

Let $\hat{u}_n$-mod be the category of admissible $\hat{u}_n$-modules with morphisms the $\hat{u}_n$-module homomorphisms. For any finite dimensional $\hat{u}_n$-module E we have that

$$E \otimes - : \hat{u}_n - \mathrm{mod} \ \rightarrow \ \hat{u}_n - \mathrm{mod}$$

is a functor. If we have an admissible $\hat{u}_n$-module M, then $E \otimes M$ is again admissible (see for example [Jantzen 2] Chapter 2).

For $\lambda \in X$, define $\hat{\mathcal{O}}_\lambda$ to be the category with objects all admissible $\hat{u}_n$-modules M such that all composition factors of M have highest weight in $W_p.\lambda$, and morphisms the $\hat{u}_n$-module homomorphisms. Then $\hat{\mathcal{O}}_\lambda$ is a union of blocks (see [Jantzen] II.9.19). In particular, for $\mu \in X$, there are no homomorphism between modules from $\hat{\mathcal{O}}_\lambda$ and $\hat{\mathcal{O}}_\mu$ if $\mu \notin W_p.\lambda$.

For M an arbitrary admissible $\hat{u}_n$-module, we define

$$\mathrm{pr}_\lambda : \hat{u}_n - \mathrm{mod} \to \hat{\mathcal{O}}_\lambda$$

to be the functor sending M to the largest submodule of M which belongs to $\hat{\mathcal{O}}_\lambda$. And for two $\hat{u}_n$-modules M and N with a homomorphism $f : M \to N$, let $\mathrm{pr}_\lambda(f)$ be the restriction of f to $\mathrm{pr}_\lambda(M)$. According to the above observation about homomorphisms this maps $\mathrm{pr}_\lambda(M)$ into $\mathrm{pr}_\lambda(N)$.

We see that any admissible $\hat{u}_n$-module M decomposes into a direct sum of such submodules, where all the direct summands again are admissible, see for example [Jantzen] 7.3.

Example 1.5.1 If $M = \hat{Z}_n(\mu)$, then M is indecomposable. Hence $\mathrm{pr}_\lambda M$ is either 0 or M. It is M if and only if $\mu \in W_p.\lambda$.

Consider $\lambda, \mu \in \bar{C}_{\mathbf{Z}}$. There is a unique $\nu_1 \in X^+ \cap W(\mu - \lambda)$ ([Hump] 13.2). We define the *translation functor*, T_λ^μ from λ to μ via

$$T_\lambda^\mu M = \mathrm{pr}_\mu(\hat{L}_n(\nu_1) \otimes \mathrm{pr}_\lambda M)$$

for any $\hat{u}_n$-module M. Since it is a composition of functors we have that T_λ^μ is a functor from $\hat{u}_n$-mod to $\hat{\mathcal{O}}_\mu$.

Lemma 1.5.2 *Let $\lambda, \mu \in \bar{C}_{\mathbf{Z}}$, and let M and N be $\hat{u}_n$-modules, then we have*

$$\mathrm{Hom}_{\hat{u}_n}(M, T_\lambda^\mu N) \simeq \mathrm{Hom}_{\hat{u}_n}(T_\mu^\lambda M, N).$$

Proof: [Jantzen] remarks p. 286 and p. 334-35. □

Lemma 1.5.3 *Assume $\lambda+\rho\in X^+$, then there exists a $\hat{u}_n$-injection*

$$\hat{Z}_n(\lambda)\hookrightarrow T^{\lambda}_{-\rho}\hat{Z}_n(-\rho).$$

Proof: By definition we have

$$\begin{aligned} T^{\lambda}_{-\rho}\hat{Z}_n(-\rho) &= \mathrm{pr}_{\lambda}(\hat{L}_n(\nu)\otimes\hat{Z}_n(-\rho)),\ \nu\in W(\lambda+\rho)\cap X^+ \\ &= \mathrm{pr}_{\lambda}(\hat{L}_n(\lambda+\rho)\otimes\hat{Z}_n(-\rho)). \end{aligned}$$

Let v_1 be a highest weight vector in $\hat{L}_n(\lambda+\rho)$ of highest weight $\lambda+\rho$, and let v_2 be a highest weight vector in $\hat{Z}_n(-\rho)$ of highest weight $-\rho$, then $v=v_1\otimes v_2$ is a $\hat{u}_n$-highest weight vector of highest weight λ. This can be seen from the fact that for $\alpha\in\Phi^+$ the action is

$$X_{\alpha,m}v=\sum_{i=0}^{m}X_{\alpha,i}v_1\otimes X_{\alpha,m-i}v_2=0.$$

That is, we have a $\hat{u}_n$-surjection $\psi:\hat{Z}_n(\lambda)\to\hat{u}_n v$, and it suffices to prove that ψ is an injection. From [Mowbray2] Corollary 3.3 we know that any non-zero submodule of $\hat{Z}_n(\lambda)$ contains $I_n y$, where y is a highest weight vector generating $\hat{Z}_n(\lambda)$, and

$$I_n=X_{-\gamma_1,p^n-1}X_{-\gamma_2,p^n-1}\dots X_{-\gamma_r,p^n-1},$$

with $\{\gamma_1,\gamma_2\dots,\gamma_r\}=\Phi^+$. If $\psi(I_n y)=I_n v\neq 0$, we conclude that the image of any non-zero submodule is non-zero, and hence that $\ker\psi$ must be zero. We have

$$\begin{aligned} \psi(I_n y) &= I_n v \\ &= \sum_{i=1}^{r}\sum_{j_i=0}^{p^n-1}X_{-\gamma_1,j_1}X_{-\gamma_2,j_2}\dots X_{-\gamma_r,j_r}v_1\otimes X_{-\gamma_1,p^n-1-j_1}X_{-\gamma_2,p^n-1-j_2}\dots X_{-\gamma_r,p^n-1-j_r}v_2, \end{aligned}$$

which is different from zero; consider, for example, $j_1=j_2=\dots=j_r=0$ which gives $v_1\otimes I_n v_2$. This is non-zero and linearly independent of the other terms, since this term is the only one where the weight distribution is $\lambda+\rho$ from the first factor and $-\rho$ from the second. $\square$

Lemma 1.5.4 *Let $\lambda, \mu \in \bar{C}_{\mathbf{Z}}$ and $w \in W_p$, then $T_\lambda^\mu \hat{Z}_n(w.\lambda)$ has a filtration with factors $\hat{Z}_n(ww_1.\mu)$, where $w_1 \in \mathrm{Stab}_{W_p}(\lambda) = \{\omega \in W_p \mid \omega.\lambda = \lambda\}$. Each different $ww_1.\mu$ occurs exactly once.*

Proof: [Jantzen], p. 335 and Proposition 7.13 p. 290. $\square$

Corollary 1.5.5 *Let $\lambda, \mu \in \bar{C}_{\mathbf{Z}}$, and let F be the facet with $\lambda \in F$. If $\mu \in \bar{F}$, then*

$$T_\lambda^\mu \hat{Z}_n(w.\lambda) \simeq \hat{Z}_n(w.\mu) \text{ for all } w \in W_p.$$

Proof: [Jantzen], II 9.19 (2). $\square$

Corollary 1.5.6 *Let $\lambda \in C \cap X_{\mathbf{Z}}$ and $\mu \in \bar{C}_{\mathbf{Z}}$. Assume there exists $s \in \Sigma$ with $\Sigma^0(\mu) = \{s\}$. Let $w \in W_p$ with $w.\lambda < ws.\lambda$, then there is an exact sequence of $\hat{u}_n$-modules*

$$0 \to \hat{Z}_n(ws.\lambda) \to T_\mu^\lambda \hat{Z}_n(w.\mu) \to \hat{Z}_n(w.\lambda) \to 0$$

Proof: [Jantzen] II 9.19 (3). $\square$

1.6 Commutation relations

Lemma 1.6.1 *If $\gamma \in \Phi^+$ and $m, n \in \mathbf{Z}_{>0}$, then*

$$[X_{\gamma,m}, X_{-\gamma,n}] = \sum_{j>0} X_{-\gamma,n-j} \binom{H_\gamma - n - m + 2j}{j} X_{\gamma,m-j}.$$

Proof: [Steinberg] Lemma 5. $\square$

Corollary 1.6.2 *If $\gamma \in \Phi^+$, $m,n \in \mathbf{Z}_{>0}$, and v^+ is a primitive weight vector in a U-module of weight λ, then*

$$X_{\gamma,m}X_{-\gamma,n}v^+ = \binom{\langle\lambda,\gamma\rangle - n + m}{m} X_{-\gamma,n-m}v^+.$$

Proof: Follows from Lemma 1.6.1, using that $X_{\gamma,m-j}v^+ = 0$ if $m - j > 0$. □

Using the commutation relations from section 1.1 (see also [Mowbray 2], Lemma 1.3 and Lemma 1.4.), we get the following two lemmas:

Lemma 1.6.3 *If $\gamma, \delta \in \Phi^+$ and $m,n \in \mathbf{Z}_{\geq 0}$, then*

$$[H_{\gamma,m}, H_{\delta,n}] = 0.$$

Lemma 1.6.4 *If $\gamma, \delta \in \Phi$, $m,n \in \mathbf{Z}_{\geq 0}$ and $\gamma + \delta \notin \Phi$, then*

$$[X_{\gamma,m}, X_{\delta,n}] = 0.$$

We also have

Lemma 1.6.5 *Let $\gamma, \delta \in \Phi$, $m,n \in \mathbf{Z}_{>0}$ and $(\mathbf{Z}\gamma + \mathbf{Z}\delta) \cap \Phi = \{\pm\gamma, \pm\delta, \pm(\gamma+\delta)\}\}$.*

(a) If $[X_\gamma, X_\delta] = X_{\gamma+\delta}$, then

$$[X_{\gamma,m}, X_{\delta,n}] = \sum_{j>0} X_{\gamma+\delta,j}X_{\delta,n-j}X_{\gamma,m-j}.$$

(b) If $[X_\gamma, X_\delta] = -X_{\gamma+\delta}$, then

$$[X_{\gamma,m}, X_{\delta,n}] = \sum_{j>0} (-1)^j X_{\gamma+\delta,j}X_{\delta,n-j}X_{\gamma,m-j}.$$

Proof: (a) [Mowbray 2], Lemma 1.5. Statement (b) follows with similar arguments, observing that

$$[X_\gamma^m, X_\delta^n] = \sum_{0<j\leq \min(m,n)} (-1)^j j! \binom{m}{j} \binom{n}{j} X_\delta^{n-j} X_\gamma^{m-j} X_{\gamma+\delta}^j.$$

□

It also follows that

Corollary 1.6.6 *Let $\gamma \in \Phi^+$, $\delta \in \Phi$ and $m, n \in \mathbf{Z}_{>0}$. Suppose $(\mathbf{Z}\gamma + \mathbf{Z}\delta) \cap \Phi = \{\pm\gamma, \pm\delta, \pm(\gamma+\delta)\}$. Let v^+ be a primitive vector in a U-module. Then*

$$X_{\gamma,m} X_{\delta,n} v^+ = X_{\gamma+\delta,m} X_{\delta,n-m} v^+, \ \textit{if}\ [X_\gamma, X_\delta] = X_{\gamma+\delta},$$

and

$$X_{\gamma,m} X_{\delta,n} v^+ = (-1)^m X_{\gamma+\delta,m} X_{\delta,n-m} v^+, \ \textit{if}\ [X_\gamma, X_\delta] = -X_{\gamma+\delta}.$$

Lemma 1.6.7 *Let $\gamma \in \Phi^+$, $\delta \in \Phi$ and $m, n \in \mathbf{Z}_{>0}$. Then in $U_{\mathbf{Z}}$ we have*

$$\binom{H_\gamma}{m} X_\delta^n / n! = X_\delta^n / n! \binom{H_\gamma + n\langle \delta, \gamma \rangle}{m}.$$

Proof: Use Lemma 1.3.4 and the idea of its proof. □

Chapter 2

Homomorphisms

In this chapter we consider primitive weights in characteristic p, $p > 0$ Verma modules $Z(\lambda)$ for finite dimensional semisimple Lie algebras $\mathcal{G}$. In the case $\lambda + \rho$ dominant, we find that only finitely many primitive weights exist, although the Verma modules do have infinite length. These primitive weights all lie in the convex hull generated by the weights $W.\lambda$, and are contained in $W_p.\lambda \subseteq X_{\mathbf{Z}}$. For any other λ there are infinitely many primitive weights.

2.1 Finitely many homomorphisms

We need the following

Lemma 2.1.1 *If $\hat{L}_n(\mu)$ is a composition factor of $\hat{Z}_n(\lambda)$, then $\mu \leq \lambda$. Suppose also that λ is integral, then μ is integral and $\mu \in W_p.\lambda$.*

Proof: The first part follows from (1.13) and Corollary 1.3.5. For the second part, see [Jantzen] Corollary 9.12 p. 328 and (2) p. 264, which uses the strong linkage principle [Andersen]. □

From this we obtain

Corollary 2.1.2 *If $\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\mu), \hat{Z}_n(\lambda)) \neq 0$, then $\mu \leq \lambda$. If in addition λ is integral, then $\mu \in W_p.\lambda$.*

Lemma 2.1.3 *Let $\lambda \in C \cap X_{\mathbf{Z}}$, and let η be a primitive weight occurring in $\hat{Z}_n(\lambda)$. Then $\eta \in A.(\lambda)$.*

Proof: By Lemma 1.3.14 it is equivalent to show that $\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\eta), \hat{Z}_n(\lambda)) \neq 0$ implies $\eta \in A.(\lambda)$. We have

$$\begin{aligned} \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\eta), \hat{Z}_n(\lambda)) &\subseteq \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\eta), T^{\lambda}_{-\rho}\hat{Z}_n(-\rho)), \text{ by Lemma 1.5.3} \\ &\simeq \mathrm{Hom}_{\hat{u}_n}(T^{-\rho}_{\lambda}\hat{Z}_n(\eta), \hat{Z}_n(-\rho)), \text{ by Lemma 1.5.2} \\ &\simeq \mathrm{Hom}_{\hat{u}_n}(T^{-\rho}_{\lambda}\hat{Z}_n(\eta), \hat{L}_n(-\rho)), \text{ by [Jantzen] p. 338} \end{aligned} \tag{2.1}$$

Suppose there is a non-zero homomorphism $\hat{Z}_n(\eta) \to \hat{Z}_n(\lambda)$, then we know from Corollary 2.1.2 that $\eta = w.\lambda$ for some $w \in W_p$. According to (2.1) there is a non-zero homomorphism from $T^{-\rho}_{\lambda}\hat{Z}_n(w.\lambda)$ to $\hat{L}_n(-\rho)$. Lemma 1.5.4 implies that the module $T^{-\rho}_{\lambda}\hat{Z}_n(w.\lambda)$ has a filtration with factors $\hat{Z}_n(ww_1.(-\rho))$ for $w_1 \in \mathrm{Stab}_{W_p}(\lambda)$. Since $\lambda \in C \cap X_{\mathbf{Z}}$ we have $\mathrm{Stab}_{W_p}(\lambda) = \{1\}$, see Example 1.4.3. Hence there is a non-zero homomorphism from $\hat{Z}_n(w.(-\rho))$ to $\hat{L}_n(-\rho)$. This is only possible for $w.(-\rho) = -\rho$, that is for $w \in \mathrm{Stab}_{W_p}(-\rho) = W$. Hence $\eta = w.\lambda \in A.(\lambda)$ □

Lemma 2.1.4 *Let $\lambda \in C \cap X_{\mathbf{Z}}$ and let $\mu \in \bar{C}_{\mathbf{Z}}$. Assume $w \in W_p$ such that $w.\lambda$ is dominant, and assume that we have $\eta \in A.(w.\lambda)$ for any primitive weight η in $\hat{Z}_n(w.\lambda)$. Then a primitive weight γ in $\hat{Z}_n(w.\mu)$ satisfies $\gamma \in A.(w.\mu)$.*

Proof: By Lemma 1.3.14 we want to find γ for which $\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\gamma), \hat{Z}_n(w.\mu)) \neq 0$. Assume we have a γ such that there is a non-zero homomorphism, then Corollary 2.1.2 implies that $\gamma = \tilde{w}.\mu$ for some $\tilde{w} \in W_p$. We have

$$\begin{aligned} \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}.\mu), \hat{Z}_n(w.\mu)) &\simeq \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}.\mu), T^{\mu}_{\lambda}\hat{Z}_n(w.\lambda)), \text{ by Corollary 1.5.5} \\ &\simeq \mathrm{Hom}_{\hat{u}_n}(T^{\lambda}_{\mu}\hat{Z}_n(\tilde{w}.\mu), \hat{Z}_n(w.\lambda)), \text{ by Lemma 1.5.2.} \end{aligned}$$

Lemma 1.5.4 yields the factors in a filtration of $T^{\lambda}_{\mu}\hat{Z}_n(\tilde{w}.\mu)$, and to obtain a non-zero homomorphism space we require $\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}s.\lambda), \hat{Z}_n(w.\lambda)) \neq 0$ for some $s \in \mathrm{Stab}_{W_p}(\mu)$.

This implies by assumption that $\tilde{w}s.\lambda \in A.(w.\lambda)$, and hence $\tilde{w}s.\mu = \tilde{w}.\mu = \gamma \in A.(w.\mu)$. $\square$

Lemma 2.1.5 *Let $\lambda \in C \cap X_{\mathbf{Z}}$, and let $w \in W_p$ be such that $w.\lambda$ is dominant. Assume we have $\eta \in A.(w.\lambda)$ for any primitive weight η in $\hat{Z}_n(w.\lambda)$. Let $\mathcal{A}$ be the alcove containing $w.\lambda$. Assume $s \in \Sigma(\mathcal{A})$ such that $sw.\lambda > w.\lambda$. Then a primitive weight γ in $\hat{Z}_n(sw.\lambda)$ satisfies $\gamma \in A.(sw.\lambda)$.*

Proof: Choose $\mu' \in \bar{\mathcal{A}}$ (the closure of $\mathcal{A}$) such that $\Sigma^0(\mu', \mathcal{A}) = \{s\}$. Then there exists a unique $\mu \in \bar{C}_{\mathbf{Z}}$ such that $w.\mu = \mu'$. We note that $s' = w^{-1}sw \in \mathrm{Stab}(\mu)$, and then by assumption we have $ws'.\lambda = sw.\lambda > w.\lambda$. Assume we have γ for which $\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\gamma), \hat{Z}_n(sw.\lambda)) \neq 0$, then $\gamma = \tilde{w}.\lambda$ for $\tilde{w} \in W_p$ (Corollary 2.1.2). Look at

$$\begin{aligned}
\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}.\lambda), \hat{Z}_n(sw.\lambda)) &= \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}.\lambda), \hat{Z}_n(ws'.\lambda)) \\
&\subseteq \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}.\lambda), T_\mu^\lambda \hat{Z}_n(w.\mu)), \text{ by Corollary 1.5.6} \\
&\simeq \mathrm{Hom}_{\hat{u}_n}(T_\lambda^\mu \hat{Z}_n(\tilde{w}.\lambda), \hat{Z}_n(w.\mu)), \text{ by Lemma 1.5.2} \\
&\simeq \mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\tilde{w}.\mu), \hat{Z}_n(w.\mu)), \text{ by Corollary 1.5.5.}
\end{aligned}$$

That this homomorphism space is non-zero gives, according to Lemma 2.1.4 and the assumptions, $\tilde{w}.\mu \in A.(w.\mu) = A.(\mu') = A.(s.\mu') = A.(sw.\mu)$. Therefore $\tilde{w}.\lambda = \gamma \in A.(sw.\lambda)$. $\square$

Theorem 2.1.6 *Let U be an arbitrary hyperalgebra, and let $\lambda + \rho \in X^+$. Then*

$$\mathrm{Hom}_U(Z(\mu), Z(\lambda)) \neq 0 \textit{ implies that } \mu \in A.(\lambda).$$

Proof: Suppose $\mathrm{Hom}_U(Z(\mu), Z(\lambda)) \neq 0$. We fix a highest weight vector v such that $Z(\mu) = Uv$. Consider the $\hat{u}_n$-submodule $\hat{u}_n v$; this is isomorphic to $\hat{Z}_n(\mu)$ (by 1.12, 1.13 and 1.3.13). Similarly, if x is a highest weight vector such that $Z(\lambda) = Ux$, then $\hat{u}_n x \simeq \hat{Z}_n(\lambda)$ for all $n \geq 1$.

