PACIFIC JOURNAL OF MATHEMATICS
Vol. 179, No. 1, 1997

SHAPOVALOV DETERMINANT FOR RESTRICTED AND QUANTIZED RESTRICTED ENVELOPING ALGEBRAS

Shrawan Kumar and Gail Letzter

As is well known, the Shapovalov bilinear form and its determinant is an important tool in the representation theory of semisimple Lie algebras over char. 0. To our knowledge, the corresponding study of the Shapovalov bilinear form and its determinant is not available in the literature in char. p or the quantum case at roots of unity. The aim of this paper is to fully determine the Shapovalov determinant for both, the restricted enveloping algebra and its quantum analog.

More precisely, let $\mathfrak{g}$ be a semisimple Lie algebra. Fix a prime $p \neq 2$ which also satisfies $p \neq 3$ whenever $\mathfrak{g}$ contains a component of type G_2. This will be our tacit assumption on p through the paper. Let ξ be a primitive p^{th} root of unity. This paper is concerned with two algebras: a certain analog $\mathfrak{u}_p$ of the restricted enveloping algebra (cf. Definition 3.1) and its quantized version $\mathfrak{u}_\xi$ which is an algebra over the cyclotomic field $\mathbb{Q}_\xi$ (cf. Definition 3.3). The main results of this paper are complete descriptions of the Shapovalov determinant for both the algebras $\mathfrak{u}_p$ and $\mathfrak{u}_\xi$ (cf. Theorems 3.2 and 3.4).

1. Introduction.

There has been tremendous interest in the representation theory of the algebra $\mathfrak{u}_p$, because of its connection with the representation theory of the associated algebraic group over char. p (via some proven conjectures of Verma and the Steinberg Tensor Product Theorem). The quantized algebra $\mathfrak{u}_\xi$ seems even richer. On the one hand (as conjectured by Lusztig, and proved for large primes by Andersen-Jantzen-Soergel [**AJS**]) its irreducible modules have the same character as that of $\mathfrak{u}_p$ and on the other hand (as shown by Kazhdan-Lusztig) its representation theory parallels that of the representation theory of the associated affine Kac-Moody Lie algebra at a certain negative level. In the sequel, we shall refer to the case of $\mathfrak{u}_p$ (resp. $\mathfrak{u}_\xi$) as the modular (resp. the quantum) case.

Our arguments in the modular case draw and expand upon Shapovalov's original paper [**S**]. For any positive root γ and positive integer m, he constructed a certain element $\Theta_{\gamma,m} \in U(\mathfrak{g})$ of weight $-m\gamma$, which when applied to a highest weight vector of a particular Verma module for $U(\mathfrak{g})$ provides another highest weight vector. In our paper, we make a careful choice of the elements $\Theta_{\gamma,m}$ with certain 'integrality' properties which enables us to take their reduction mod p. The whole of our Section 5 is devoted to constructing these elements and proving certain properties satisfied by them crucial for decomposing the Shapovalov determinant (cf. Propositions 5.2 and 5.6). But the Lie algebra of type G_2 poses additional problems for the root $\gamma = 2\alpha_1 + \alpha_2$, which is handled separately in Section 6. Mimicking the arguments in [**S**], we calculate the highest degree term of the Shapovalov determinant for the algebra $\mathfrak{u}_p$ (cf. Lemma 8.1). Now the explicit nature of the highest degree term shows that the factors of the Shapovalov determinant in the modular case obtained from the existence of the elements $\Theta_{\gamma,m}$ exhaust all the factors of the determinant, thereby completing the proof of Theorem (3.2).