Because of the assumption there is a primitive vector in $Z(\lambda)$ of weight μ, w say. For n large enough we have $w \in \hat{u}_n x$. Fix such n. Then it follows that

$$\mathrm{Hom}_{\hat{u}_n}(\hat{Z}_n(\mu), \hat{Z}_n(\lambda)) \neq 0.$$

By Corollary 2.1.2 we deduce $\mu \leq \lambda$ and $\mu \in W_p.\lambda$. In the case where $\lambda \in C \cap X_{\mathbf{Z}}$, it follows from Lemma 2.1.3 that $\mu \in A.(\lambda)$. Starting with $\lambda \in C \cap X_{\mathbf{Z}}$ we move to the upper wall using Lemma 2.1.4, and from there across the wall to the next alcove using Lemma 2.1.5. And the result follows for general $\lambda + \rho \in X^+$. □

The following is immediate consequences of Theorem 2.1.6

Corollary 2.1.7 *Let U be an arbitrary hyperalgebra, and let $\lambda + \rho \in X^+$. Then we have only finitely many primitive weights occurring in $Z(\lambda)$.*

Remark 2.1.8 In the special case $\lambda = -\rho$ we can see that

$$Z(-\rho) = L(-\rho).$$

This also follows from [Mowbray 2] Lemma 2.9, where we, for $\gamma_1, \gamma_2 \in X$, have

$$[Z(\gamma_1) : L(\gamma_2)] = [\hat{Z}_n(\gamma_1) : \hat{L}_n(\gamma_2)] \text{ for } n \gg 0, \tag{2.2}$$

and [Jantzen] p. 338.

Remark 2.1.9 Let $\lambda + \rho \in X^+$. Note that $A.(\lambda)$ is the convex hull in $W_p.\lambda$ generated by $W.\lambda$. However, we know that most weights in this set are not primitive. See Example 3.2.1 in Chapter 3.

Remark 2.1.10 Corollary 2.1.7 can be obtained directly[1]. Let $\lambda+\rho \in X^+$, then $Z(\lambda) \subseteq Z(-\rho) \otimes L(\lambda+\rho)$, and we get

$$\begin{aligned}\mathrm{Hom}_U(Z(\mu), Z(\lambda)) &\subseteq \mathrm{Hom}_U(Z(\mu), Z(-\rho) \otimes L(\lambda+\rho)) \\ &\simeq \mathrm{Hom}_U(Z(\mu) \otimes L(\lambda+\rho)^*, Z(-\rho)) \\ &\simeq \mathrm{Hom}_U(Z(\mu) \otimes L(\lambda+\rho)^*, L(-\rho)).\end{aligned}$$

We know that $Z(\mu) \otimes L(\lambda+\rho)^*$ has a filtration with Verma modules as quotients. These Verma modules have highest weights $\mu+\nu$, where $\nu \in L(\lambda+\rho)^*$. Since $L(\lambda+\rho)$ is finite dimensional for $\lambda+\rho \in X^+$ ([Hump] 21.2) we obtain something non-zero for finitely many μ.

2.2 Primitive weight vectors

We define and find all first generation primitive weight vectors for a given Verma module. Recall the notation c_a and $a(k)$ introduced in 1.2.4 and 1.2.5 in Chapter 1, and also that for $\lambda \in X$ we have $\lambda_i \in \mathbf{Z}_p$.

Proposition 2.2.1 *Let U be a hyperalgebra, and $Z(\lambda)$ a Verma module with highest weight $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_l) \in X$ and highest weight vector v. Fix some i such that $\lambda_i \neq -1$, and let w be the weight vector $X_{-\alpha_i,n}v$ of weight $\mu = \lambda - n\alpha_i$, where $n \geq 1$. Then w is a primitive vector if and only if $n \in \{1 + \lambda_i(k) \mid k \geq c_{\lambda_i}\}$.*

Remark 2.2.2 From [Jantzen 4], Teil 1, Satz 7 we know that a hyperalgebra U is generated by $X_{\alpha,a}$ and $X_{-\alpha,a}$ for $\alpha \in \Delta$ and $a \in \mathbf{Z}_{\geq 0}$.

Proof: Clearly, w is non-zero. As an immediate consequence of Lemma 1.2.6 and Corollary 1.6.2 we obtain that w is an α_i-primitive weight vector. Since $X_{\alpha_j,m}$ and $X_{-\alpha_i,n}$ commute for all $\alpha_j \in \Delta\backslash\{\alpha_i\}$ (Lemma 1.6.4), the vector w is primitive. □

[1]This was pointed out to the author by Professor S. Donkin, QMW, London

We call these primitive vectors *first generation* primitive vectors.

2.3 Infinitely many homomorphisms

Now we consider the case when $\lambda + \rho$ is not dominant.

Theorem 2.3.1 *Let U be a hyperalgebra, and let $\lambda + \rho \in X \backslash X^+$. Then there exist infinitely many weights $\mu \in X$ such that*

$$\mathrm{Hom}_U(Z(\mu), Z(\lambda)) \neq 0.$$

Thus there exist infinitely many primitive weights in $Z(\lambda)$.

Proof: Recall that $X = \Psi((\mathbf{Z}_p)^l)$ and $X^+ = \Psi((\mathbf{Z}_{\geq 0})^l)$, hence $\lambda + \rho \in X \backslash X^+$ implies that there exists an entry in λ corresponding to a simple root, α say, such that $(\lambda_\alpha + 1) \in \mathbf{Z}_p \backslash \mathbf{Z}_{\geq 0}$, that is $\lambda_\alpha \in \mathbf{Z}_p \backslash \mathbf{Z}_{\geq -1}$. Therefore the p-adic expansion of λ_α does not terminate, and not all coefficients are $p - 1$. Let v^+ be the highest weight vector generating $Z(\lambda)$, then we have, by Proposition 2.2.1, infinitely many specified integers n such that $w = X_{-\alpha,n} v^+$ is a primitive weight vector. $\square$

Chapter 3

Primitive weight vectors, sl_3

In the case $\mathcal{G} = sl_3$ we are able to construct certain primitive weights. If $\lambda + \rho$ is dominant a systematic analysis shows that the weights found are not always the full set of the finitely many primitive weights, which occur in the Verma module, $Z(\lambda)$.

3.1 Primitive weights

Let the order of the roots in the root system be $\Phi = \{-\alpha, -\beta, -\alpha - \beta, \alpha, \beta, \alpha + \beta\}$. Choose the sign $[X_\alpha, X_\beta] = X_{\alpha+\beta}$.

In section 2.2 we found some first generation primitive weight vectors. For sl_3 we furthermore find

Proposition 3.1.1 *Let $Z(\lambda)$ be a Verma module with highest weight $\lambda = (r, s) \in X$, $\Delta = \{\alpha, \beta\}$, and let v be a highest weight vector. The vector $w = X_{-\alpha,m_\alpha} X_{-\beta,n_\beta} v$ is a primitive weight vector of weight $\mu = (r + n_\beta - 2m_\alpha, s - 2n_\beta + m_\alpha)$ if and only if (n_β, m_α) belongs to the set $\{(1 + s(k), 1 + (r + n(k))(\tilde{k})) \mid k \geq c_s, \tilde{k} \geq c_{r+n_\beta(k)}\}$.*

Proof: Since U is generated by $X_{\pm\alpha,k}$ and $X_{\pm\beta,k}$, it suffices to prove that w is an α and a β primitive weight vector. For n arbitrary, $w_1 = X_{-\beta,n} v$ is an α-primitive weight vector of primitive weight $\mu_1 = (r+n, s-2n)$. It follows from Proposition 2.2.1 that $w = X_{-\alpha,m_\alpha} w_1$ is an α-primitive weight vector if and only if $m_\alpha \in \{1 + y\}$, where $y = (r + n)(k)$ for some

$k \geq c_{r+n}$. Since $X_{\beta,k}$ and $X_{-\alpha,m_\alpha}$ commute, $w = X_{-\alpha,m_\alpha} X_{-\beta,n} v$ is a β-primitive weight vector exactly when $w_1 = X_{-\beta,n} v$ is a β-primitive weight vector. □

Remark 3.1.2 Since sl_3 is symmetric with respect to α and β, we get a similar statement for $w = X_{-\beta,m_\beta} X_{-\alpha,n_\alpha} v$ being a primitive weight vector. We call primitive weight vectors of the kind found in Proposition 3.1.1 and here *second generation* primitive weight vectors.

Remark 3.1.3 Notice that for any finite dimensional semisimple Lie algebra $\mathcal{G}$, where U^- according to Remark 2.2.2 is generated by $X_{-\alpha,k}$ for $\alpha \in \Delta$, we can find second generation primitive weight vectors in a similar way.

Proposition 3.1.4 *Let $Z(\lambda)$ be a Verma module with highest weight $\lambda = (r,s) \in X$, $\Delta = \{\alpha, \beta\}$ and highest weight vector v. The vector $w = X_{-\beta,t_\beta} X_{-\alpha,m_\alpha} X_{-\beta,n_\beta} v$ is a primitive weight vector of weight $\mu = (r + n_\beta - 2m_\alpha + t_\beta, s - 2n_\beta + m_\alpha - 2t_\beta)$, if*

$$\begin{cases} n_\beta = 1 + s(k) \text{ for some } k \geq c_a \\ m_\alpha = 1 + (r + n_\beta(k))(\tilde{k}) \text{ for some } \tilde{k} \geq c_{r+n_\beta(k)} \\ t_\beta = 1 + (s - 2n_\beta(k) + m_\alpha(\tilde{k}))(\bar{k}) \text{ for some } \bar{k} \geq c_{s-2n_\beta(k)+m_\alpha(\tilde{k})} \end{cases}$$

and there exists an i, $0 \leq i \leq \min(m_\alpha, t_\beta)$, such that $\binom{n_\beta+t_\beta-i}{n_\beta} \neq 0$.

Proof: The conditions follow by using Propositions 2.2.1 and 3.1.1 together, and recalling that we require $w \neq 0$ □

Let f_a map a weight vector to $X_{\alpha,a}$ times the weight vector, that is $f_a(w) = X_{\alpha,a} w$. Similarly, let g_a map a weight vector to $X_{\beta,a}$ times the vector, that is $g_a(w) = X_{\beta,a} w$. With this notation,

$$w \text{ is a primitive weight vector if and only if } w \in (\cap_{a\geq 1} \ker f_a) \cap (\cap_{b \geq 1} \ker g_b). \quad (3.1)$$

Let v be a highest weight vector of highest weight $\lambda = (r,s) \in X$ generating $Z(\lambda)$. We want to find out for what values of n and m we get a primitive weight vector w with primitive weight $\mu = \lambda - n\alpha - m\beta$. Since we have symmetry in α and β it suffices to look at the case where $n \leq m$. Assume $w = \sum_{i=0}^{n} c_i X_{-\alpha,n-i} X_{-\beta,m-i} X_{-\alpha-\beta,i} v$ for $c_i \in K$. With a weight consideration it is easy to see that $w \in \ker f_a$ for all $a > n$, and $w \in \ker g_b$ for all $b > m$. Therefore condition (3.1) can be reformulated as

$$w \text{ is a primitive weight vector if and only if } w \in (\cap_{1\leq a\leq n} \ker f_a) \cap (\cap_{1\leq b\leq m} \ker g_b). \quad (3.2)$$

Proposition 3.1.5 *Let $Z(\lambda)$ be a Verma module with highest weight $\lambda = (r, s)$, $\lambda \in X$ and highest weight vector v. Let $n, m \in \mathbf{Z}_{\geq 0}$ and assume w is a weight vector of weight $\mu = \lambda - n\alpha - m\beta$ with $n \leq m$, say $w = \sum_{i=0}^{n} c_i X_{-\alpha,n-i} X_{-\beta,m-i} X_{-\alpha-\beta,i} v$, where $c_i \in K$.*

(1) The weight vector $w \in \ker f_a$ if and only if $c_0, c_1, \cdots, c_n$ are a solution to the following system of equations:

$$\sum_{j=i}^{i+a} c_j (-1)^{j-i} \binom{r+m-n+a-j}{a-j+i} \binom{m-i}{j-i} \equiv 0 \pmod{p} \text{ for } 0 \leq i \leq n-a.$$

(2) The weight vector $w \in \ker g_a$ if and only if the scalars $c_0, c_1, \cdots, c_n$ are a solution to the following system of equations:

$$\sum_{j=i}^{\min(i+a,n)} c_j \binom{s-m+i+a}{a-j+i} \binom{n-i}{j-i} \equiv 0 \pmod{p} \text{ for } 0 \leq i \leq \min(n, m-a).$$

Proof: (1) We want to find a solution to the equation $X_{\alpha,a} w = 0$. We get

$$\begin{aligned}
X_{\alpha,a} w &= X_{\alpha,a} \sum_{i=0}^{n} c_i X_{-\alpha,n-i} X_{-\beta,m-i} X_{-\alpha-\beta,i} v \\
&\quad \text{(By Lemma 1.6.1)} \\
&= \sum_{i=0}^{n} \sum_{j=0}^{\min(a,n-i)} c_i X_{-\alpha,n-i-j} \binom{H_\alpha - a - n + i + 2j}{j} X_{\alpha,a-j} X_{-\beta,m-i} X_{-\alpha-\beta,i} v \\
&\quad \text{(By Corollary 1.6.6)} \\
&= \sum_{i=0}^{n} \sum_{j=\max(0,a-i)}^{\min(a,n-i)} c_i X_{-\alpha,n-i-j} \binom{H_\alpha - a - n + i + 2j}{j} \\
&\qquad X_{-\beta,m-i} (-1)^{a-j} X_{-\beta,a-j} X_{-\alpha-\beta,i+j-a} v
\end{aligned}$$

(By Lemma 1.6.7)

$$= \sum_{i=0}^{n} \sum_{j=\max(0,a-i)}^{\min(a,n-i)} c_i(-1)^{a-j} \binom{r+m-n+a-i}{j} \binom{m+a-(i+j)}{a-j} X_{-\alpha,n-(i+j)} X_{-\beta,m+a-(i+j)} X_{-\alpha-\beta,i+j-a} v$$

(With $k = i + j$)

$$= \sum_{k=a}^{n} \sum_{j=0}^{a} c_{k-j}(-1)^{a-j} \binom{r+m-n+a-k+j}{j} \binom{m+a-k}{a-j} X_{-\alpha,n-k} X_{-\beta,m+a-k} X_{-\alpha-\beta,k-a} v$$

(With $k = k - a$)

$$= \sum_{k=0}^{n-a} \sum_{j=0}^{a} c_{k+a-j}(-1)^{a-j} \binom{r+m-n-k+j}{j} \binom{m-k}{a-j} X_{-\alpha,n-a-k} X_{-\beta,m-k} X_{-\alpha-\beta,k} v$$

(With $j = a - j + k$)

$$= \sum_{k=0}^{n-a} \sum_{j=k}^{k+a} c_j(-1)^{j-k} \binom{r+m-n+a-j}{a-(j-k)} \binom{m-k}{j-k} X_{-\alpha,n-a-k} X_{-\beta,m-k} X_{-\alpha-\beta,k} v$$

(2) Recall 1.11 from Chapter 1 and the result follows with calculations similar to the above. □

Remark 3.1.6 We can think of the equations as $Ac = 0$, where $c = (c_0, c_1, \cdots, c_n)$, and A is a matrix with products of binomial coefficients as entries. Finding a non-trivial solution is equivalent to finding the rank of A less than or equal to n.

From Proposition 3.1.5 it follows that w lies in the kernel of f_1 if and only if

$$-c_{i+1}(m-i) + c_i(r+m-n+1-i) \equiv 0 \pmod{p} \quad \text{for } 0 \le i \le n-1, \tag{3.3}$$

and in the kernel of g_1 if and only if

$$c_{i+1}(n-i) + c_i(s-m+1+i) \equiv 0 \pmod{p} \quad \text{for } 0 \le i \le n-1, \tag{3.4}$$

and

$$c_n(s+n-m+1) \equiv 0 \pmod{p} \quad \text{if } n < m. \tag{3.5}$$

Adding together the f_1 and g_1 equations, (3.3) and (3.4), we obtain

$$c_{i+1}(n-m) + c_i(r+s+2-n) \equiv 0 \pmod{p} \quad \text{for } 0 \leq i \leq n-1. \tag{3.6}$$

From (3.6) we have four different cases:

(1) Assuming $n-m \not\equiv 0 \pmod{p}$ and $r+s+2-n \equiv 0 \pmod{p}$ gives $c_{i+1} \equiv (r+s+2-n)/(n-m)c_i \pmod{p}$. This implies $c_1 = c_2 = \cdots = c_n = 0$, and hence $w = X_{-\alpha,n}X_{-\beta,m}v$. These are second generation primitive weight vectors all of which are found in Proposition 3.1.1.

(2) Assume $n-m \not\equiv 0 \pmod{p}$ and $r+s+2-n \not\equiv 0 \pmod{p}$. Using (3.6) we get $c_{i+1} \equiv (r+s+2-n)/(n-m)c_i \equiv ((r+s+2-n)/(n-m))^i c_0 \pmod{p}$. Hence in order, to have a non-trivial solution, all the c_i's must be non-zero. Because $n-m \not\equiv 0 \pmod{p}$ and $n \leq m$, we get $n < m$, and therefore (3.5) gives $s+n-m+1 \equiv 0 \pmod{p}$. For $i = n-1$ we obtain from (3.4), $(r+s+2-n)/(n-m) \equiv m-n-s \pmod{p}$. Thus $c_0 = c_1 = \cdots = c_n$, and $w = c\sum_{i=0}^{n} X_{-\alpha,n-i}X_{-\beta,m-i}X_{-\alpha-\beta,i}v = cX_{-\beta,m}X_{-\alpha,n}v$. These are second generation primitive weight vectors covered by Proposition 3.1.1.

(3) Assume $n-m \equiv 0 \pmod{p}$ and $r+s+2-n \not\equiv 0 \pmod{p}$, then $c_i \equiv (n-m)/(r+s+2-n)c_{i+1} \pmod{p}$. Therefore $c_0 = c_1 = \cdots = c_{n-1} = 0$, and by letting $i = n-1$ in (3.4) also $c_n = 0$ follows.

(4) For $n-m \equiv 0 \pmod{p}$ and $r+s+2-n \equiv 0 \pmod{p}$ we get $n \equiv m \equiv r+s+2 \pmod{p}$.

This means that apart from case (4), where $n \equiv m \equiv r+s+2 \pmod{p}$, we know when the system of equations in Proposition 3.1.5 has non-trivial solutions. The relevant n and m values are then determined by Propositions 2.2.1 and 3.1.1, and we do not need to look further at the equations. In case (4) we can not obtain general results, but we calculate some examples in the following section.

Remark 3.1.7 We notice that if $r+s \notin \mathbf{Z}$, we only get first and second generation primitive weight vectors and all these can be found using Propositions 2.2.1 and 3.1.1.

3.2 Examples

For $\lambda+\rho \in X^+$, we established in Chapter 2 that at most finitely many primitive weights occur in $Z(\lambda)$, which all lie in a bounded convex area (Remark 2.1.9). Thus Proposition 3.1.5 can, for fixed λ, be used to construct all primitive weights, by going through all possible n and m values. This is done using a symbolic manipulation package (Reduce). As observed above Remark 3.1.7 it suffices to restrict analysis to case (4). The code for this Reduce program can be found in Appendix A.

Example 3.2.1

(1) For $\mathcal{G} = sl_3, p = 3$ and $\lambda = (5,10)$ we find first and second generation primitive weights $\mu = \lambda - n\alpha - m\beta$ for the following values of n and m:

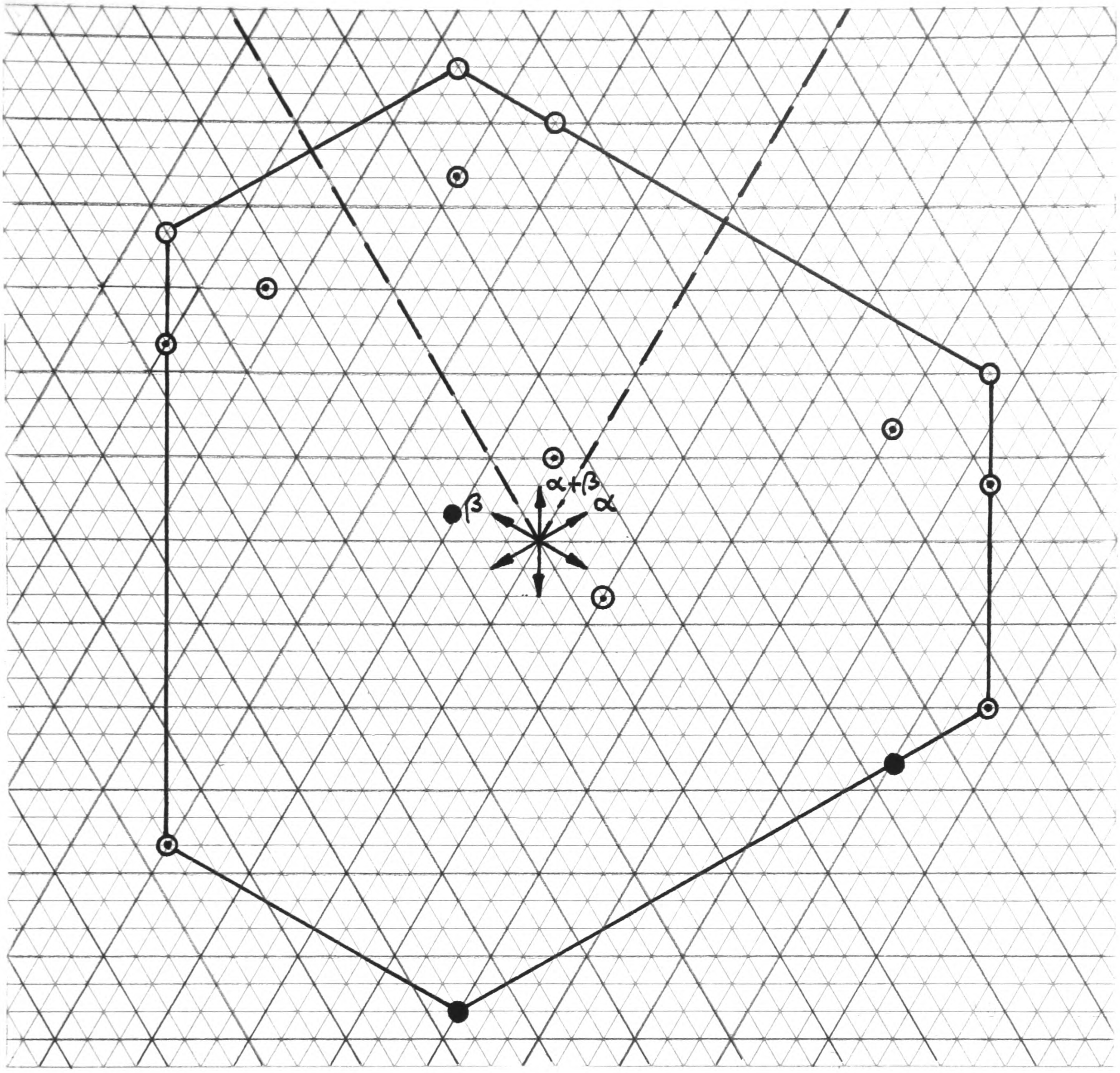
$$\begin{aligned}(n,m) \in \; & \{(6,0),(6,2),(6,8),(6,17),(0,2),(0,11),\\ & (2,2),(8,2),(2,11),(8,11),(17,11)\}.\end{aligned}$$

Proposition 3.1.4 gives third generation primitive weights for

$$(n,m) \in \{(2,11),(8,8),(8,17),(17,17)\}.$$

Case by case analysis, where $n \equiv m \equiv r+s+2 \equiv 1 \pmod p$, shows that $\mu = \lambda - n\alpha - m\beta$ is a primitive weight for

$$(n,m) \in \{(2,2),(2,11),(8,8),(8,11),(8,17),(17,17)\}.$$



○ 1st generation ● 3rd generation
⊙ 2nd generation

Figure 3.1: Primitive weights in $Z(5,10)$ for $p=3$.

Hence by finding third generation primitive weights we missed out on

$$(n,m) \in \{(2,2),(8,11)\},$$

but these are both second generation primitive weights. See Figure 3.1.

(2) For $\mathcal{G} = sl_3$, $p = 3$ and $\lambda = (13,4)$ we find first and second generation primitive

weights $\mu = \lambda - n\alpha - m\beta$ for the following values of n and m :

$$\begin{aligned}(n,m) \;\in\; & \{(2,0),(5,0),(14,0),(2,1),(2,7),(5,1),(5,10),(14,1),\\ & (14,19),(0,2),(0,5),(1,2),(7,2),(16,2),(1,5),(19,5)\}.\end{aligned}$$

Proposition 3.1.4 gives third generation primitive weights for

$$\begin{aligned}(n,m) \;\in\; & \{(4,7),(7,4),(7,10),(10,7),(10,10),(16,4),\\ & (16,10),(16,19),(19,7),(19,10),(19,19)\}.\end{aligned}$$

Case by case analysis, where $n \equiv m \equiv r+s+2 \equiv 1 \pmod p$, gives that $\mu = \lambda - n\alpha - m\beta$ is a primitive weight for

$$\begin{aligned}(n,m) \;\in\; & \{(1,1),(4,4),(4,7),(7,4),(7,10),(10,7),(10,10),\\ & (16,4),(16,10),(16,19),(19,7),(19,10),(19,19)\}.\end{aligned}$$

Hence by finding first, second, and third generation primitive weights we missed out on

$$(n,m) \in \{(1,1),(4,4)\}.$$

We note that these both lie on the diagonal. See Figure 3.2.

(3) For $\mathcal{G} = sl_3$, $p = 3$ and $\lambda = (7,16)$ we find first and second generation primitive weights $\mu = \lambda - n\alpha - m\beta$ for the following values of n and m

$$\begin{aligned}(n,m) \;\in\; & \{(2,0),(8,0),(2,1),(2,19),(8,1),(8,7),(8,25),(0,2),(0,8),\\ & (0,17),(1,2),(10,2),(1,8),(7,8),(16,8),(1,17),(7,17),(25,17)\}.\end{aligned}$$

Proposition 3.1.4 gives third generation primitive weights for

$$(n,m) \;\in\; \{((4,19),(7,10),(7,19),(10,4),(10,7),(10,25),$$

$$(16,10),(16,16),(16,25),(25,19),(25,25)\}.$$

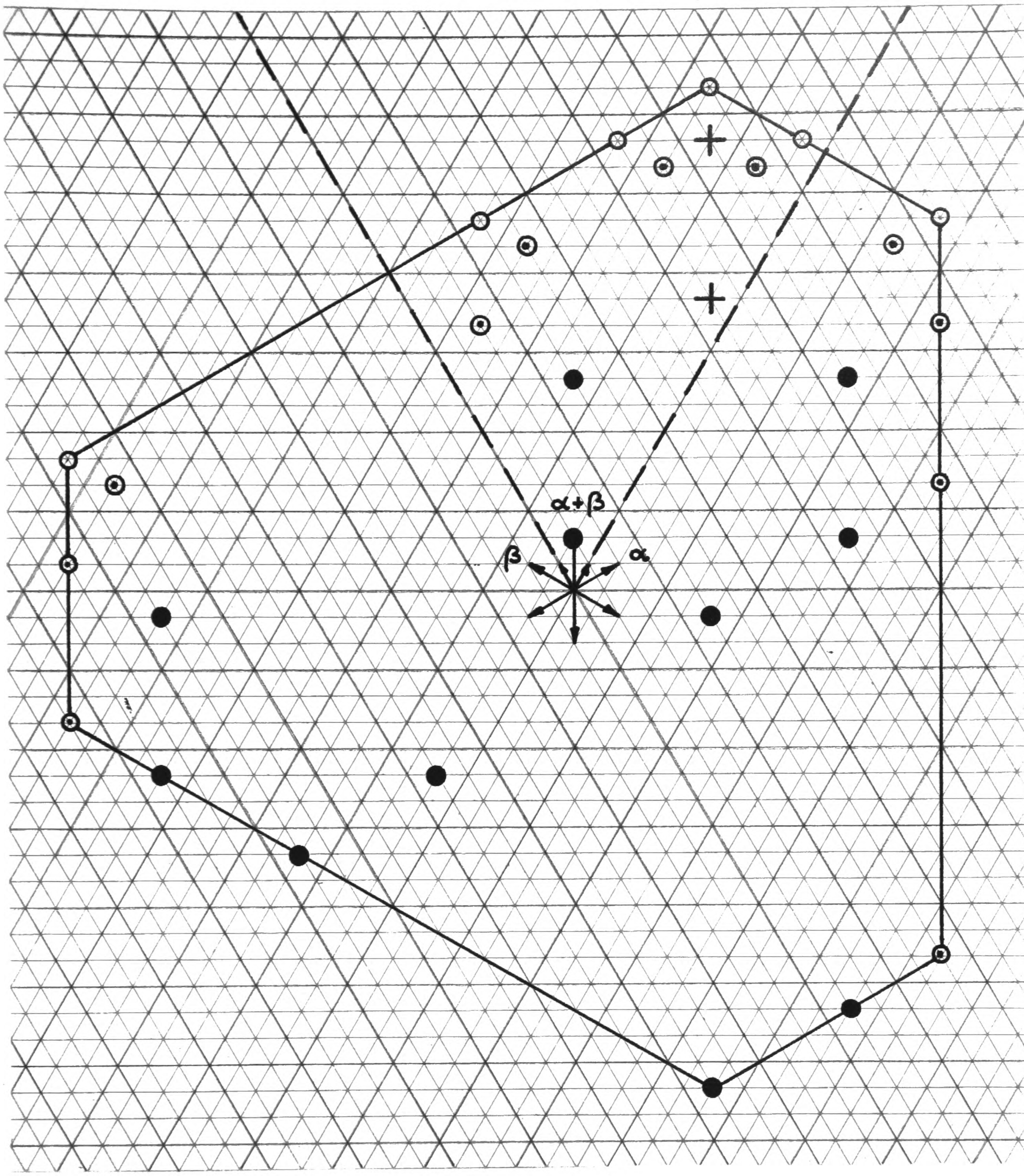
Case by case analysis, where $n \equiv m \equiv r+s+2 \equiv 1 \pmod p$, shows that $\mu = \lambda - n\alpha - m\beta$ is a primitive weight for

$$\begin{aligned}(n,m) \in \{&(1,1),(4,4),(4,10),(4,19),(7,7),(7,10),(7,19),(10,4),\\ &(10,7),(10,25),(16,10),(16,16),(16,25),(25,19),(25,25)\}.\end{aligned}$$

Hence by finding first, second and third generation primitive weights we missed out on

$$(n,m) \in \{(1,1),(4,4),(4,10),(7,7)\}.$$

In this case $(4,7)$ is not an element on the diagonal and it is not a second generation primitive weight. See Figure 3.3. Numerous examples were calculated, but no general conjecture describing the total set of primitive weights in $Z(\lambda)$ could be extracted.

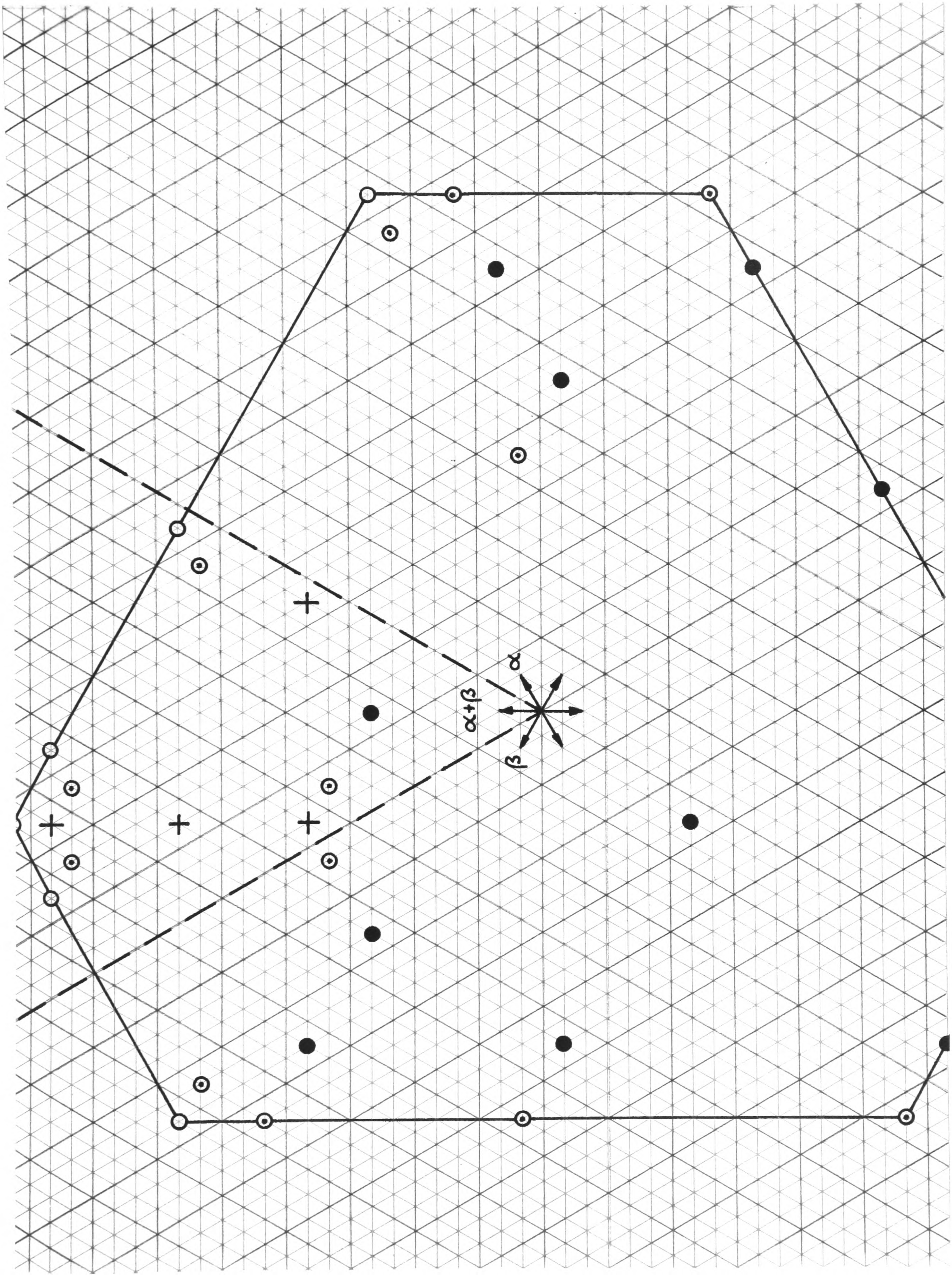


○ 1st generation ● 3rd generation
⊙ 2nd generation + additional

Figure 3.2: Primitive weights in $Z(13,4)$ for $p=3$.

On the following page we find

Figure 3.3: Primitive weights in $Z(7,16)$ for $p=3$.


α
α+β
β

Chapter 4

Twisted tensor products

We find some tensor product results in this chapter. For weights $\lambda \in X$ of the special kind $\lambda = p^n\lambda_1 + (p^n - 1)\rho$ with $\lambda_1 \in X$, we show that $Z(\lambda)$ is isomorphic to the tensor product of the n-th Steinberg module with the n-th Frobenius twisted $Z(\lambda_1)$. For $\mathcal{G} = sl_2$ we see that for $\lambda + \rho \in X^+$ it suffices to determine $Z(\mu)$ for certain weights $\mu \in X_1$, and then tensor them together appropriately to obtain $Z(\lambda)$. Analogue results are known for Weyl modules, see [Jantzen 3] Bemerkung 3.8 (2).

4.1 Twisted tensor products

For characteristic p Verma modules, we get

Proposition 4.1.1 *Let U be a hyperalgebra. Let $n \in \mathbf{Z}_{>0}$, $\lambda_1 \in X$, and $\lambda = p^n\lambda_1 + (p^n - 1)\rho \in X$. Then*

$$Z(\lambda) \simeq St_n \otimes Z(\lambda_1)^{F^n},$$

where $St_n = L((p-1)\rho) \otimes L((p-1)\rho)^F \cdots \otimes L((p-1)\rho)^{F^{n-1}}$ is the n-th Steinberg module.

Before proving this, let us have a look at an example, and the following lemmas.

Lemma 4.1.2 *Let v be a highest weight vector generating $L((p-1)\rho))$, then*

$$\prod_{\alpha\in\Phi^+} X_{-\alpha,p-1+pm_\alpha}v \neq 0$$

implies $m_\alpha = 0$ for all $\alpha \in \Phi^+$.

Proof: Assume there exists a $m_\alpha \neq 0$, then $m_\alpha > 0$ and the weight we obtain is lower than the lowest weight in $L((p-1)\rho)$, and we have a contradiction. □

Lemma 4.1.3 *Let $\lambda = p\lambda_1 + \lambda_0$, where $\lambda_0 \in X_1$, and $\lambda_1 \in X$. Let x, v and w be highest weight vectors generating $Z(\lambda)$, $\hat{Z}_1(\lambda_0)$ and $Z(\lambda_1)^F$, respectively. Then we have a U^0-isomorphism*

$$\eta : Z(\lambda) \to \hat{Z}_1(\lambda_0) \otimes Z(\lambda_1)^F,$$

where $\eta(\prod_{\alpha\in\Phi^+} X_{-\alpha,m_\alpha}x) = (\prod_{\alpha\in\Phi^+} X_{-\alpha,m_{\alpha0}}v)\otimes(\prod_{\alpha\in\Phi^+} X_{-\alpha,m_{\alpha1}}w)$ with $m_\alpha = m_{\alpha0}+pm_{\alpha1}$ for $0 \leq m_{\alpha0} \leq p-1$ and $0 \leq m_{\alpha1}$.

Proof: Since by definition η is K-linear and maps the K-basis to the K-basis, we only have to show that the map preserves the weight-spaces. This follows from Remark 1.3.3 in Chapter 1. □

Example 4.1.4 Let $\mathcal{G} = sl_2, p = 3$, then we find the following example, by use of [Mowbray 1] Theorem 2.1: $\lambda = 5 = (2,1,0,---), \lambda_0 = 2$ and $\lambda_1 = 1$. The result is shown in Figure 4.1. The weight -7 is obtained as $2+p(-3)$, -13 as $2+p(-5)$ and so on, up to $5 = 2+p\cdot 1$.

Now we can prove Proposition 4.1.1.