The quantum arguments are quite similar; the only added difficulty lies in choosing various correct powers of q. We construct the q-version $\Theta^q_{\gamma,m}$ of the elements $\Theta_{\gamma,m}$ in Section 7. Its required properties are contained in Proposition (7.1). The proof of this proposition makes repeated use of certain commutation relations, which we collect in Section 4. The quantum case, however, uses two types of specialization: One from the generic q to the root of unity ξ, and the other from ξ to char. p (cf. Definition 9.2). To make this possible, we must work over a larger ring $\mathcal{B} \supset \mathbb{Z}[q, q^{-1}]$ (cf. §2). In particular, we define a certain $\mathcal{B}$-form $\mathfrak{U}_{\mathcal{B}}$ of the quantized enveloping algebra $U_q(\mathfrak{g})$ and prove various freeness properties (cf. Proposition 4.4), which allow us to specialize both ways. Proofs of both the Theorems (3.2) and (3.4) are completed in §9.

We present some applications of our Shapovalov determinant formulae: As an immediate consequence of our Theorems (3.2) and (3.4), we deduce the irreducibility of the Steinberg module for $\mathfrak{u}_p$ (as well as $\mathfrak{u}_\xi$) (cf. Corollary 3.5). This result is well known (and proved by other methods). The second, given in Section 10, is a new proof of the character-sum formula (cf. Theorem 10.1) for the Jantzen filtration for the algebras $\mathfrak{u}_p$ and $\mathfrak{u}_\xi$, obtained by Andersen-Jantzen-Soergel [**AJS**] by different methods. Finally, as in [**AJS**, §6], the Strong Linkage Principle for the algebra $\mathfrak{u}_p$ with p at least the Coxeter number h of $\mathfrak{g}$ and for $\mathfrak{u}_\xi$ with arbitrary p (cf. Theorem 10.3) follows easily from Theorem (10.1). It may be recalled that the Strong Linkage Principle in the modular case was proved for arbitrary p in general by Andersen [**A**] and in the quantum case by Andersen-Polo-Wen [**APW**].

Acknowledgement. We thank J.E. Humphreys for some comments on this work.

2. Preliminaries and Notation.

Let $\mathfrak{g}$ be the complex semisimple Lie algebra of rank n associated to a Cartan matrix $A = (a_{ij})_{1\leq i,j\leq n}$. Fix a triangular decomposition

$$\mathfrak{g} = \mathfrak{n}^- \oplus \mathfrak{h} \oplus \mathfrak{n}^+. \tag{1}$$

Let Δ^+ denote the set of positive roots of $\mathfrak{g}$ (i.e., the set of roots of $\mathfrak{n}^+$), $\{\alpha_1, \ldots, \alpha_n\}$ the set of simple (positive) roots, and $\{f_\beta, e_\beta, H_i; \beta \in \Delta^+, 1 \leq i \leq n\}$ a Chevalley basis for $\mathfrak{g}$. Here, f_β corresponds to the negative root $-\beta$, e_β corresponds to the positive root β, and H_i is the simple coroot corresponding to the root α_i. For the simple root α_i, we also denote e_{α_i} (resp. f_{α_i}) simply by e_i (resp. f_i). Let $r_1, \ldots, r_n$ be the (simple) reflections corresponding to the simple roots $\alpha_1, \ldots, \alpha_n$ respectively. Fix an ordering $\beta_1, \ldots, \beta_N$ of the positive roots and set

$$e^t = e_{\beta_1}^{t_1} \cdots e_{\beta_N}^{t_N} \quad \text{and} \quad f^t = f_{\beta_N}^{t_N} \cdots f_{\beta_1}^{t_1}, \tag{2}$$

for any N-tuple of non-negative integers $t = (t_1, \ldots, t_N)$ (where $N = |\Delta^+|$).

Let $\mathfrak{g}_\mathbb{Z}$ be the Lie subalgebra of $\mathfrak{g}$ generated by $\{f_\beta, e_\beta, H_i; \beta \in \Delta^+, 1 \leq i \leq n\}$ over $\mathbb{Z}$ and set

$$\mathfrak{n}^\pm_\mathbb{Z} = \mathfrak{n}^\pm \cap \mathfrak{g}_\mathbb{Z}, \quad \mathfrak{h}_\mathbb{Z} = \mathfrak{h} \cap \mathfrak{g}_\mathbb{Z}. \tag{3}$$

For any prime p, let $\mathbf{F}_p$ be the prime field (of order p) and set $\mathfrak{g}_p = \mathfrak{g}_\mathbb{Z} \otimes_\mathbb{Z} \mathbf{F}_p$. Note that

$$\mathfrak{g}_p = \mathfrak{n}_p^- \oplus \mathfrak{h}_p \oplus \mathfrak{n}_p^+, \tag{4}$$

where $\mathfrak{n}_p^- = \mathbf{F}_p \otimes_\mathbb{Z} \mathfrak{n}_\mathbb{Z}^-$, etc.