Proof: Let us begin with $n = 1$. Assume that v, w, and x are highest weight vectors generating $L((p-1)\rho)$, $Z(\lambda_1)^F$ and $Z(\lambda)$, respectively. Recall that $Z(\lambda_1)^F$ has K-basis $\{\prod_{\alpha\in\Phi^+} X_{-\alpha,m_\alpha}w \mid 0 \leq m_\alpha\}$ and $L((p-1)\rho)$ has K-basis $\{\prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha}v \mid 0 \leq n_\alpha < p\}$. It is easy to see that $v \otimes w$ is a highest weight vector of highest weight λ, and hence, by

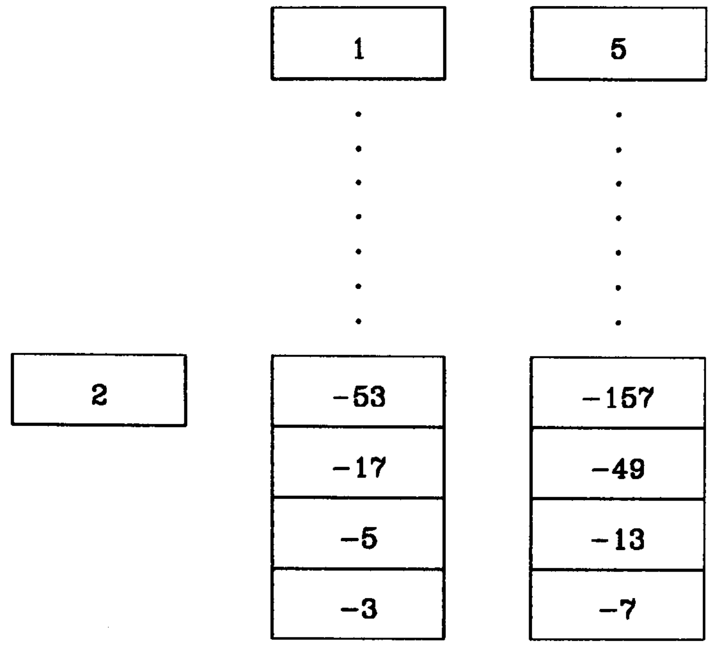


Figure 4.1: $Z(5) \simeq L(2) \otimes Z(1)^1$ for $\mathcal{G} = sl_2$ and $p = 3$.

the universal property of Verma modules, we have a well-defined U-homomorphism

$$\psi : Z(\lambda) \to L((p-1)\rho) \otimes Z(\lambda_1)^F,$$

where $\psi(ux) = u(v \otimes w)$ for $u \in U$. We prove that ψ is an isomorphism. Let b_1 be an element of the K-basis of $L((p-1)\rho)$, and b_2 an element of the K-basis of $Z(\lambda_1)^F$, then the following induction argument on the weight of b_1 shows that $b_1 \otimes b_2 \in \mathrm{Im}\psi$. The smallest possible weight in $L((p-1)\rho)$ is $-(p-1)\rho$, and it is only obtained for $b_1 = \prod_{\alpha\in\Phi^+} X_{-\alpha,p-1}v$. Using Lemmas 1.3.2 and 4.1.2 and recalling the Frobenius action we get

$$\begin{aligned}
\psi(\prod_{\alpha\in\Phi^+} X_{-\alpha,p-1+pm_\alpha}x) &= \prod_{\alpha\in\Phi^+} X_{-\alpha,p-1+pm_\alpha}\psi(x) \\
&= \prod_{\alpha\in\Phi^+} X_{-\alpha,p-1+pm_\alpha}(v\otimes w) \\
&= \prod_{\alpha\in\Phi^+} \sum_{0\le j_\alpha\le p-1+pm_\alpha} (X_{-\alpha,p-1+pm_\alpha-j_\alpha}v \otimes F(X_{-\alpha,j_\alpha})w) \\
&= \prod_{\alpha\in\Phi^+} \sum_{0\le j_\alpha\le m_\alpha} (X_{-\alpha,p-1+pm_\alpha-pj_\alpha}v \otimes X_{-\alpha,j_\alpha}w) \\
&= b_1 \otimes \prod_{\alpha\in\Phi^+} X_{-\alpha,m_\alpha}w.
\end{aligned}$$

We observe that

$$\begin{aligned}\psi(\prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha+pm_\alpha}x) &= \prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha}v\otimes F(\prod_{\alpha\in\Phi^+} X_{-\alpha,pm_\alpha})w+\sum\hat{b_1}\otimes\hat{b_2} \\ &= \prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha}v\otimes \prod_{\alpha\in\Phi^+} X_{-\alpha,m_\alpha}w+\sum\hat{b_1}\otimes\hat{b_2},\end{aligned}$$

where the sum is over different weight vectors $\hat{b}_1 \in L((p-1)\rho)$ and $\hat{b}_2 \in Z(\lambda_1)^F$. For all $\hat{b_1}$ in the sum the weight is strictly smaller than the weight of $\prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha}v$, and hence, by induction assumption, we know that the sum is contained in $\mathrm{Im}\psi$. Thus ψ is surjective.

We know $\hat{Z}_1((p-1)\rho) \simeq L((p-1)\rho)$ by [Jantzen] p. 338, and from Lemma 4.1.3 we get a U^0-isomorphism. Hence injectivity of ψ follows.

The remainder of the statement follows by induction, noticing that $St_n = L((p-1)\rho)\otimes St_{n-1}^F$, and λ can be written $\lambda = p^n\lambda_1 + (p^n-1)\rho = p(p^{n-1}\lambda_1 + (p^{n-1}-1)\rho)) + (p-1)\rho$. □

4.2 Exact sequences, for $\mathcal{G} = sl_2$

We restrict our interest to the case $\mathcal{G} = sl_2$, and find

Proposition 4.2.1 *Let U be the hyperalgebra for sl_2. Let $\lambda \in X$ such that $\lambda = p\lambda' + \lambda_0$, where $0 \le \lambda_0 \le p-2$ and $\lambda' \in X$, then we have*

(1) a short exact sequence of U-modules

$$0 \to M \otimes Z(\lambda'-\rho)^F \to Z(\lambda) \to M' \otimes Z(\lambda')^F \to 0,$$

where $M \simeq L(p-2-\lambda_0)$ and $M' \simeq L(\lambda_0)$

(2) a long exact sequence of U-modules

$$\cdots \to Z(\lambda_{-1}) \to Z(\lambda_0) \to Z(\lambda_1) \to Z(\lambda_2) \to \cdots$$

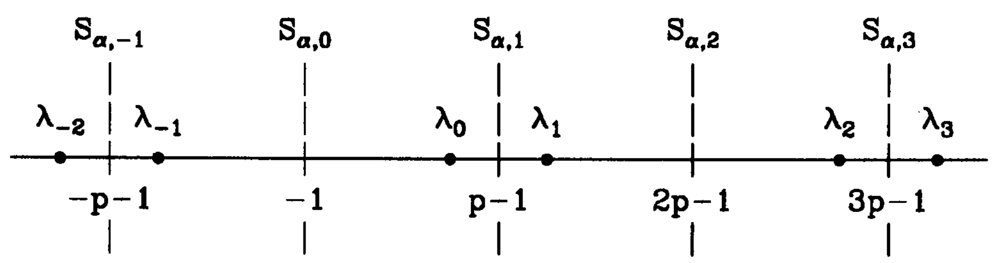


Figure 4.2: Reflection in the walls

where $i \in \mathbf{Z}_{>0}$, $\lambda_i = s_{\alpha,i}s_{\alpha,i-1}\cdots s_{\alpha,1}.\lambda_0$ *and* $\lambda_{-i} = s_{\alpha,-(i-1)}s_{\alpha,-(i-2)}\cdots s_{\alpha,0}.\lambda_0$. *See Figure 4.2.*

Proof: (1) Assume v, w, $\hat{v}$, $\hat{w}$ and x are highest weight vectors generating the modules $L(\lambda_0)$, $Z(\lambda')^F$, $L(p-2-\lambda_0)$, $Z(\lambda'-\rho)^F$ and $Z(\lambda)$, respectively. By the universal property we have a homomorphism

$$\psi : Z(p\lambda' + \lambda_0) \to L(\lambda_0) \otimes Z(\lambda')^F,$$

where $\psi(ux) = u(v \otimes w)$. We get

$$\begin{aligned}
\psi(X_{-\alpha,pm_1+m_0}x) &= X_{-\alpha,pm_1+m_0}\psi(x) \\
&= X_{-\alpha,pm_1+m_0}(v \otimes w) \\
&= \sum_{0\le i\le pm_1+m_0} X_{-\alpha,pm_1+m_0-i}v \otimes F(X_{-\alpha,i})w \\
&= \sum_{0\le j\le m_1} X_{-\alpha,pm_1+m_0-pj}v \otimes X_{-\alpha,j}w \\
&= X_{-\alpha,m_0}v \otimes X_{-\alpha,m_1}w,
\end{aligned}$$

where the last equality follows since $L(\lambda_0)$ has K-basis $\{X_{-\alpha,m}v \mid 0 \le m \le \lambda_0\}$. The surjectivity of ψ follows.

If $m > \lambda_0 + 1$, then Lemma 1.6.1 gives that $X_{\alpha,m}X_{-\alpha,\lambda_0+1}x = 0$. Now let $1 \leq m \leq \lambda_0 + 1$, then by Corollary 1.6.2 and Lemma 1.2.3

$$\begin{aligned} X_{\alpha,m}X_{-\alpha,\lambda_0+1}x &= \binom{\lambda - \lambda_0 - 1 + m}{m} X_{-\alpha,\lambda_0+1-m}x \\ &= \binom{p\lambda' - 1 + m}{m} X_{-\alpha,\lambda_0+1-m}x = 0, \end{aligned}$$

and we obtain that the vector $y = X_{-\alpha,\lambda_0+1}x$ is a primitive weight vector in $Z(\lambda)$.

By the universal property we have U-homomorphisms, $\hat{\psi}$ and θ, from $Z(p\lambda' - 2 - \lambda_0)$ to $L(p - 2 - \lambda_0) \otimes Z(\lambda' - 1)^F$ and $Z(\lambda)$, respectively.

$$\begin{tikzcd} Z(p\lambda' - 2 - \lambda_0) \arrow[rr, "\hat{\psi}"] \arrow[dr, "\theta"'] & & L(p - 2 - \lambda_0) \otimes Z(\lambda' - 1)^F \\ & Z(\lambda) \arrow[ur, dashed, "\eta"'] & \end{tikzcd}$$

Let $u \in U$, and let z be the highest weight vector generating $Z(p\lambda' - 2 - \lambda_0)$, then we know that

$$\hat{\psi}(uz) = u(\hat{v} \otimes \hat{w}),$$

and

$$\theta(uz) = uy = uX_{-\alpha,\lambda_0+1}x.$$

Since z, v, w and y are primitive weight vectors, we only need to consider u of the form

$$u = \sum_i c_i X_{-\alpha,i},$$

where $c_i \in K$. If we show that $\mathrm{Ker}\hat{\psi} \subseteq \mathrm{Ker}\theta$, the fundamental homomorphism theorem gives us a U-homormorphism, η, such that $\eta \circ \hat{\psi} = \theta$. If we show that $\mathrm{Ker}\hat{\psi} = \mathrm{Ker}\theta$, we obtain that η is injective, since surjectivity of $\hat{\psi}$ follows similarly to surjectivity of ψ above. Recall that the usual K-basis of $L(p - 2 - \lambda_0) \otimes Z(\lambda' - \rho)^F$ is of the form

$X_{-\alpha,m_0}\hat{v} \otimes X_{-\alpha,m_1}\hat{w} = X_{-\alpha,m_0+pm_1}(\hat{v}\otimes\hat{w})$ for $0 \leq m_0 \leq p-2-\lambda_0$. Assume that $u \in$ Ker$\hat{\psi}$, then

$$\begin{aligned} 0 &= u(\hat{v}\otimes\hat{w}) \\ &= \sum_i c_i X_{-\alpha,i}(\hat{v}\otimes\hat{w}) \\ &= \sum_i c_i \sum_{j=0}^{i} X_{-\alpha,i-j}\hat{v} \otimes F(X_{-\alpha,j})\hat{w} \\ &= \sum_i c_i X_{-\alpha,i_0}\hat{v} \otimes X_{-\alpha,i_1}\hat{w}, \end{aligned}$$

where $i = pi_1 + i_0$ with $0 \leq i_0 \leq p-1$. This is zero exactly when c_i is zero or $p-2-\lambda_0 < i_0 \leq p-1$. Assume that $u \in$ Kerθ, then

$$\begin{aligned} 0 &= \theta(uz) = uy = \sum_i c_i X_{-\alpha,i}X_{-\alpha,\lambda_0+1}x \\ &= \sum_i c_i \binom{i+\lambda_0+1}{\lambda_0+1} X_{-\alpha,i+\lambda_0+1}x, \end{aligned}$$

which is zero exactly when c_i or $\binom{i+\lambda_0+1}{\lambda_0+1}$ is zero. Since $\lambda_0+1<p$ we know that $\binom{i+\lambda_0+1}{\lambda_0+1}$ is zero exactly when $p-2-\lambda_0 < i_0 \leq p-1$. This implies that Ker$\hat{\psi}$ =Kerθ, and η is injective.

It is clear that $\psi\circ\eta = 0$, hence Im$\eta \subseteq$ Kerψ. The other inclusion follows by comparing the weight spaces: We know that $\hat{Z}_1(\lambda_0)$ has exactly the two simples $L(\lambda_0)$ and $L(p-2-\lambda_0)$ as composition factors. Therefore the weights appearing in the two end-terms of the exact sequence are

$$\{\lambda_0 - 2j + p(\lambda' - 2m) \mid 0 \leq j \leq p-1, m \geq 0\}.$$

These are exactly the weights of $Z(\lambda)$.

(2) Follows from (1) by noting that the short exact sequences fit together as can be seen in Figure 4.3. $\square$

$$\begin{tikzcd}[column sep=small]
0 \arrow[dr] & & & & 0 \arrow[dr] & & 0 & & \\
& L(\lambda_0)\otimes Z(-2)^F \arrow[dr] & & & & L(\lambda_0)\otimes Z(0)^F \arrow[ur] \arrow[dr] & & & \\
{} \arrow[rr] & & Z(\lambda_{-1}) \arrow[rr] \arrow[dr] & & Z(\lambda_0) \arrow[rr] \arrow[ur] & & Z(\lambda_1) \arrow[rr] \arrow[dr] & & {} \\
& & & L(p-2-\lambda_0)\otimes Z(-1)^F \arrow[ur] \arrow[dr] & & & & L(p-2-\lambda_0)\otimes Z(1)^F \arrow[ur] \arrow[dr] & \\
& & 0 \arrow[ur] & & 0 & & 0 \arrow[ur] & & 0
\end{tikzcd}$$

Figure 4.3: Long exact sequence.

Remark 4.2.2 The same sort of arguments can be used to obtain a generalized version of Steinberg's tensor product theorem,

$$L(\lambda) \simeq \otimes_{i\geq 0} L(\lambda_i)^{F^i},$$

see [Steinberg 2] or [Haboush].

Remark 4.2.3 Let $\lambda \in X^+$ and $\mathcal{G} = sl_2$. Using Proposition 4.2.1, the problem of finding a description of the Verma module $Z(\lambda)$ can be reduced to establishing the structure of the Verma modules for weights $\mu \in X_1$ determined from λ, and tensoring the results together. For $\mu \in X_1$ we have that $Z(\mu)$ is uniserial (this follows from the description of sl_2 Verma modules in [Mowbray 1]).

Example 4.2.4 Let $\mathcal{G} = sl_2$ and $p = 3$, and have a look at $Z(\lambda)$ for $\lambda = p\hat{\lambda} + \lambda_0 = 19 = (1, 0, 2, 0, - - -)$, $\hat{\lambda} = 6$, and $\lambda_0 = 1$. Then we have a short exact sequence

$$0 \to L(0) \otimes_K Z(5)^F \to Z(19) \to L(1) \otimes_K Z(6)^F \to 0.$$

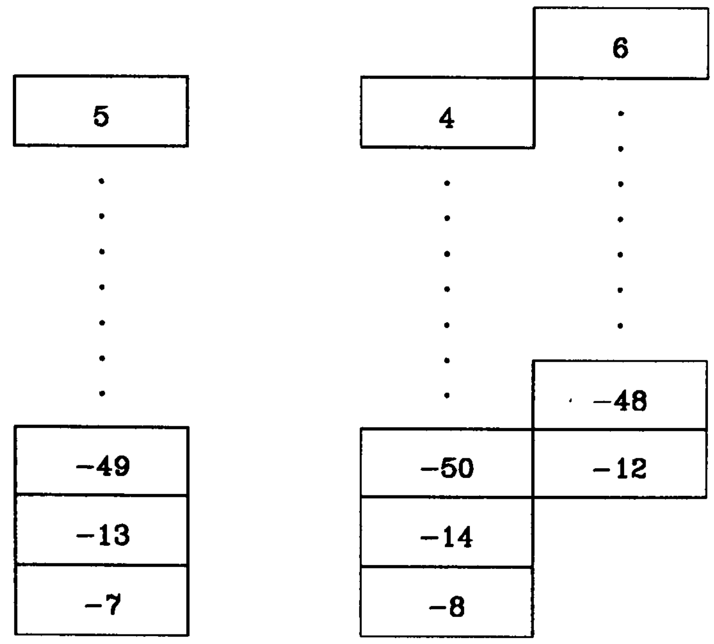


Figure 4.4: $Z(5)$ and $Z(6)$

Using the methods from [Mowbray 1] we find the composition series depicted in Figures 4.4 and 4.5.

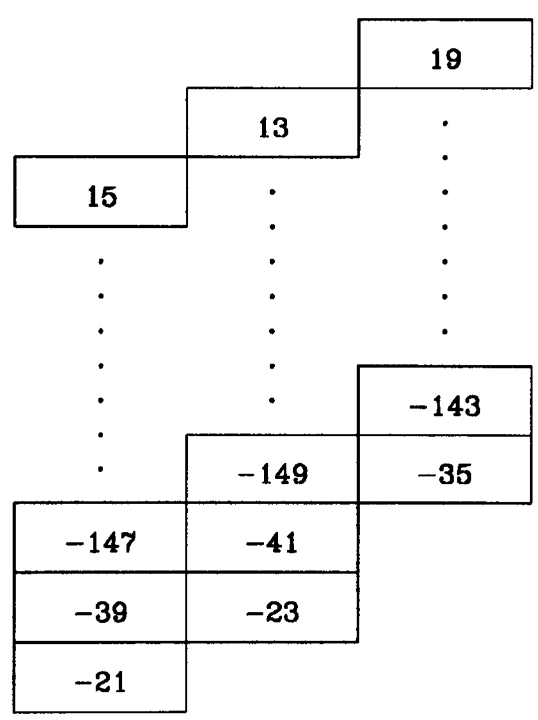


Figure 4.5: $Z(19)$

Chapter 5

Concerning the hyperalgebra

In this chapter we consider the connection between the subalgebra u_1^- of the hyperalgebra U for a finite dimensional semisimple Lie algebra, and a group algebra KG for some suitable p-group G. In special cases, u_1^- and the group algebra KG are isomorphic; however, this does not hold in general, and a bound on the characteristic of the field is found. Before doing this, some properties of the hyperalgebra are established.

Let us remark that because of the symmetry between u_n^- and u_n^+, we may work with either subalgebra. Because of its closer connection to Verma modules, we specifically chose to work with the former.

Throughout this chapter we adopt the notation $\Lambda = u_1^-$, and also we assume that we have a fixed ordering on the roots.

5.1 Alternative K-bases

5.1.1 An alternative K-basis of u_1^-

Let us recall that u_n^- has a K-vector space basis

$$\left\{ \prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha} \mid 0 \le n_\alpha < p^n \right\}, \tag{5.1}$$

and especially for Λ a K-basis is

$$\left\{ \prod_{\alpha\in\Phi^+} X_{-\alpha,n_\alpha} \mid 0 \leq n_\alpha < p \right\}, \tag{5.2}$$

which is of cardinality $p^{|\Phi^+|}$.

For $\alpha \in \Phi^+$, let $\mathcal{X}_\alpha$ be defined by

$$\mathcal{X}_\alpha = \sum_{j=0}^{p-1} X_{-\alpha,j}.$$

We note $(X_{-\alpha,1})^a = a!X_{-\alpha,a}$ in U, and we find $\mathcal{X}_\alpha = \exp(X_{-\alpha,1})$ in u_1^-. Similarly, define

$$\mathcal{X}_{\alpha,p^i} = \sum_{j=0}^{p-1} X_{-\alpha,p^i j}.$$

In the associated Chevalley group, G, we have some interesting equalities (see [Steinberg] Lemma 15). For example for $\mathcal{G} = sl_3$

$$\exp(X_{-\beta})\exp(X_{-\alpha}) = \exp(X_{-\alpha})\exp(X_{-\beta})\exp(X_{-\alpha-\beta}) \quad \text{in } G.$$

It would be desirable that these equalities also hold in u_1^-, but unfortunately they do not. The following example points to the general problem. Let $\mathcal{G} = sl_3$, $p = 2$, then

$$\mathcal{X}_\beta\mathcal{X}_\alpha = (1 + X_{-\beta,1})(1 + X_{-\alpha,1}) = 1 + X_{-\alpha,1} + X_{-\beta,1} + X_{-\alpha,1}X_{-\beta,1} + X_{-\alpha-\beta,1},$$

but, on the other hand,

$$\mathcal{X}_\alpha\mathcal{X}_\beta\mathcal{X}_{\alpha+\beta} = (1 + X_{-\alpha,1})(1 + X_{-\beta,1})(1 + X_{-\alpha-\beta,1}).$$

Recall that $X_{-\alpha,i}X_{-\alpha,j} = \binom{i+j}{j}X_{-\alpha,i+j}$, and $(m+1)^k = \sum_{j=0}^{k}\binom{k}{j}m^j$, then by induction on m we obtain

$$\mathcal{X}_\alpha^m = \sum_{j=0}^{p-1} m^j X_{-\alpha,j}. \tag{5.3}$$

We call $\psi \subseteq \Phi^+$ *closed*, if $\alpha, \beta \in \psi$ and $\alpha+\beta \in \Phi^+$ implies $\alpha+\beta \in \psi$. Assume ψ to be closed throughout this section. By the notation $n^+(\psi)$ we mean $\oplus_{\alpha\in\psi} K X_\alpha$, which is a Lie subalgebra of $\mathcal{G}$. The restricted enveloping algebra of $n^+(\psi)$, denoted $u_1^-(n^+(\psi))$, is $\langle X_{-\alpha,1} \mid \alpha \in \psi\rangle$. With a given ordering of the roots in ψ, the algebra $u_1^-(n^+(\psi))$ has a K-basis

$$\left\{ \prod_{\alpha\in\psi} X_{-\alpha,n_\alpha} \mid 0 \le n_\alpha < p \right\}, \tag{5.4}$$

which is of order $p^{|\psi|}$. Similarly, we have $u_n^-(n^+(\psi))$ which is $\langle X_{-\alpha,p^j} \mid 0 \le j < n,\ \alpha \in \psi\rangle$. With a given ordering of the roots in ψ, the algebra $u_n^-(n^+(\psi))$ has a K-basis

$$\left\{ \prod_{\alpha\in\psi} X_{-\alpha,n_\alpha} \mid 0 \le n_\alpha < p^n \right\}. \tag{5.5}$$

Proposition 5.1.1 *For $\psi \subseteq \Phi^+$ closed with a given ordering on the roots,*

$$\left\{ \prod_{\alpha\in\psi} \mathcal{X}_\alpha^{r_\alpha} \mid 0 \le r_\alpha < p \right\}, \tag{5.6}$$

is a K-basis of $u_1^-(n^+(\psi))$.

Proof: We show that the elements in (5.6) are K-linearly independent. If so, the result follows, since the two sets, (5.4) and (5.6), have the same cardinality. For suitable choices of orderings of the two sets, we express the elements of (5.6) in the K-basis (5.4), and establish that the determinant of the resulting $(p^{|\psi|} \times p^{|\psi|})$ matrix is non-zero. We proceed by induction on $|\psi|$. For $\psi = \{\alpha\}$, let V be the matrix whose columns correspond to elements of

$$\left\{1, \mathcal{X}_\alpha, \mathcal{X}_\alpha^2, \cdots, \mathcal{X}_\alpha^{p-1}\right\}, \tag{5.7}$$

expressed in the K-basis (5.4). Then, by (5.3),

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1^1 & 2^1 & 3^1 & \cdots & (p-1)^1 \\ 0 & 1^2 & 2^2 & 3^2 & \cdots & (p-1)^2 \\ & & \cdots & & & \\ & & \cdots & & & \\ 0 & 1^{p-1} & 2^{p-1} & 3^{p-1} & \cdots & (p-1)^{p-1} \end{pmatrix} \tag{5.8}$$

is a Vandermonde matrix with known determinant, $\prod_{0\leq i<j\leq p-1}(j-i)$, which is different from zero.

Assume that ψ is closed with $|\psi| = n$. It is then possible to choose an element, β say, such that $\tilde{\psi} = \psi\backslash\{\beta\}$ and $\{\beta\}$ are closed. By induction assumption we know that the elements of

$$\left\{\prod_{\alpha\in\tilde{\psi}} \mathcal{X}_\alpha^{r_\alpha} \mid 0 \leq r_\alpha < p\right\} \tag{5.9}$$

are K-linearly independent, and the elements of

$$\{1, \mathcal{X}_\beta, \mathcal{X}_\beta^2, \cdots, \mathcal{X}_\beta^{p-1}\} \tag{5.10}$$

are K-linearly independent. We now have two sets of K-linearly independent elements. Here tensoring over K yields linear independence of the elements of

$$\{\mathcal{X}_\beta^{r_\beta} \prod_{\alpha\in\tilde{\psi}} \mathcal{X}_\alpha^{r_\alpha} \mid 0 \leq r_\alpha, r_\beta < p\}. \tag{5.11}$$

□

In particular, taking $\psi = \Phi^+$ we have

Corollary 5.1.2 *The following is a K-basis of* $\Lambda = u_1^-$:

$$\left\{ \prod_{\alpha \in \Phi^+} \mathcal{X}_\alpha^{j_\alpha} \mid 0 \leq j_\alpha < p \right\}. \tag{5.12}$$

So we have two different K-bases for $\Lambda = u_1^-$.

5.1.2 An alternative K-basis of $u_n^-(sl_2)$

We find another K-basis of $u_n^-(sl_2)$.

Proposition 5.1.3 *The following is a K-basis of* $u_n^-(sl_2)$:

$$\left\{ \prod_{0 \leq i \leq n-1} \mathcal{X}_{\alpha,p^i}^{j_i} \mid 0 \leq j_i < p \right\}. \tag{5.13}$$

Proof: We note that the set (5.13) has the same cardinality as the set (5.1). Linear independence follows using the same arguments as in the proof of Proposition 5.1.1. □

5.1.3 An alternative K-basis of u_n^-

We can proceed further, to find

Proposition 5.1.4 *For* $\psi \subseteq \Phi^+$ *closed with a given ordering on the roots, the set*

$$\left\{ \prod_{\alpha \in \psi} \prod_{0 \leq i < n} \mathcal{X}_{\alpha,p^i}^{r_{\alpha,i}} \mid 0 \leq r_{\alpha,i} < p \right\}, \tag{5.14}$$

is a K-basis of $u_n^-(n^+(\psi))$.

Proof: The idea of the proof is very similar to that of Proposition 5.1.1. The result will follow from K-linear independence of the elements of (5.14), since the two sets, (5.5) and (5.14), have the same cardinality. We proceed by induction on $|\psi|$. For $\psi = \{\alpha\}$, the result follows from Proposition 5.1.3. Assume that ψ is closed. It is then possible to choose an element, β say, such that $\tilde{\psi} = \psi \backslash \{\beta\}$ and $\{\beta\}$ are closed. By induction assumption we know that the elements of

$$\left\{\prod_{\alpha\in\tilde{\psi}}\prod_{0\leq i<n}\mathcal{X}_{\alpha,p^i}^{r_{\alpha,i}} \mid 0\leq r_{\alpha,i}<p\right\} \tag{5.15}$$

are K-linearly independent, and the elements of

$$\left\{\prod_{0\leq j<n}\mathcal{X}_{\beta,p^j}^{r_{\beta,j}} \mid 0\leq r_{\beta,j}<p\right\} \tag{5.16}$$

are K-linearly independent. We now have two sets of K-linearly independent elements. Here tensoring over K yields linear independence of the elements of

$$\left\{\prod_{0\leq j<n}\mathcal{X}_{\beta,p^j}^{r_{\beta,j}}\prod_{\alpha\in\tilde{\psi}}\prod_{0\leq i<n}\mathcal{X}_{\alpha,p^i}^{r_{\alpha,p^i}} \mid 0\leq r_{\alpha,i},r_{\beta,j}<p\right\}. \tag{5.17}$$

□

Let $\psi=\Phi^+$. We obtain

Corollary 5.1.5 *The algebra u_n^- has K-basis*

$$\left\{\prod_{\alpha\in\Phi^+}\prod_{0\leq i<n}\mathcal{X}_{\alpha,p^i}^{r_{\alpha,i}} \mid 0\leq r_{\alpha,i}<p\right\}.$$

Theorem 5.1.6 *The algebra U^- has a K-basis*

$$\left\{\prod_{\alpha\in\Phi^+}\prod_{0\leq i\leq n}\mathcal{X}_{\alpha,p^i}^{r_{\alpha,i}} \mid n\in\mathbf{Z}_{\geq 0},\ \ 0\leq r_{\alpha,i}<p\right\}.$$

Proof: The result is an immediate consequence of Corollary 5.1.5, since U^- is the union of the u_n^-. □

5.2 The centre of the algebra

This section contains some observations about the centre of the algebras, u_n^-.

5.2.1 The centre of u_1^-

Let Λ be u_1^-, then the centre of Λ is $Z(\Lambda) = \{\omega \in \Lambda \mid \omega X_{-\alpha,1} = X_{-\alpha,1}\omega \text{ for all } \alpha \in \Phi^+\}$. From [Hump] Lemma A, p. 52 we know that relative to $\leq$ there is a unique maximal root, which we denote by $\tilde{\beta}$. We observe that $X_{-\tilde{\beta},i} \in Z(\Lambda)$ for $0 \leq i \leq p-1$. Furthermore, we notice that

$$X_{-\alpha,i}X_{-\alpha,j} = \binom{i+j}{i} X_{-\alpha,i+j}. \tag{5.18}$$

Especially for $j = p-1$ we get

$$X_{-\alpha,i}X_{-\alpha,p-1} = \binom{p-1+i}{i} X_{-\alpha,p-1+i}, \tag{5.19}$$

which is zero whenever $0 < i < p$.

Lemma 5.2.1 *For $\gamma \in \Phi^+ \setminus \Delta$ and $j \in \{1, \cdots, p-1\}$, we have*

$$X_{-\gamma,j} z = 0, \tag{5.20}$$

where $z = \prod_{\eta \in \Phi^+ \setminus \Delta} X_{-\eta,p-1}$. Actually place $X_{-\gamma,j}$ anywhere in z, and we get zero.

Proof: We notice that it suffices to show the result for $j = 1$, since $1 \leq j \leq p-1$. Let the height of a root α be $\text{ht}(\alpha) = \sum_{i=1}^{l} k_i$, if $\alpha = \sum_{i=1}^{l} k_i \alpha_i$ with $\alpha_i \in \Delta$. We know that $X_{-\gamma,p-1}$ appears in z, and in order to be able to use (5.19) we want to commute $X_{-\gamma,1}$ to there. Assume the first root in z with which γ does not commute is η_1, then while interchanging $X_{-\gamma,1}$ and $X_{-\eta_1,p-1}$ we get an additional term with $X_{-\gamma-\eta_1,1}$ in it. Moving $X_{-\gamma,1}$ further, we obtain an additional term with $X_{-\gamma-\eta_j,1}$ in it for each interchange where γ does not commute with η_j. We note that the absolute height of the root $-\gamma - \eta_j$ in the additional part $X_{-\gamma-\eta_j,1}$ is larger. Finally, we get $X_{-\gamma,1}$ moved to $X_{-\gamma,p-1}$, and according to (5.19) this is zero. Left are the additional terms. For each of those, we repeat the process of moving; this time $X_{-\gamma-\eta_j,1}$ to $X_{-\gamma-\eta_j,p-1}$. Since the absolute height of the root appearing in the additional term (to the additional term) is larger, we end up with additional terms including $X_{-\tilde{\beta},1}$, where $\tilde{\beta}$ is the maximal root. Since $\tilde{\beta}$ commute with everything the terms are zero because of (5.19). $\square$

Look at some element w in $\Lambda\prod_{\eta\in\Phi^+\setminus\Delta} X_{-\eta,p-1}$. In order to express w in the basis with the given ordering, we might have to interchange some elements in w, and therefore we get additional terms. In those terms $X_{-\gamma,a}$ appears for some $\gamma \in \Phi^+ \setminus \Delta$ and $0 < a < p$, and hence they vanish because of Lemma 5.2.1. Thus $\Lambda\prod_{\eta\in\Phi^+\setminus\Delta} X_{-\eta,p-1}$ has K-basis

$$\{X_{-\alpha_1,r_1}X_{-\alpha_2,r_2}\cdots X_{-\alpha_l,r_l}\prod_{\eta\in\Phi^+\setminus\Delta} X_{-\eta,p-1} \quad 0 \le r(1), r(2), \cdots, r(l) \le p-1\}, \qquad (5.21)$$

where $\{\alpha_1, \alpha_2, \cdots, \alpha_l\} = \Delta$.

Commuting an element from Λ with an element from $\Lambda\prod_{\eta\in\Phi^+\setminus\Delta} X_{-\eta,p-1}$ yields additional terms contributed from non-zero commutators, in which $X_{-\gamma,a}$ appears for some $\gamma \in \Phi^+ \setminus \Delta$ and $0 < a < p$. Again, these terms all vanish, and therefore $\Lambda\prod_{\eta\in\Phi^+\setminus\Delta} X_{-\eta,p-1} \subseteq Z(\Lambda)$. We have

$$\mathrm{span}_K\{1, X_{-\tilde{\beta},i}, 0 < i < p-1\} \oplus \Lambda \prod_{\eta\in\Phi^+\setminus\Delta} X_{-\eta,p-1} \subseteq Z(\Lambda). \qquad (5.22)$$

By counting we find $\dim_K(Z(\Lambda)) \ge p^{|\Delta|} + p - 1$.

In section 5.2.2 below we find a complete description of the centre of $u_n^-(sl_3)$ for $n \ge 1$. From this it follows that we obtain equality in (5.22).

Observation 5.2.2 In (5.22) equality does not hold in general; let $\mathcal{G}$ be of type sl_4 with root system $\Phi^+ = \{\alpha, \beta, \gamma, \alpha+\beta, \beta+\gamma, \alpha+\beta+\gamma\}$. We can represent $\mathcal{G}$ as the algebra of strictly upper triangular 4 by 4 matrices over K, and get the following signs:

$$[X_{-\beta}, X_{-\alpha}] = X_{-\alpha-\beta}, \quad [X_{-\gamma}, X_{-\beta}] = X_{-\beta-\gamma},$$

and

$$[X_{-\beta-\gamma}, X_{-\alpha}] = X_{-\alpha-\beta-\gamma} = [X_{-\alpha-\beta}, X_{-\gamma}].$$

The element $w = X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} - X_{-\beta,1}X_{-\alpha-\beta-\gamma,1}$ lies in the centre $Z(u_1^-(sl_4)) = Z(\Lambda)$, since Λ is generated by $X_{-\alpha,1}$, $X_{-\beta,1}$ and $X_{-\gamma,1}$, and we have

$$\begin{aligned}
X_{-\alpha,1}w &= X_{-\alpha,1}X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} - X_{-\alpha,1}X_{-\beta,1}X_{-\alpha-\beta-\gamma,1}, \\
wX_{-\alpha,1} &= X_{-\alpha,1}X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} + X_{-\alpha-\beta,1}X_{-\alpha-\beta-\gamma,1} \\
&- X_{-\alpha,1}X_{-\beta,1}X_{-\alpha-\beta-\gamma,1} - X_{-\alpha-\beta,1}X_{-\alpha-\beta-\gamma,1},
\end{aligned}$$

and

$$X_{-\beta,1}w = X_{-\beta,1}X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} - 2X_{-\beta,2}X_{-\alpha-\beta-\gamma,1}$$

$$wX_{-\beta,1} = X_{-\beta,1}X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} - 2X_{-\beta,2}X_{-\alpha-\beta-\gamma,1},$$

and

$$\begin{aligned}
X_{-\gamma,1}w &= X_{-\gamma,1}X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} - X_{-\beta,1}X_{-\gamma,1}X_{-\alpha-\beta-\gamma,1} - X_{-\beta-\gamma,1}X_{-\alpha-\beta-\gamma,1}, \\
wX_{-\gamma,1} &= X_{-\gamma,1}X_{-\alpha-\beta,1}X_{-\beta-\gamma,1} - X_{-\beta-\gamma,1}X_{-\alpha-\beta-\gamma,1} - X_{-\beta,1}X_{-\gamma,1}X_{-\alpha-\beta-\gamma,1}.
\end{aligned}$$

We note that w is not contained in the left hand side of (5.22).

5.2.2 The centre of $u_n^-(sl_3)$

We now restrict our interest to the Lie algebra $\mathcal{G} = sl_3$, and we obtain a complete description of the centre $Z(u_n^-(sl_3))$ for all $n \geq 1$. Throughout the subsection we use the notation $\Lambda_i = u_i^-(sl_3)$. Define $\Lambda_0 = K$.