For any Lie algebra $\mathfrak{s}$ over a commutative ring R, we denote its universal enveloping algebra by $U(\mathfrak{s})$.

Now let $U_q(\mathfrak{g})$ denote the *quantized enveloping algebra* associated to $\mathfrak{g}$ (rather to the Cartan matrix A) defined by V.G. Drinfeld and M. Jimbo. Recall that $U_q(\mathfrak{g})$ is defined to be the associative algebra over the function field $\mathbb{Q}(q)$ generated by $\{E_i, F_i, K_i^{\pm 1}\}_{1\leq i\leq n}$ and subject to the relations:

$$K_iK_j = K_jK_i, \quad K_iK_i^{-1} = K_i^{-1}K_i = 1, \qquad \text{for all } i,j \tag{R1}$$

$$K_iE_jK_i^{-1} = q^{d_ia_{ij}}E_j, \quad K_iF_jK_i^{-1} = q^{-d_ia_{ij}}F_j, \qquad \text{for all } i,j \tag{R2}$$

$$E_iF_j - F_jE_i = \delta_{i,j}\frac{K_i - K_i^{-1}}{q^{d_i} - q^{-d_i}}, \qquad \text{for all } i,j, \quad \text{and} \tag{R3}$$

$$\sum_{m=0}^{1-a_{ij}} (-1)^m E_i^{(1-a_{ij}-m)} E_j E_i^{(m)} = 0, \qquad \text{and} \tag{R4}$$

$$\sum_{m=0}^{1-a_{ij}} (-1)^m F_i^{(1-a_{ij}-m)} F_j F_i^{(m)} = 0, \qquad \text{for } \ i \neq j,$$

where $D = \operatorname{diag}(d_1, \dots, d_n)$ is the unique diagonal matrix with positive integral entries so that the matrix DA is symmetric, and the entries of D are the smallest possible. In the above relation (R4), the following standard notation is being used:

$$E_i^{(m)} := \frac{E_i^m}{[m]!_{d_i}}, \quad F_i^{(m)} := \frac{F_i^m}{[m]!_{d_i}}, \tag{5}$$

$$[m]!_{d_i} := [1]_{d_i}[2]_{d_i} \cdots [m]_{d_i} \qquad \text{and} \tag{6}$$

$$[m]_{d_i} := \frac{q^{d_i m} - q^{-d_i m}}{q^{d_i} - q^{-d_i}}. \tag{7}$$

Then $U_q(\mathfrak{g})$, in fact, has a Hopf algebra structure with the comultiplication Δ, counit ϵ, and antipode σ defined as follows:

$$\Delta E_i = E_i \otimes 1 + K_i \otimes E_i,\ \Delta F_i = F_i \otimes K_i^{-1} + 1 \otimes F_i,\ \Delta K_i = K_i \otimes K_i; \tag{8}$$

$$\epsilon K_i = 1, \quad \epsilon E_i = \epsilon F_i = 0; \quad \text{and} \tag{9}$$

$$\sigma E_i = -K_i^{-1} E_i, \quad \sigma F_i = -F_i K_i, \quad \sigma K_i = K_i^{-1}. \tag{10}$$

For any Hopf algebra H, one defines an *adjoint action* by

$$(\text{ad } a)b = \sum_i a_i^1 b \sigma(a_i^2) \quad \text{for } \ a, b \in H, \tag{11}$$

where $\Delta a = \sum_i a_i^1 \otimes a_i^2$. In particular, for $a \in U_q(\mathfrak{g})$, we have

$$\begin{gathered}(\text{ad } F_i)a = F_i a K_i - a F_i K_i, \quad (\text{ad } E_i)a = E_i a - K_i a K_i^{-1} E_i, \\ (\text{ad } K_i)a = K_i a K_i^{-1}.\end{gathered} \tag{12}$$