Let $\Phi^+ = \{\alpha, \beta, \alpha+\beta\}$, and recall that in $u_n^-(sl_3)$ we have $X_{-\gamma,1}^p = X_{-\gamma,p}^p = \cdots = X_{-\gamma,p^{n-1}}^p = 0$ for all $\gamma \in \Phi^+$. With the sign choice for sl_3 introduced in Chapter 3, we have $X_{-\alpha-\beta,1} = [X_{-\beta,1}, X_{-\alpha,1}]$. Recall from Lemma 1.6.5 that $X_{-\alpha-\beta,a} = X_{-\beta,a}X_{-\alpha,a} - X_{-\alpha,a}X_{-\beta,a} - \sum_{j=1}^{j=a-1} X_{-\alpha,a-j}X_{-\beta,a-j}X_{-\alpha-\beta,j}$ for $1 \leq a < p^n$, and we see that the centre of Λ_n is

$$Z(\Lambda_n) = \{\omega \in \Lambda_n \mid \omega X_{-\gamma,j} = X_{-\gamma,j}\omega,\ 0 \leq j < p^n \text{ for all } \gamma \in \Phi^+\}$$

$$= \{\omega \in \Lambda_n \mid \omega X_{-\gamma,p^i} = X_{-\gamma,p^i}\omega,\ 0 \leq i < n \text{ for all } \gamma \in \Phi^+\}$$
$$= \{\omega \in \Lambda_n \mid \omega X_{-\gamma,p^i} = X_{-\gamma,p^i}\omega,\ 0 \leq i < n \text{ for all } \gamma \in \Delta\}.$$

Recall that for $k \in \mathbf{Z}_p$ we let $c = c_k$ be the smallest integer such that $k_c \neq p-1$. We notice that $X_{-\gamma,a}X_{-\gamma,k} = \binom{k+a}{a}X_{-\gamma,k+a}$, which is zero for $1 \leq a \leq p^c - 1$. Assume $k < p^i \leq p^n$, then, as can be seen by looking at the calculations in the proof below, $\Lambda_c \cdot X_{-\alpha-\beta,k}$ is contained in $Z(\Lambda_i)$, since every term contributed from a non-zero commutator vanishes. We have

$$\oplus_{0 \leq k \leq p^n-1} \Lambda_{c_k} \cdot X_{-\alpha-\beta,k} \subseteq Z(\Lambda_n). \tag{5.23}$$

In fact we obtain equality:

Proposition 5.2.3 *The centre of* Λ_n *is*

$$Z(\Lambda_n) = \oplus_{0 \leq k \leq p^n-1} \Lambda_{c_k} \cdot X_{-\alpha-\beta,k}.$$

Proof: According to (5.23) it is sufficient to check that no element from $\Lambda_n \setminus \oplus_{0 \leq k \leq p^n-1} \Lambda_{c_k} \cdot X_{-\alpha-\beta,k}$ is contained in the centre. These elements have the form

$$\omega = \sum_{i,j,k} c_{i,j,k} X_{-\alpha,i} X_{-\beta,j} X_{-\alpha-\beta,k},$$

where $c_{i,j,k} = 0$ whenever both i and j are strictly smaller than p^{c_k}, or phrased differently:

$$\text{If } c_{i,j,k} \neq 0, \text{ then either } i \text{ or } j \text{ is at least } p^{c_k}. \tag{5.24}$$

Using Lemma 1.6.5 we get

$$\omega X_{-\alpha,a} - X_{-\alpha,a}\omega = \sum c_{i,j,k} \sum_{l=1}^{a} \binom{a-l+i}{i}\binom{k+l}{l} X_{-\alpha,i+a-l} X_{-\beta,j-l} X_{-\alpha-\beta,k+l}, \tag{5.25}$$

and

$$X_{-\beta,a}\omega - \omega X_{-\beta,a} = \sum c_{i,j,k} \sum_{l=1}^{a} \binom{a-l+j}{j} \binom{k+l}{l} X_{-\alpha,i-l} X_{-\beta,j+a-l} X_{-\alpha-\beta,k+l}. \quad (5.26)$$

For ω to be in the centre we need (5.25) and (5.26) to be zero for $1 \leq a \leq p^n - 1$. Starting with $a = 1$ the two equations become

$$0 = \omega X_{-\alpha,1} - X_{-\alpha,1}\omega = \sum c_{i,j,k}(k+1) X_{-\alpha,i} X_{-\beta,j-1} X_{-\alpha-\beta,k+1}, \quad (5.27)$$

and

$$0 = X_{-\beta,1}\omega - \omega X_{-\beta,1} = \sum c_{i,j,k}(k+1) X_{-\alpha,i-1} X_{-\beta,j} X_{-\alpha-\beta,k+1}. \quad (5.28)$$

For $c_{i,j,k}$ to be non-zero (5.27) gives that $j = 0$ or $k + 1 \equiv 0 \pmod p$, and (5.28) gives $i = 0$ or $k + 1 \equiv 0 \pmod p$. By (5.24) we can not have $i = j = 0$, and therefore $k + 1 \equiv 0 \pmod p$, that is $c_k \geq 1$. Setting $a = p$ in (5.25) and (5.26), then we obtain $\binom{k+l}{l} \equiv 0 \pmod p$ unless $l = p$, and therefore

$$0 = \omega X_{-\alpha,p} - X_{-\alpha,p}\omega = \sum c_{i,j,k} \binom{k+p}{p} X_{-\alpha,i} X_{-\beta,j-p} X_{-\alpha-\beta,k+p}, \quad (5.29)$$

and

$$0 = X_{-\beta,p}\omega - \omega X_{-\beta,p} = \sum c_{i,j,k} \binom{k+p}{p} X_{-\alpha,i-p} X_{-\beta,j} X_{-\alpha-\beta,k+p}. \quad (5.30)$$

Equations (5.29) and (5.30) together imply that for $c_{i,j,k}$ to be non-zero either $i < p$ and $j < p$, or we have $c_k > 1$. From (5.24) we know that the former can not be the case, and therefore $c_k > 1$. This line of arguments continues for $a = p^2, p^3 \cdots, p^{n-1}$, and hence $c_k > n - 1$. Thus there are no elements in the centre of Λ_n, which are not in $\oplus_{0 \leq k \leq p^n - 1} \Lambda_{c_k} \cdot X_{-\alpha-\beta,k}$. □

Corollary 5.2.4 *The centre of Λ_n has K-dimension,*

$$\dim_K(Z(\Lambda_n)) = p^{n-1}(p^{n+1} + p^n - 1).$$

Proof: Follows from Proposition 5.2.3 by collecting terms with the same Λ_{c_k}, starting with Λ_{c_0}, and counting:

$$\begin{aligned}(p-1)p^{n-1} &+ p^2\cdot 1\cdot(p-1)p^{n-2}+p^4\cdot 1\cdot 1\cdot(p-1)p^{n-3}+\cdots\\ &+ p^{2(n-1)}\cdot 1\cdots 1\cdot(p-1)+p^{2n}\cdot 1\\ &= (p-1)p^{n-1}(1+p+p^2+\cdots p^{n-1})+p^{2n}\\ &= p^{n-1}(p^{n+1}+p^n-1)\ \square\end{aligned}$$

Corollary 5.2.5 *The centre of $U^-(sl_3)$ is*

$$Z(U^-(sl_3))=\oplus_{k\geq 0}\Lambda_{c_k}\cdot X_{-\alpha-\beta,k}.$$

Proof: An element in $Z(\Lambda_n)$ is in the centre of $U^-(sl_3)$ if and only if it lies in the intersection $\cap_{m>n}Z(\Lambda_m)$. $\square$

5.3 Generators and relations

This section contains a presentation of u_n^- as a quiver algebra with generators and relations. We use this description of u_n^- in section 5.4 below. Let Φ be the irreducible root system corresponding to $\mathcal{G}$ with simple roots $\Delta=\{\alpha_1,\alpha_2,\cdots,\alpha_l\}$, $l=|\Delta|$. With respect to $\leq$ we have a unique maximal root, call it $\tilde{\beta}$.

In u_1^- we have $X_{-\alpha,1}^p=0$ for all $\alpha\in\Phi^+$, and for $\alpha\in\Phi^+\setminus\Delta$ there exists a commutator, which generates $X_{-\alpha,1}$, e.g. $\alpha=\alpha_1+\alpha_2$, $X_{-\alpha,1}=c_{\alpha_1,\alpha_2}[X_{-\alpha_1,1},X_{-\alpha_2,1}]$ for some constant c_{α_1,α_2} (see [Hump] 25.2).

Observation 5.3.1 The quiver corresponding to u_1^- has one vertex and l arrows corresponding to $X_{-\alpha,1}$ for $\alpha\in\Delta$, call them $a_1,a_2,\cdots,a_l$. The relations $a_1^p=a_2^p=\cdots=a_l^p=0,(a_1a_2-a_2a_1)^p=0$ etc., which correspond to relations in u_1^-, are satisfied. For u_n^- we have $l\cdot n$ arrows corresponding to $X_{-\alpha,p^i}$ for $0\leq i<n$ and $\alpha\in\Delta$.

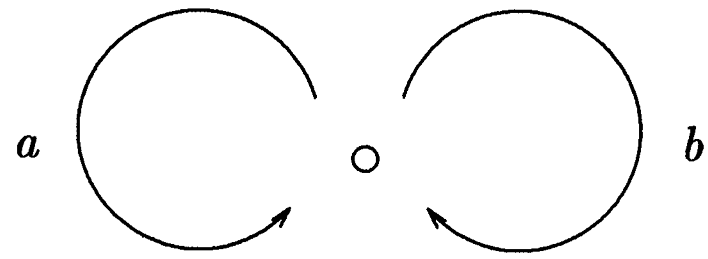


Figure 5.1: $u_1^-(sl_3)$ quiver.

Example 5.3.2 Recall the sign choice made for sl_3 in Chapter 3, $[X_{-\beta}, X_{-\alpha}] = X_{-\alpha-\beta}$.
(1) The quiver for $u_1^-(sl_3)$ has two arrows, a and b say, where a corresponds to $X_{-\alpha,1}$ and b to $X_{-\beta,1}$. The relations are

$$a^p = b^p = 0,\ (ba - ab)^p = 0,\ a(ba - ab) = (ba - ab)a,\ b(ba - ab) = (ba - ab)b.$$

Hence

$$u_1^-(sl_3) \simeq K\langle a, b\rangle/(a^p, b^p, (ba - ab)^p, a^2b - 2aba + ba^2, b^2a - 2bab + ab^2).$$

See Figure 5.1.
(2) The quiver for $u_2^-(sl_3)$ has four arrows, a, b, c and d say, where the correspondence is a to $X_{-\alpha,1}$, b to $X_{-\beta,1}$, c to $X_{-\alpha,p}$ and d to $X_{-\beta,p}$. See Figure 5.2. Use the notation $e = (dc - cd - \sum_{j=1}^{p-1} a^{p-j}/(p-j)!b^{p-j}/(p-j)!(ba - ab)^j/j!)$. Then the relations are

$$\begin{aligned}
&a^p = b^p = c^p = d^p = 0,\ (ba - ab)^p = 0,\ ac = ca,\ bd = db,\\
&a^2b - 2aba + ba^2,\ b^2a - 2bab + ab^2,\\
&c(ba - ab) = (ba - ab)c,\ d(ba - ab) = (ba - ab)d,\\
&e^p = 0,\ ae = ea,\ be = eb,\ ce = ec,\ de = ed,\\
&ad = da - bab^{p-1}/(p-1)!,\ bc = cb + aba^{p-1}/(p-1)!.
\end{aligned}$$

Using Wilsons theorem ($(p-1)! \equiv -1 \pmod{p}$), the relations can be somewhat simplified

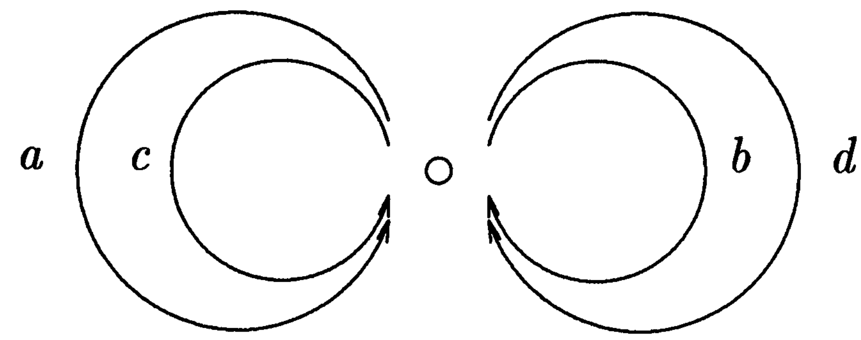


Figure 5.2: $u_2^-(sl_3)$ quiver.

to get

$$\begin{aligned} u_2^-(sl_3) \simeq K\langle a,b,c,d\rangle/ \quad & (a^p,\ b^p,\ c^p,\ d^p,\ (ba-ab)^p,\ e^p, \\ & ac-ca,\ bd-db,\ ad-da+bab^{p-1}, \\ & bc-cb+aba^{p-1}, \\ & c(ba-ab)-(ba-ab)c,\ d(ba-ab)-(ba-ab)d, \\ & ae-ea,\ be-eb,\ ce-ec,\ de-ed, \\ & a^2b-2aba+ba^2,\ b^2a-2bab+ab^2). \end{aligned}$$

5.4 A group algebra, KG

In this section the possibility of finding a suitable group G, such that u_1^- is isomorphic to the group algebra, KG, where K is a field of characteristic p, is investigated. And more generally we ask, whether we can find G, such that u_n^- is isomorphic to KG. Since the dimension of u_n^- is a power of p, the group is necessarily a p-group.

5.4.1 A surjective homomorphism

We define a group by

Definition 5.4.1 *Let G_n be the group*

$$G_n = \langle \mathcal{X}_{\alpha_i,p^j}, 0 \leq j \leq n-1, \alpha_i \in \Phi^+ \rangle,$$

where $\mathcal{X}_{\alpha_i,p^j} = \sum_{k=0}^{p-1} X_{-\alpha_i,kp^j} \in u_n^-$.

Especially we have

$$G_1 = \langle \mathcal{X}_{\alpha_i,1} \mid \alpha_i \in \Phi^+ \rangle.$$

Remark 5.4.2

(a) The group G_n is finite, since the elements are in the span of the $\prod_i X_{-\alpha_i,j_i}$ for $0 \leq j_i \leq p^n - 1$ over a finite field.

(b) For $\mathcal{G} = sl_2$ we have $G_n \simeq C_p \times C_p \times \cdots \times C_p$ with n copies of the cyclic group of order p.

Let K be a field of characteristic p, and G a finite group, then the *group algebra* KG has K-basis $\{g \mid g \in G\}$ with algebra multiplication induced by the group multiplication. For a subset X of G we write $[X]$ for the sum $\sum_{g \in X} g$. Then $[X]$ is an element in KG.

Lemma 5.4.3 *We have an algebra homomorphism,*

$$\psi : KG_1 \to \Lambda = u_1^-,$$

mapping $\mathcal{X}_{\alpha_i,1}$ to $\sum_{j=0}^{p-1} X_{\alpha_i,j}$. The homomorphism ψ is a surjection.

Proof: We have a natural map sending $\mathcal{X}_{\alpha_i,1}$ to $\sum_{j=0}^{p-1} X_{\alpha_i,j}$ and with linear extension we get an algebra homomorphism. According to Corollary 5.1.2, the image of the K-basis elements of KG_1 span Λ. Hence ψ is surjective. □

From [Passman] Lemma 3.4 we have

Lemma 5.4.4 *Let G be a finite group, and K a field. If $G = G_1 \times G_2$, then the group algebra is an algebra tensor product*

$$KG = K(G_1 \times G_2) \simeq KG_1 \otimes KG_2.$$

Proposition 5.4.5 *Let $\mathcal{G} = sl_2$, then we have*

$$u_n^-(sl_2) \simeq KG_n \simeq K(C_p \times C_p \times \cdots \times C_p),$$

for $n \geq 1$.

Proof: Since $\mathcal{X}_{\alpha,p^i}$ and $\mathcal{X}_{\alpha,p^j}$ commute, this is an immediate consequence of Lemma 5.4.4 and Proposition 5.1.3. □

Now we study the subalgebra u_1^- of the hyperalgebra for a finite dimensional semisimple Lie algebra. The main result is stated in Theorem 5.4.11 below. For the proof[1] we need some more general results and notation.

5.4.2 Conjugacy classes

Lemma 5.4.6 *Let H be any finite group. Let K be a field of $\mathrm{char}K = p$, and KH the group algebra of H over K, with group basis $\{h \mid h \in H\}$ and algebra multiplication given by the group multiplication, $g \cdot h = gh$. Let $C(H) = span_K\{xy - yx \mid x, y \in KH\}$, then*

$$C(H) = \{\sum c_h h \in KH \mid \sum_{h \in X} c_h = 0 \; for \; X \in Cl(H)\},$$

where $Cl(H)$ denotes the set of conjugacy classes of H.

Proof: This can be found on p. 426 in [Külshammer] □

We use the Lemma in the following way:

[1] The strategy was suggested by Dr K. Erdmann

Let $\Lambda = u_1^-$, and assume that $\Lambda \simeq KG$ for some finite p-group G. Let $\tilde{\beta}$ be the maximal root, then $X_{-\tilde{\beta},1} \in Z(\Lambda)$ and $X_{-\tilde{\beta},1} \in [\Lambda, \Lambda]$. From Lemma 5.4.6 follows that

$$X_{-\tilde{\beta},1} = \sum_{|\mathcal{C}_i|>1} c_i[\mathcal{C}_i], \tag{5.31}$$

where $[\mathcal{C}_i]$ is the class sum of the conjugacy class $\mathcal{C}_i$.

5.4.3 Loewy structure of Λ

The algebra Λ is local, since $\mathrm{span}_K\{X_{-\alpha_1,a_1}X_{-\alpha_2,a_2}\cdots X_{-\alpha_N,a_N} \mid a_i > 0 \text{ for some } i\}$ is a nilpotent ideal of codimension 1.

Let $J = \mathrm{rad}\Lambda$. We have Λ filtered by the powers of J; and by induction on $\mathrm{ht}(\alpha)$ it can be seen that

$$X_{-\alpha,1} \in J^a, \tag{5.32}$$

where $a = \mathrm{ht}(\alpha) = \sum_i a_i$ for $\alpha = \sum_i a_i\alpha_i$ with $\alpha_i \in \Delta$.

Let V be any finite dimensional U-module with highest weight λ. Set

$$V(r) = \oplus_{\mathrm{ht}(\lambda-\mu)\geq r} V_\mu,$$

then

$$\cdots \subset V(r) \subset V(r-1) \subset \cdots \subset V(1) \subset V(0) = V.$$

It is clear that

$$JV(r) \subseteq V(r+1),$$

and hence

$$J^r(V/V(r)) = 0.$$

Specify $V = St_1$, the Steinberg module, with highest weight vector v^+. Then V has a K-basis

$$X_{-\alpha_1,r_1}X_{-\alpha_2,r_2}\cdots X_{-\alpha_N,r_N}v^+,$$

where $0 \le r_i < p$. Looking at $X_{-\alpha,1}$ from (5.32) we get

$$X_{-\alpha,1}v^+ \in V(a) \setminus V(a+1).$$

Thus we obtain

$$X_{-\alpha,1}v^+ \notin J^{a+1}v^+,$$

and

$$X_{-\alpha,1} \notin J^{a+1}.$$

In particular, the maximal root $\tilde{\beta}$ is a sum of $g-1$ simple roots, where g is the Coxeter number, and therefore

$$X_{-\tilde{\beta},1} \in J^{g-1} \setminus J^g. \tag{5.33}$$

5.4.4 Loewy structure of KG

Suppose G is some p-group. We summarize results by Jennings (see for example [Huppert]) on the Loewy structure of KG.

Let $\psi : KG \to K$ be the algebra homomorphism sending $g \in G$ to 1. Denote by ω the augmentation ideal in KG, that is the ideal which is $\ker \psi$. We have a K-basis for ω

$$\mathrm{span}\{g - 1 \mid 1 \neq g \in G\}.$$

The augmentation ideal is nilpotent, hence we have $\omega^N = 0$ for some N. According to [Passmann] 8.1.17 the augmentation ideal is the Jacobson radical.

Let G_r be defined as

$$G_r = \{g \in G \mid g - 1 \in \omega^r\}.$$

Then we have a finite chain

$$1 = G_N \subseteq G_{N-1} \subseteq \cdots \subseteq G_2 \subseteq G_1 = G.$$

The G_r's are all normal subgroups of G, and $[G_r, G_s] \subseteq G_{r+s}$. Therefore G_r/G_{r+1} is abelian. Moreover, if $x \in G_r$, then $x^p \in G_{pr}$, since $x^p - 1 = (x-1)^p$ over a field of characteristic p. In particular, $x^p \in G_{r+1}$, and therefore the quotient group G_r/G_{r+1} is elementary abelian.

By [Huppert] VIII 2.7 we have

$$G_r = \kappa_r(G),$$

where $\kappa_r(G)$ is the group occurring in Jenning's Theorem:

$$\kappa_r(G) = \prod_{ip^k \geq r} \gamma_i(G)^{p^k}, \tag{5.34}$$

with γ_i defined by

$$\gamma_1(G) = G, \quad \gamma_i(G) = [\gamma_{i-1}(G), G] \text{ for } i > 1.$$

If $w \in G_i \setminus G_{i+1}$, then

$$(w-1) \in \omega^i \setminus \omega^{i+1} \tag{5.35}$$

according to [Huppert] VIII Theorem 2.6.

5.4.5 Class sums: reduction

We investigate bounds for k such that the class sums $[\mathcal{C}]$, where $|\mathcal{C}| > 1$, belong to J^k. The first step is a reduction:

It suffices to consider the conjugacy class of x in H, where $C_G(x)$ has index p in H.

To see this, let us recall the following known results: For a group W with elements y and z we have $C_W(z^y) = C_W(z)^y$. For a finite p-group G we have, G contains an element of order p, and furthermore, if H is a proper subgroup of G, then H is a proper subgroup of $N_G(H)$, the normalizer of H in G.