Lusztig [L1, L2] introduced certain automorphisms T_i of $U_q(\mathfrak{g})$ corresponding to the simple roots α_i. As in [DK, Remark 1.6],

$$\begin{aligned} &T_i E_j = (\text{ad} -E_i^{(-a_{ij})})E_j, \qquad \text{if } \ i \neq j \quad \text{and} \\ &T_i E_i = -F_i K_i. \end{aligned}$$

Any choice of a reduced expression $r_{i_1}\cdots r_{i_N}$ of the longest element w_o of the Weyl group W associated to $\mathfrak{g}$ gives rise to an ordering of the positive roots:

$$\beta_1=\alpha_{i_1},\quad \beta_2=r_{i_1}\alpha_{i_2},\dots,\quad \beta_N=r_{i_1}\cdots r_{i_{N-1}}\alpha_{i_N}, \tag{13}$$

and the "root vectors" ([**L1**, **L2**]) for any $1\le k\le N$:

$$E_{\beta_k}:=T_{i_1}\cdots T_{i_{k-1}}E_{i_k},\quad F_{\beta_k}:=T_{i_1}\cdots T_{i_{k-1}}F_{i_k}. \tag{14}$$

In the sequel we shall use this ordering of positive roots.

For any $t=(t_1,\dots,t_N)\in\mathbb{Z}_+^N$ (where $\mathbb{Z}_+$ denotes the set of non-negative integers), set

$$E^t=E_{\beta_1}^{t_1}\cdots E_{\beta_N}^{t_N}\quad\text{and}\quad F^t=F_{\beta_N}^{t_N}\cdots F_{\beta_1}^{t_1}. \tag{15}$$

Let $a:=\max\{-a_{ij}\}_{i\neq j}$, where a_{ij} are the entries of the Cartan matrix A. Let $\mathcal{B}$ be the subring

$$\mathbb{Z}\left[q,q^{-1},([a]!_{d_1})^{-1},\dots,([a]!_{d_n})^{-1}\right]$$

of $\mathbb{Q}(q)$. Define the $\mathcal{B}$-subalgebra $\mathfrak{U}_{\mathcal{B}}$ of $U_q(\mathfrak{g})$ generated by $\{E_i,F_i,K_i^{\pm1};1\le i\le n\}$. Set

$$\mathfrak{U}_{\mathcal{B}}^o=\mathfrak{U}_{\mathcal{B}}\cap U_q^o,\quad \mathfrak{U}_{\mathcal{B}}^{\pm}=\mathfrak{U}_{\mathcal{B}}\cap U_q^{\pm}, \tag{16}$$

where U_q^o (resp. U_q^+, resp. U_q^-) is the $\mathbb{Q}(q)-$subalgebra of $U_q(\mathfrak{g})$ generated by $\{K_i^{\pm1}\}_{1\le i\le n}$ (resp. $\{E_i;1\le i\le n\}$, resp. $\{F_i;1\le i\le n\}$).

Fix an odd prime p which is further assumed not to be equal to 3 if G_2 is a factor of $\mathfrak{g}$. *This will be our tacit assumption in this paper.* Also fix a primitive p-th root of unity ξ, and let $\mathbb{Q}_\xi$ be the cyclotomic field gotten by attaching ξ to $\mathbb{Q}$. Define the homomorphism $f_\xi:\mathcal{B}\to\mathbb{Q}_\xi$ by $q\mapsto\xi$. It is easy to see, by our restriction on p, that this map is well defined. Set

$$\mathfrak{U}_\xi=\mathbb{Q}_\xi\otimes_{\mathcal{B}}\mathfrak{U}_{\mathcal{B}},\quad \mathfrak{U}_\xi^{\pm}=\mathbb{Q}_\xi\otimes_{\mathcal{B}}\mathfrak{U}_{\mathcal{B}}^{\pm},\quad\text{and}\quad \mathfrak{U}_\xi^o=\mathbb{Q}_\xi\otimes_{\mathcal{B}}\mathfrak{U}_{\mathcal{B}}^o. \tag{17}$$

By Proposition 4.4(b), $\mathfrak{U}_\xi^0$ is the algebra $\mathbb{Q}_\xi[K_1^{\pm},\dots,K_n^{\pm}]$ of Laurent polynomials in the variables $\{K_1,\cdots,K_n\}$.

Let $(,)$ denote the Killing form on $\mathfrak{h}^*$, normalized so that

$$\frac{(\alpha_i,\alpha_i)}{2}=d_i.$$

Set $\check{\beta}=2\beta/(\beta,\beta)$ for $\beta\neq0\in\mathfrak{h}^*$. Let ρ denote the half sum of the positive roots. Then $(\rho,\check{\alpha}_i)=1$ for each $1\le i\le n$. Set $\mathfrak{h}_{\mathbb{Z}}^*=\{\lambda\in\mathfrak{h}^*;(\lambda,\check{\alpha}_i)\in\mathbb{Z}\text{ for all }1\le i\le n\}$. For any $\beta\in\Delta^+$, let $H_\beta\in\mathfrak{h}$ be the coroot defined by

$$\chi(H_\beta)=(\chi,\check{\beta}),\qquad\text{for all }\chi\in\mathfrak{h}^*. \tag{18}$$

3. The Shapovalov determinant – Statement of the main results.

Definition 3.1. The triangular decomposition of $\mathfrak{g}_p$ (cf. (4) of §2) gives rise to the decomposition

$$U(\mathfrak{g}_p) = (\mathfrak{n}_p^- U(\mathfrak{g}_p) + U(\mathfrak{g}_p)\mathfrak{n}_p^+) \oplus U(\mathfrak{h}_p), \tag{1}$$

and hence gives the Harish-Chandra homomorphism (by projecting on the second factor)

$$\mathfrak{H}_p : U(\mathfrak{g}_p) \to U(\mathfrak{h}_p).$$

Let ω be the Chevalley anti-automorphism $\mathfrak{g}_p \to \mathfrak{g}_p$ defined by $\omega(f_i) = e_i, \omega(e_i) = f_i, \omega(H_i) = H_i$, for all $1 \le i \le n$; where (as in §2) e_i (resp. f_i) corresponds to the simple root α_i (resp. the negative root $-\alpha_i$). Now, define the *Shapovalov bilinear form*

$$S_p : U(\mathfrak{n}_p^-) \times U(\mathfrak{n}_p^-) \to U(\mathfrak{h}_p) \quad \text{by}$$

$$S_p(a, b) = \mathfrak{H}_p(\omega(a)b).$$

It is easy to see that e_β^p and f_β^p are central elements in $U(\mathfrak{g}_p)$. Let $\mathfrak{u}_p$ be the quotient algebra $U(\mathfrak{g}_p)/\langle e_\beta^p, f_\beta^p; \beta \in \Delta^+\rangle$, where $\langle\ \rangle$ denotes the ideal generated by the elements inside the parentheses. Similarly, let $\mathfrak{u}_p^+$ (resp. $\mathfrak{u}_p^-$) be the quotient algebra $U(\mathfrak{n}_p^+)/\langle e_\beta^p; \beta \in \Delta^+\rangle$(resp. $U(\mathfrak{n}_p^-)/\langle f_\beta^p; \beta \in \Delta^+\rangle$), and $\mathfrak{b}(\mathfrak{u}_p)$ (resp. $\mathfrak{b}^-(\mathfrak{u}_p)$) be the quotient algebra $U(\mathfrak{b}_p)/\langle e_\beta^p; \beta \in \Delta^+\rangle$ (resp. $U(\mathfrak{b}_p^-)/\langle f_\beta^p; \beta \in \Delta^+\rangle$), where $\mathfrak{b}_p := \mathfrak{h}_p + \mathfrak{n}_p^+$ (resp. $\mathfrak{b}_p^- := \mathfrak{h}_p + \mathfrak{n}_p^-$). Observe that

$$\mathfrak{b}(\mathfrak{u}_p) \simeq \mathfrak{u}_p^+ \otimes U(\mathfrak{h}_p) \quad \text{and} \quad \mathfrak{b}^-(\mathfrak{u}_p) \simeq \mathfrak{u}_p^- \otimes U(\mathfrak{h}_p). \tag{2}$$