Now fix an element $x \in \mathcal{C}$, where $|\mathcal{C}| > 1$, then $C_G(x)$ is a proper subgroup of G. Furthermore, there exists an element $\hat{e} \neq \hat{g} \in N_G(C_G(x))/C_G(x)$ such that $\hat{g}^p = \hat{e} = C_G(x)$. For some $g \in N_G(C_G(x))\backslash C_G(x)$ we conclude $C_G(x) = \hat{g}^p = (gC_G(x))^p = g^pC_G(x)$, and hence $g^p \in C_G(x)$. That is there exists an element

$$g \in G \setminus C_G(x), g \in N_G(C_G(x)) \text{ and } g^p \in C_G(x).$$

Define a subgroup H of G by

$$H = \langle C_G(x), g\rangle \leq G.$$

Then $C_G(x)$ has index p in H. Let $\{x_i\}$ be coset representatives of H in G, and let $\tilde{\mathcal{C}}$ be the conjugacy class of x in H, then

$$[\mathcal{C}] = \sum[\tilde{\mathcal{C}}]^{x_i}.$$

Since J^k is closed under conjugation and addition we get the reduction:

$$[\tilde{\mathcal{C}}] \in J^k \text{ implies } [\mathcal{C}] \in J^k.$$

5.4.6 Class sums: Jennings basis

Keeping the same x as above, we now determine an expression of $[\tilde{\mathcal{C}}]$ in terms of a Jennings basis for KG (see [Huppert] Theorem VIII 2.6). We have $C_G(x) < H = \langle C_G(x), g\rangle$. Then the elements $1, g, g^2, \cdots, g^{p-1}$ are coset representatives for $C_G(x)$ in H, and with $x^g = g^{-1}xg$ we have

$$\tilde{\mathcal{C}} = \{x, x^g, x^{g^2}, \cdots, x^{g^{p-1}}\}. \tag{5.36}$$

Since all elements of H normalize $C_G(x)$, we get $C_G(x) = C_G(x^{g^i})$ for all $i \in \{0, 1, \cdots, p-1\}$, and therefore any two elements in $\tilde{\mathcal{C}}$ commute.

We introduce some additional notation. Let

$$w_1 = x^{-1}g^{-1}xg = x^{-1}x^g,$$

then $x^g = xw_1$. Observe that $(x^g)^g = (xw_1)^g = x^g w_1^g$, and let $w_2 = w_1^{-1}w_1^g$, then $w_1^g = w_1 w_2$, and therefore $x^{g^2} = xw_1^2 w_2$. Define

$$w_{i+1} = w_i^{-1}w_i^g \quad \text{for } i \geq 1.$$

We note that $w_1 \in G_2$, actually $w_i \in G_{i+1}$. Let r be maximal such that $w_r \neq 1$.

By an induction argument on k we obtain

$$x^{g^k} = xw_1^k w_2^{\binom{k}{2}} \cdots w_r^{\binom{k}{r}} \quad \text{for } 0 \leq k \leq p-1. \tag{5.37}$$

Let $X_i = w_i - 1 \in KG$, then (5.37) becomes

$$x^{g^k} = x(X_1+1)^k (X_2+1)^{\binom{k}{2}} \cdots (X_r+1)^{\binom{k}{r}} \quad \text{for } 0 \leq k \leq p-1. \tag{5.38}$$

Recalling (5.36) we obtain

$$[\tilde{C}] = x\sum_{k=0}^{p-1}(X_1+1)^k (X_2+1)^{\binom{k}{2}} \cdots (X_r+1)^{\binom{k}{r}}. \tag{5.39}$$

Recall that (5.39) may be expressed as a linear combination of monomials $X_1^{a_1}X_2^{a_2}\cdots X_r^{a_r}$, and the coefficients are given by binomial formulae.

We know that $w_1 \in G_2$, and Jenning's theory (see (5.35)) implies that $X_1 \in \omega^2$. Similarly, $w_i \in G_{i+1}$ implies $X_i \in \omega^{i+1}$. This means that $X_{g-1} \in \omega^g$. Furthermore, $X_i^a X_j^b \in \omega^{a(i+1)+b(j+1)}$. Now $X_1^{a_1}X_2^{a_2}\cdots X_r^{a_r} \in \omega^m$, where $m = \sum_{i=1}^{r} a_i(i+1)$.

5.4.7 Binomial coefficient formulae

By an induction argument on a, using Pascal's formula, we obtain

Lemma 5.4.7 *Let a and b be positive integers, then in* $\mathbf{Z}$

$$\sum_{k=0}^{a} \binom{k}{b} = \binom{a+1}{b+1}.$$

Corollary 5.4.8 *Let a and b be positive integers, then in* $\mathbf{Z}$

$$\sum_{k=0}^{p-1} \binom{k+a}{b+a} = \binom{p+a}{b+a+1}.$$

Proof: We obtain

$$\begin{aligned}
\sum_{k=0}^{p-1} \binom{k+a}{b+a} &= \sum_{s=0}^{p-1+a} \binom{s}{b+a} - \sum_{s=0}^{a-1} \binom{s}{b+a} \text{ where } s = k+a \\
&= \sum_{s=0}^{p-1+a} \binom{s}{b+a} \text{ by Lemma 5.4.7} \\
&= \binom{p+a}{b+a+1} \text{ by Lemma 5.4.7.}
\end{aligned}$$

□

Lemma 5.4.9 *Let a, b, c and k be positive integers, then in* $\mathbf{Z}$ *we have*

$$\binom{k}{a}\binom{k+c}{b+c} = \sum_{j=0}^{a} (-1)^{a-j} \binom{a+c}{a-j}\binom{b+c+j}{j}\binom{k+c+j}{b+c+j}.$$

Proof: For $a = 1$ we have

$$k\binom{k+c}{b+c} = (b+c+1)\binom{k+c+1}{b+c+1} - (c+1)\binom{k+c}{b+c}$$

And the induction step follows as

$$\binom{k}{a}\binom{k+c}{b+c} = (k-a+1)/a\binom{k}{a-1}\binom{k+c}{b+c}$$
$$= (k-a+1)/a\sum_{j=0}^{a-1}(-1)^{a-1-j}\binom{a-1+c}{a-1-j}\binom{b+c+j}{j}\binom{k+c+j}{b+c+j}$$

$$
\begin{aligned}
&= \sum_{j=0}^{a-1}(-1)^{a-j}\binom{a-1+c}{a-1-j}\binom{b+c+j}{j} \\
&\qquad ((a+c+j)/a\binom{k+c+j}{b+c+j} - (b+c+j+1)/a\binom{k+c+j+1}{b+c+j+1}) \\
&= (-1)^a\binom{a-1+c}{a-1}\binom{b+c}{0}(a+c)/a\binom{k+c}{b+c} \\
&\quad + \left[\sum_{j=1}^{a-1}(-1)^{a-j}\left\{\binom{a-1+c}{a-1-j}(a+c+j)/a\binom{b+c+j}{j}\right.\right. \\
&\qquad \left.\left. + \binom{a-1+c}{a-j}\binom{b+c+j-1}{j-1}(b+c+j)/a\right\}\binom{k+c+j}{b+c+j}\right] \\
&\quad + \binom{a-1+c}{0}\binom{b+c+a-1}{a-1}(b+a+c)/a\binom{k+c+a}{b+c+a} \\
&= (-1)^a\binom{a+c}{a}\binom{k+c}{b+c} \\
&\quad + \left[\sum_{j=1}^{a-1}(-1)^{a-j}\left\{\binom{a-1+c}{a-1-j}(a+c+j)/a\right.\right. \\
&\qquad \left.\left. + \binom{a-1+c}{a-j}j/a\right\}\binom{b+c+j}{j}\binom{k+c+j}{b+c+j}\right] \\
&\quad + \binom{b+c+a}{a}\binom{k+c+a}{b+c+a} \\
&= \sum_{j=0}^{a}(-1)^{a-j}\binom{a+c}{a-j}\binom{b+c+j}{j}\binom{k+c+j}{b+c+j},
\end{aligned}
$$

since

$$
\begin{aligned}
\binom{a-1+c}{a-1-j}(a+c+j)/a + \binom{a-1+c}{a-j}j/a
&= j/a\binom{a+c}{a-j} + (a+c)/a\binom{a-1+c}{a-1-j} \\
&= (j/a + (a-j)/a)\binom{a+c}{a-j} \\
&= \binom{a+c}{a-j}
\end{aligned}
$$

□

Lemma 5.4.10 *Let a, b and k be positive integer, then in* $\mathbf{Z}$

$$\binom{\binom{k}{a}}{b}$$

is a finite sum of binomial coefficients of the form

$$\binom{k+c}{a+c},$$

where $0 \leq c \leq a(b-1)$.

Proof: We have that

$$\binom{\binom{k}{a}}{b} = 1/b\left(\binom{k}{a} - b + 1\right)\binom{\binom{k}{a}}{b-1},$$

and by induction assumption $\binom{\binom{k}{a}}{b-1}$ is a finite sum of binomial coefficients of the form $\binom{k+c}{a+c}$, and therefore the result follows using Lemma 5.4.9. □

Theorem 5.4.11 *Let $\Lambda = u_1^-$. Assume there exists a p-group G, such that*

$$\Lambda \simeq KG,$$

then $\mathrm{char}K = p < g$, *where g is the Coxeter number.*

Proof: We identify Λ with KG (to simplify notation), then J is identified with ω. Let $\tilde{\beta}$ be the maximal root, then $X_{-\tilde{\beta},1} \in J^{g-1} \setminus J^g$ (see (5.33)). Moreover, by (5.31) we have

$$X_{-\tilde{\beta},1} = \sum_{|\mathcal{C}_i|>1} c_i[\mathcal{C}_i], \tag{5.40}$$

where $[\mathcal{C}_i]$ is the class sum of the conjugacy class $\mathcal{C}_i$. Hence there exists some class of size greater than 1 such that its class sum belongs to $J^{g-1} \setminus J^g$. To prove the theorem, we show that the hypothesis $g \leq p$ implies that $[\mathcal{C}_i] \in J^g$ for all conjugacy classes with $|\mathcal{C}_i| > 1$. Let $[\mathcal{C}]$ be a class of size greater than 1, and let $\tilde{\mathcal{C}}$ be as in (5.36). It suffices to show that $[\tilde{\mathcal{C}}] \in J^g$. We found in (5.39) that

$$[\tilde{\mathcal{C}}] = x\sum_{k=0}^{p-1}(X_1+1)^k(X_2+1)^{\binom{k}{2}}\cdots(X_r+1)^{\binom{k}{r}}, \tag{5.41}$$

and since x is a unit, which does not change the power in the radical series, we must show that

$$\sum_{k=0}^{p-1}(X_1+1)^k(X_2+1)^{\binom{k}{2}}\cdots(X_r+1)^{\binom{k}{r}} \in J^g. \tag{5.42}$$

We can expand this expression, and examine whether the sum in each degree lies in J^g.

We know that $w_1 \in G_2$, and Jenning's theory implies that $X_1 \in J^2$. Similarly, $w_i \in G_{i+1}$ implies $X_i \in J^{i+1}$. This means that $X_{g-1} \in J^g$. Furthermore, $X_i^a X_j^b \in J^{a(i+1)+b(j+1)}$.

For degree zero we have $\sum_{k=0}^{p-1} 1 = p \equiv 0 \pmod p$. In case of degree one we look at each X_i for $1 \leq i \leq g-2$, and we get $\sum_{k=0}^{p-1}\binom{k}{i}$. Using Lemma 5.4.7 this is $\binom{p}{i+1}$, which is zero (mod p) because $i+1 < g \leq p$ (Lemma 1.2.3). For degree two we need to check the coefficient of X_iX_j, when $(i+1)+(j+1) = i+j+2 < g$, (else in J^g). Let $i \neq j$, then the coefficient is

$$\sum_{k=0}^{p-1}\binom{k}{i}\binom{k}{j}. \tag{5.43}$$

According to Lemma 5.4.9 this is

$$\begin{aligned}
&\sum_{k=0}^{p-1}\sum_{l=0}^{i}(-1)^{i-l}\binom{i}{i-l}\binom{j+l}{l}\binom{k+l}{j+l}\\
&=\sum_{l=0}^{i}(-1)^{i-l}\binom{i}{i-l}\binom{j+l}{l}\sum_{k=0}^{p-1}\binom{k+l}{j+l}\\
&=\sum_{l=0}^{i}(-1)^{i-l}\binom{i}{i-l}\binom{j+l}{l}\binom{p+l}{j+l+1}, \text{ by Lemma 5.4.8.}
\end{aligned}$$

We have j a positive integer, and $i+j+1 < p$, therefore by Lemma 1.2.3 $\binom{p+l}{j+l+1}$ is zero (mod p) for all $0 \leq l \leq i$. For $i = j$ the coefficient is

$$\sum_{k=0}^{p-1}\binom{\binom{k}{i}}{2}.$$

By Lemma 5.4.9

$$
\begin{aligned}
\binom{\binom{k}{i}}{2} &= 1/2\binom{k}{i}(\binom{k}{i}-1) \\
&= 1/2\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{i-j}\binom{i+j}{j}\binom{k+j}{i+j} - 1/2\binom{k}{i}.
\end{aligned}
$$

Summing up over the k's, and using Corollary 5.4.8 we obtain

$$
1/2\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{i-j}\binom{i+j}{j}\binom{p+j}{i+j+1} - 1/2\binom{p}{i+1},
$$

which is zero (mod p), since $i+j+1<p$.

This argument can be extended to degree $b>1$, where we only need to look at the coefficient of $X_{i_1}^{a_1}X_{i_2}^{a_2}\cdots X_{i_s}^{a_s}$, where $\sum_{l=1}^{s} a_l = b$ and $\sum_{l=1}^{s} a_l(i_l+1) < g \leq p$ (else the element is in J^g). The coefficient is of the form

$$
\binom{\binom{k}{i_1}}{a_1}\binom{\binom{k}{i_2}}{a_2}\cdots\binom{\binom{k}{i_s}}{a_s}. \tag{5.44}
$$

This we can think of as

$$
\binom{\binom{k}{i_1}}{a_1}\cdots\left(\binom{k}{i_{s-1}}(\binom{k}{i_{s-1}}-1)\cdots(\binom{k}{i_{s-1}}-a_{s-1}+1)\right)/a_{s-1}!\binom{\binom{k}{i_s}}{a_s}. \tag{5.45}
$$

Now use Lemma 5.4.10 on $\binom{\binom{k}{i_s}}{a_s}$, and Lemma 5.4.9 several times with the $\binom{k}{i_{s-1}}$ expressions. Continue with $s-2$ etc., and it follows that (5.44) can be written as finite sums of binomial coefficients of the form $\binom{k+c}{i_s+c}$, where we have $i_s+c<p$, since $\sum_{l=1}^{s} a_l(i_l+1)<p$. Summing over the k's, we obtain zero (mod p) with Corollary 5.4.8. □

Remark 5.4.12 From the degree one analysis it follows that $p<g$ is the best bound we can get using this method.

In the special case char$K=2$ and $\mathcal{G}=sl_3$, we find

Proposition 5.4.13 *Assume that* $\mathrm{char}K = p = 2$. *Then we have an isomorphism*

$$u_1^-(sl_3) \simeq KD,$$

where D is the dihedral group of order 8,

$$D = \langle \sigma, \tau : \sigma^2 = 1 = \tau^2, (\sigma\tau)^2 = (\tau\sigma)^2 \rangle$$

Proof: According to Example 5.3.2 we need to prove

$$KD \simeq K\langle a, b\rangle / (a^2, b^2, (ab)^2 - (ba)^2).$$

Let $a = 1 + \sigma, b = 1 + \tau$ and the result follows from straightforward calculations. □

Turning to a general hyperalgebra we actually have not been able to establish whether such groups exist or not. Calculations become rather complicated already for sl_4.

Let us assume that $p = 2$, then we deduce from Example 5.3.2 (2) that

$$\begin{aligned} u_2^-(sl_3) \simeq K\langle a, b, c, d\rangle / \quad & (a^2, b^2, c^2, d^2, (ba - ab)^2, (dc - cd)^2, \\ & ac - ca, bd - db, ad - da - bab, bc - cb - aba). \end{aligned}$$

The subalgebra generated by a and b, call it $\hat{u}$, corresponds to the subalgebra $u_1^-(sl_3)$, which, according to Proposition 5.4.13, is isomorphic to KD, where D is the dihedral group of order 8. If we equip the associative algebra $u_2^-(sl_3)$ with the usual Lie algebra structure, then $\hat{u}$ is a Lie ideal.

Assume that a p-group G with a subgroup H exists such that $u_2^-(sl_3) \simeq KG$, and the subalgebra $u_1^-(sl_3)$ of $u_2^-(sl_3)$ is isomorphic to KH. The above observation about $u_1^-(sl_3)$ being a Lie ideal implies that for all $h \in H$ we have $gh = hg$ for elements g lying in G but not in H. Hence H is normal in G. Calculations with arbitrary choices for a, b, c and d expressed in the KG basis show that it is impossible to find a group, for which all the relations are fulfilled at the same time. This leads to:

Observation 5.4.14 Assume $p = 2$, then no p-group G with a subgroup H exists such that $u_2^-(sl_3) \simeq KG$, and the subalgebra $u_1^-(sl_3)$ of $u_2^-(sl_3)$ is isomorphic to KH.

5.5 A restricted enveloping algebra, $U^{[p]}(\mathrm{Lie}(G))$

We start with a finite abelian p-group G, and we find that $U^{[p]}(\mathrm{Lie}(G))$, the restricted enveloping algebra for $\mathrm{Lie}(G)$, is the group algebra KG, where K is an algebraically closed field of characteristic p. Recall the results about G in section 5.4 above.

We define the Lie algebra associated to G by

$$\mathrm{Lie}(G) = \oplus_{i=1}^{N} G_i/G_{i+1},$$

where the Lie bracket is the linear extension of

$$[gG_{r+1}, hG_{s+1}] = ghg^{-1}h^{-1}G_{r+s+1},$$

for $g \in G_r$ and $h \in G_s$. It is a p-Lie algebra with p map

$$x^{[p]} = g^p G_{pr+1} \in G_{pr}/G_{pr+1} \quad \text{for } x = gG_{r+1} \in G_r/G_{r+1},$$

(see [Huppert] Chapter VIII, 9). We recall that the restricted enveloping algebra $U^{[p]}$ is obtained from the usual enveloping algebra by factoring out the ideal generated by the elements $x^{[p]} - x^p$ for x in the Lie algebra.

Example 5.5.1 Look at the cyclic group of order 4, and let the characteristic of the field be 2.

$$G = \langle x \mid x^4 = 1 \rangle.$$

We get

$$\omega = \mathrm{span}_K\{x-1, x^2-1, x^3-1\} = \mathrm{span}_K\{X, X^2, X^3\},$$

where X=x-1. Furthermore,

$$\omega^2 = \mathrm{span}_K\{X^2, X^3\}, \quad \omega^3 = \mathrm{span}_K\{X^3\} \quad \text{and } \omega^4 = 0.$$

Hence

$$G_1 = G, \quad G_2 = \langle 1, x^2 \rangle \quad \text{and } G_3 = 1,$$

and

$$\mathrm{Lie}(G) = G_1/G_2 \oplus G_2/G_3,$$

where G_1/G_2 is generated by $a = xG_2$, and G_2/G_3 is generated by $b = x^2G_3$. The p-power map looks like $a^{[2]} = x^2G_3 = b$ and $b^{[2]} = 0$. And we have $[a, b] = 0$, since G is abelian. From this it follows that the restricted enveloping algebra is

$$U^{[2]}(\mathrm{Lie}(G)) = K\langle A, B \mid A^2 = B, B^2 = 0\rangle = K\langle A \mid A^4 = 0\rangle.$$

Hence for G cyclic of order 4

$$KG \simeq U^{[2]}(\mathrm{Lie}(G)).$$

Generally we obtain

Proposition 5.5.2 *Let G be a cyclic group of order p^n, and K a field of characteristic p. Then*

$$KG \simeq U^{[p]}(\mathrm{Lie}(G)).$$

Proof: Let $G = \langle x \mid x^{p^n} = 1\rangle$ be a cyclic group of order p^n, then we have a chain of subgroups

$$1 = H_n < H_{n-1} < \cdots < H_2 < H_1 < H_0 = G,$$

where $H_i = \langle x^{p^i} \rangle$. Recall the notation introduced in section 5.4.4, then

$$\omega = \mathrm{span}_K\{x - 1, x^2 - 1, \cdots, x^{p^n - 1} - 1\} = \mathrm{span}_K\{X, X^2, \cdots, X^{p^n - 1}\},$$

where X=x-1. Furthermore,

$$\omega^2 = \text{span}_K\{X^2, X^3, \cdots, X^{p^n-1}\}, \quad \cdots \quad , \omega^{p^n-1} = \text{span}_K\{X^{p^n-1}\} \quad \text{and } \omega^{p^n} = 0.$$

Since the characteristic of the field is p, we obtain $X^p = (x-1)^p = x^p - 1$, and therefore $x^p \in \omega^r$ for $1 \leq r \leq p$. Moreover, we observe $x \notin \omega^r$ for $2 \leq r \leq p$, and we conclude that

$$G_1 = G$$

and

$$G_2 = G_3 = \cdots = G_p = \langle 1, x^p \rangle = H_1.$$

With similar arguments we get

$$G_{p+1} = G_{p+2} = \cdots = G_{p^2} = \langle 1, x^{p^2} \rangle = H_2,$$

$$\vdots$$

$$G_{p^{n-1}+1} = G_{p^{n-1}+2} = \cdots = G_{p^n} = \langle 1 \rangle = H_n.$$

Hence

$$\text{Lie}(G) = G_1/G_p \oplus G_p/G_{p^2} \oplus \cdots \oplus G_{p^{n-1}}/G_{p^n},$$

where $G_{p^i}/G_{p^{i+1}}$ is generated by $a_i = x^{p^i}G_{p^{i+1}}$ for $0 \leq i \leq n-1$, and the p power map sends a_i to a_{i+1}. The restricted enveloping algebra is

$$U^{[p]}(\text{Lie}(G)) = K\langle A_i \mid A_i^p = A_{i+1} \rangle = K\langle A_1 \mid A_1^{p^n} = 0 \rangle. \ \square$$

Lemma 5.5.3 *Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two Lie algebras over K with enveloping algebras U_i for $i = 1, 2$. Let $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ with enveloping algebra U. Then*

$$U \simeq U_1 \otimes_K U_2,$$

Similarly, suppose we have two p-Lie algebras, then the restricted enveloping algebra of $\mathcal{G}$ is

$$U^{[p]}(\mathcal{G}) \simeq U^{[p]}(\mathcal{G}_1) \otimes_K U^{[p]}(\mathcal{G}_2).$$

Proof: For the first statement see [Bourbaki] 2.2. Suppose $\mathcal{G}_1$ and $\mathcal{G}_2$ are p-Lie algebras, then one can show that the following is a p-map

$$\begin{aligned} [p] : \mathcal{G} &\rightarrow \mathcal{G} \\ (x_1, x_2)^{[p]} &\rightarrow (x_1^{[p]}, x_2^{[p]}). \end{aligned}$$

Let I_i be the ideal of U_i such that $U_i^{[p]} = U_i/I_i$ for $i = 1, 2$, then the ideal I of U such that $U^{[p]} = U/I$ is identified

$$I = I_1 \otimes 1 + 1 \otimes I_2. \ \square$$

Theorem 5.5.4 *Let G be a finite abelian p-group. Then*

$$KG \simeq U^{[p]}(\mathrm{Lie}(G)).$$

Proof: Any finite abelian p-group is a direct product of cyclic p-groups, and the result follows from Lemmas 5.4.4 and 5.5.3 and Proposition 5.5.2. $\square$

Before looking at an example, an induction on k gives us

Lemma 5.5.5 *Let*

$$g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

then

$$g^k = \begin{pmatrix} 1 & ka & kb + \binom{k}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}.$$

In particular, if $p > 2$ then $g^p = 1$ for all $g \in G$, where

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in \mathbf{F}_p \right\}. \tag{5.46}$$

Example 5.5.6 Let G be the above group (5.46) of order p^3. To calculate Lie(G), we need G_r. Assume $p > 2$, then Lemma 5.5.5 implies that $\gamma_i(G)^{p^j} = 1$ for all $j \geq 1$, and therefore (5.34) simplifies to

$$\kappa_r(G) = \prod_{i \geq r} \gamma_i(G) = \gamma_r.$$

For our G we get

$$\gamma_1(G) = G, \quad \gamma_2(G) = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad \gamma_3 = 1.$$

Therefore

$$\{1\} = G_3 < G_2 = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} < G_1 = G,$$

where G/G_2 has order p^2, and $G_2/G_3 = G_2$ has order p. Fix a basis of G/G_2, e.g. $X_i = x_i G_2$, where

$$x_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } x_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$[X_1, X_2] = [x_1 G_2, x_2 G_2] = x_1 x_2 x_1^{-1} x_2^{-1} G_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} G_3,$$

which is central. Hence Lie(G) is the 3-dimensional Lie algebra over $\mathbf{F}_p$ with basis X_1, X_2 and $[X_1, X_2]$, where $[X_1, X_2]$ is central. According to Lemma 5.5.5 the p-map is trivial. We obtain

$$U^{[p]}(\text{Lie}(G)) \simeq u_1^-(sl_3) \text{ for } p > 2. \tag{5.47}$$

Corollary 5.5.7 *Let the group be*

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in \mathbf{F}_p \right\},$$

and assume the characteristic of the field to be $p > 2$, then the group algebra KG is not isomorphic to $gr(KG)$, where $gr(KG)$ is the graded algebra with respect to powers of the augmentation ideal, ω.

Proof: By [Quillen] we have $\mathrm{gr}(KG) \simeq U^{[p]}(\mathrm{Lie}(G))$. The right hand side is isomorphic to $u_1^-(sl_3)$ according to (5.47). From Theorem 5.4.11 we know that this is not isomorphic to a group algebra, when $p > 2$. Therefore $\mathrm{gr}(KG)$ is not isomorphic to any group algebra, and in particular not isomorphic to KG. $\square$

Appendix A

Reduce program

This appendix contains a Reduce program. The program is described in Chapter 3, where it is used to calculate some examples.

This procedure calculates $n!$ for n a positive integer.

```
procedure fac n5;
if (not(fixp(n5)) or n5<0) then rederr "FAC called with invalid argument"
else
if n5>1 then n5*fac(n5-1)
else 1;
```

This procedure calculates the binomial coefficient for n an integer, m a positive integer.

```
procedure bin(n4,m4);
if (not(fixp(n4)) or not(fixp(m4)) or m4<0) then
      rederr "BIN called with invalid argument"
else
(for i1:=(n4-m4+1):n4 product i1)/fac(m4);
```

This procedure finds the smallest i, such that n lies between p^i and p^{i+1}.

```
procedure findb(n3,p);
if  (not(fixp(n3)) or not(fixp(p)) or n3<0) then
                    rederr "FINDB called with invalid argument"
```

```
else
     <<i1:=0;
      while p**i1 <= n3 do i1:=i1+1;
      i1-1>>;
```

This procedure calculates the matrix with the f and g equations.

```
procedure matree(r,s,p,n,m);
begin;
b:=findb(n,p);
c:=findb(m,p);
d:=m-n;
e1:=findb(d,p);
f:=(b+1)*(n+1) - (p**(b+1)-1)/(p-1);
rows:= f
      +(c+1)*(n+1)  + (c-e1)*d
      -( p**(c+1)-p**(e1+1))/(p-1);
columns:=n+1;
matrix a(rows,columns);

for k:=0:b do
<< firstco:=k*(n+1) - (p**k-1)/(p-1);
   for i1:=1:(n+1-p**k) do
<<      firstco:=firstco+1;
        a(firstco,i1):=bin(r+d+p**k+1-i1,p**k);
        for j:=1:(i1-1) do
           a(firstco,j):=0;
        for j:=i1+1:(i1+p**k) do
           (if a(firstco,j-1)=0 then
            a(firstco,j):=
           (-1)**(j-i1)*bin(r+d+p**k+1-j,p**k-(j-i1))*bin(m+1-i1,j-i1)
           else
            a(firstco,j):=
           (-1)*a(i1+k*(n+1)-(p**k-1)/(p-1),j-1)*
                  (p**k-(j-i1)+1)/(r+d+p**k+2-j)*(m+2-j)/(j-i1));
        for j:=(i1+p**k+1):n+1 do
           a(firstco,j):=0;
>>;
>>;

for k:=0:c do
<< firstcor:=f+k*(n+1)+
      (if d<p**(k-1) then (k-1-e1)*d - (p**k-p**(e1+1))/(p-1) else 0);
```

```
   for i1:=1:(n+1-(if d<p**k then (p**k-d) else 0)) do
<<    bound:=min(i1+p**k,n+1);
      firstcor:=firstcor+1;
      a(firstcor,i1):=bin(s-m+i1+p**k-1,p**k);
      for j:=1:(i1-1) do
           a(firstcor,j):=0;
        for j:=i1+1:bound do
            (if a(firstcor,j-1)=0 then
           a(firstcor,j):=bin(s-m+i1+p**k-1,p**k-(j-i1))*bin(n+1-i1,j-i1)
           else
           a(firstcor,j):=a(firstcor,j-1)
                          *(p**k-(j-i1)+1)/(s-m+j-1)*(n+2-j)/(j-i1));
        for j:=(bound+1):n+1 do
           a(firstcor,j):=0;
>>;
>>;
return a;
end;
```

This procedure finds the value of t modulo p

```
procedure prest(tt,p);
(tt-remainder(tt,p))/p;
```

This procedure checks through all (n,m) values, where $n \equiv m \equiv r+s+2 \pmod{p}$ and $n \leq m$. It returns the (n,m) for which $\mu = (r,s) - n\alpha - m\beta$ is a primitive weight.

```
procedure pweight(r9,s9,p);
begin;
setmod p;
tt:=r9+s9+2;
z9:={};
for i1:=0:prest(tt,p) do
   for j:=i1:min(i1+prest(s9,p),prest(tt,p)) do
<<
        n9:=remainder(tt,p)+p*i1;
        m9:=remainder(tt,p)+p*j;
        if m9 neq 0 then
            << a9:=matree(r9,s9,p,n9,m9);
            on modular;
```

```
            b9:=nullspace(a9);
            if b9 neq {} then test:=t else test:=nil;
            off modular;
            if test then
            <<  write "(",n9,",",m9,",",tp(first(b9)),")";
                if rest(b9) neq {} then write "bigger nullspace";
              z9:=append(z9,{{n9,m9}});
            >>;
            >>;
>>;
return(z9);
end;
```

This procedure does the same as pweight, but does not check $n = m$ again.

```
procedure pweightspecial(r10,s10,p);
begin;
setmod p;
tt:=r10+s10+2;
z10:={};
for i1:=0:prest(tt,p) do
   for j:=i1:min(i1+prest(s10,p),prest(tt,p)) do
<<
        n10:=remainder(tt,p)+p*i1;
        m10:=remainder(tt,p)+p*j;
        if m10 neq 0 then
          << if n10  neq m10 then
            << a10:=matree(r10,s10,p,n10,m10);
            on modular;
            b10:=nullspace(a10);
            if b10 neq {} then test:=t else test:=nil;
            off modular;
            if test then
            << if rest(b10) neq {} then write "bigger nullspace";
              z10:=append(z10,{{n10,m10}});
            >>;
            >>;
           >>;
>>;
return(z10);
end;
```

This procedure checks all $n \equiv m \equiv r + s + 2 \pmod p$ for $Z(r, s)$. It returns the values of (n, m) for which we have that $\mu = (r, s) - n\alpha - m\beta$ is a primitive weight.

```
procedure pw(rh,sh,p);
begin;
 ah:=pweight(rh,sh,p);
 bh:=pweightspecial(sh,rh,p);
 lengthbh:=length(bh);
 for j:=1:lengthbh do
  << ah:=append(ah,{{second(first(bh)),first(first(bh))}});
     bh:=rest(bh)>>;
 return(ah);
end;
```

Now follows the other half of the program, where we calculate for what values of (n, m) we have first or second generation primitive weights. And we find the third generation primitive weights found in the Proposition in Chapter 3.

This procedure gives the p-adic expansion of r with respect to p.

```
procedure padic(r8,p);
begin;
          a8:={};
          while r8 neq 0 do
          << rem:=remainder(r8,p);
             a8:=append(a8,{rem});
             r8:=(r8-rem)/p
          >>;
return a8;
end;
```

This procedure finds first generation primitive weights.

```
procedure priw(r7,p);
begin;
expand:=padic(r7,p);
```

```
a7:={};
n7:=1;
l7:=length expand;
expand:=append(expand,{0});
if first(expand)=0 then a7:=append(a7,{1});
for j:=1:l7 do
<<   n7:=n7+first(expand)*p**(j-1);
     if
     (remainder(n7,p**(j)) neq 0 or second(expand)=0) and
     first(expand) neq 0 then
         a7:=append(a7,{n7});
     expand:=rest(expand);
>>;
return a7;
end;
```

This procedure finds all second generation primitive weights of kind either $X_{\beta,m}X_{\alpha,n}$ or $X_{\alpha,n}X_{\beta,m}$. To find the latter call the procedure with (s,r) instead of (r,s) and the result is (m,n) values.

```
procedure priw2(r6,s6,p);
begin;
h6:=priw(r6,p);
z6:={};
lengthh6:=length(h6);
for j:=1:lengthh6 do
<<
 b6:=first h6;
 c6:=priw(b6+s6,p);
 lengthc6:=length(c6);
 for i1:=1:lengthc6 do <<z6:=append(z6,{{b6,first c6}});c6:=rest c6;>>;
 h6:=rest(h6);
>>;
return z6;
end;
```

This procedure finds the third generation primitive weight vectors found in Chapter 3. That is to say either of kind $X_{\alpha,v_2}X_{\beta,m}X_{\alpha,v_1}$ or $X_{\beta,t_2}X_{\alpha,n}X_{\beta,t_1}$, where $t_1+t_2=m$ and $v_1+v_2=n$.

```
procedure priw3(r3,s3,p);
begin;
setmod p;
h3:=priw2(r3,s3,p);
z3:={};
length3:=length(h3);
for j3:=1:length3 do
<<
      b3:=first(first(h3));
      c3:=second(first(h3));
      w:=r3-2*b3+c3;
      if w > 0 then
      << d3:=priw(w,p);
         lengthd3:=length(d3);
         for i1:=1:lengthd3 do
         <<j:=0;
         while j<=min(first(d3),c3) do
              << help3:=bin(b3+first(d3)-j,b3);
                 on modular;
                 if help3=0
                 then <<off modular; j:=j+1>>
                 else <<off modular; j:=(min(first(d3),c3)+1);
                      z3:=append(z3,{append(first(h3),{first(d3)})})>>;
                 >>;
         d3:=rest(d3);>>;
      >>;
         h3:=rest(h3);
>>;
return(z3);
end;
```

This procedure comes back with a list of all the (n, m) values for which we have a third generation primitive weight vector, using the methods in Chapter 3. Some (n, m) pairs might appear twice.

```
procedure primweight(r,s,p);
begin;
s1:=priw3(r,s,p);
nm:={};
lengths1:=length(s1);
for j:=1:lengths1 do
<<    b1:=first(first(s1));
```

```
      c1:=second(first(s1));
      d1:=third(first(s1));
      nm:=append(nm,{append({b1+d1},{c1})});
      s1:=rest(s1);
>>;
s11:=priw3(s,r,p);
lengths11:=length(s11);
for j:=1:lengths11 do
<<    b11:=first(first(s11));
      c11:=second(first(s11));
      d11:=third(first(s11));
      nm:=append(nm,{append({c11},{b11+d11})});
      s11:=rest(s11);
>>;
return(nm);

end;
```

References

[Andersen]: H. Haahr-Andersen: The strong linkage principle, *J. reine angew. Math.* **315**, 53-59, (1980)

[Bourbaki]: *Éléments de mathématique, Groupes et Algèbres de Lie, Chapitre 1, Algèbres de Lie*, Paris: Hermann, 1960.

[Carter]: R.W. Carter: *Simple Groups of Lie type*, London-New York: Wiley and Sons, 1972.

[Donkin]: S. Donkin: The blocks of a semisimple algebraic group. *J. Alg.* **67**, 36-53, (1980).

[Donkin 2]: S. Donkin: *Representations of the hyperalgebra of a semisimple group.* in preparation.

[Haboush]: W. Haboush: Central Differential operators on split semisimple groups over fields of positive characteristic. In *Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin*, ed. M.P. Malliavin, Paris, Proceedings publ. as Lecture notes in Mathematics, **795**, Berlin-Heidelberg-New York: Springer-Verlag, 1979.

[Hump]: J.E. Humphreys: *Introduction to Lie algebras and Representation Theory*, Graduate Texts in Mathematics 9, Berlin-Heidelberg-New York: Springer-Verlag, 1972.

[Hump 2]: J.E. Humphreys: On the hyperalgebra of a semisimple algebraic group. In *Contributions to Algebra: A collection of papers dedicated to Ellis Kolchin*, New York-San Francisco-London: Academic Press, 1977.

[Huppert]: B. Huppert, N. Blackburn: *Finite Groups II*, Grundlehren der mathematischen Wissenschaften 242, Berlin-Heidelberg-New York: Springer-Verlag, 1982.

[Irving]: R.S. Irving: The socle filtration of a Verma module. *Ann. Sci. de l' Éc. Norm. Sup.* 4^e *série*, **21**, p.47-65, 1988.

[Jantzen]: J.C. Jantzen: *Representations of Algebraic Groups*, Academic Press, INC, 1987.

[Jantzen 2]: J.C. Jantzen: *Moduln mit einem höchsten Gewicht*, Lecture Notes in Mathematics, **750**, Berlin-Heidelberg-New York: Springer-Verlag, 1980.

[Jantzen 3]: J.C. Jantzen: Darstellungen halbeinfacher Gruppen und ihrer Frobenius-Kerne, *J. reine angew. Math.*, **317**, 157-199, 1980.

[Jantzen 4]: J.C. Jantzen: Darstellungen halbeinfacher algebraischer Gruppen und zugeordnete kontravariante Formen, *Bonner math. Sch.*, **67**, 1973.

[Kac]: V.G. Kac: *Infinite dimensional Lie Algebras*, Cambridge-New York-Sydney: Cambridge University Press, 1985.

[Kostant]: B. Kostant: Groups over **Z**, pp. 90-98 in: A. Borel, G.D. Mostow (eds.) *Algebraic Groups and Their Discontinuous Subgroups*, (Proc. Symp. Pure Math. **8**), Providence, R.I.: Amer. Math. Soc. 1966.

[Külshammer]: B. Külshammer: Group-theoretical descriptions of ring-theoretical invariants of group algebras, Progress in Mathematics, **95**, Basel: Birkhäuser Verlag, 1991.

[Mowbray 1]: M. Mowbray: The submodule Structure of Characteristic p Verma modules for groups of type A_1, *Comm. in Alg.* **17(6)**, 1407-1423 (1989).

[Mowbray 2]: M. Mowbray: On Verma modules in characteristic p. Thesis, Queen Mary and Westfield College, London, 1988.

[Passman]: D.S. Passman: *The algebraic structure of group rings*, New York-London-Sydney-Toronto: John Wiley and Sons, Inc., 1977.

[Quillen]: D.G. Quillen: On the Associated Graded Ring of a Group Ring, *Journal of Algebra*, **10**, 411-418 (1967).

[Samelson]: H. Samelson: *Notes on Lie Algebras*, Van Nostrand Reinhold Mathematical Studies No. 23, New York: Van Nostrand Reinhold, 1969.

[Steinberg]: R. Steinberg: *Lectures on Chevalley Groups*, New Haven, Conn.: Yale University Press, 1968.

[Steinberg 2]: R. Steinberg: Representations of algebraic groups, *Nagoya Math. J.*, **22**, 33-56 (1963).

[Strade]: H. Strade, F. Farnsteiner: *Modular Lie Algebras and their Representations*, New York, Basel: Marcel Dekker, Inc., 1988.