The bilinear form S_p factors through $\mathfrak{u}_p^-$. We denote the bilinear form $\mathfrak{u}_p^- \times \mathfrak{u}_p^- \to U(\mathfrak{h}_p)$ thus obtained by the symbol s_p.

As is well known, the algebra $\mathfrak{u}_p^+$ (resp. $\mathfrak{u}_p^-$) has the elements $\{e^t\}$ (resp. $\{f^t\}$) (cf. (2) of §2) as a $\mathbf{F}_p$-basis, where $t = (t_1, \dots, t_N)$ ranges over those elements of $\mathbb{Z}_+^N$ such that $0 \le t_j < p$, for all j .

Let $Q := \sum_{i=1}^n \mathbb{Z}\alpha_i$ denote the root lattice in $\mathfrak{h}^*$. For any $\eta \in Q$, define

$$\mathcal{P}(\eta) = \{t \in \mathbb{Z}_+^N :\mid t \mid = \eta\}, \qquad \text{and} \tag{3}$$

$$\mathcal{P}_{\text{res}}(\eta) = \{t = (t_1, \dots, t_N) \in \mathcal{P}(\eta) : 0 \le t_j < p, \ \text{ for all } \ j\}, \tag{4}$$

where, for $t \in \mathbb{Z}_+^N, \mid t \mid := \sum_{j=1}^N t_j\beta_j$ and $\{\beta_j\}$ is the ordering as in (13) of §2. Of course $\mathcal{P}(\eta) = \phi$, unless $\eta \in Q^+ := \sum_{i=1}^n \mathbb{Z}_+\alpha_i$. Also, for $\beta_j \in \triangle^+$ and $m \in \mathbb{Z}_+$, define

$$\mathcal{P}_{\text{res}}(\eta, m\beta_j) = \{t \in \mathbb{Z}_+^N : (t_1, \dots, t_{j-1}, t_j + m, t_{j+1}, \dots, t_N) \in \ \mathcal{P}_{\text{res}}(\eta)\}, \tag{5}$$

and set
(6)

$$P(\eta) = \#\ \mathcal{P}(\eta),\ P_{\mathrm{res}}(\eta) = \#\ \mathcal{P}_{\mathrm{res}}(\eta), \text{ and } P(\eta, m\beta_j) = \#\ \mathcal{P}_{\mathrm{res}}(\eta, m\beta_j).$$

For any $\eta \in Q^+$, set

$$\det_\eta(s_p) = \det(s_p(f^\varphi, f^\psi))_{\varphi,\psi \in\ \mathcal{P}_{\mathrm{res}}(\eta)} \in U(\mathfrak{h}_p).$$

The following result gives the decomposition of $\det_\eta(s_p)$.

Theorem 3.2. *With the notation as above, for any $\eta \in Q^+$,*

$$\det_\eta(s_p) = \prod_{\beta \in \Delta^+} \prod_{0<m<p} [H_\beta + (\rho, \check{\beta}) - m]^{P(\eta, m\beta)},$$

up to a non-zero scalar multiple in $\mathbf{F}_p$, where $H_\beta, \check{\beta}, \rho$, and the Killing form $(\ ,\ )$ are as in Section 2.

Definition 3.3. By virtue of Proposition 4.4(c), we get

$$\mathfrak{U}_\xi = (\mathcal{I}(\mathfrak{U}_\xi^-)\mathfrak{U}_\xi + \mathfrak{U}_\xi \mathcal{I}(\mathfrak{U}_\xi^+)) \oplus \mathfrak{U}_\xi^o,$$

where $\mathcal{I}(\mathfrak{S})$ denotes the augmentation ideal of any augmented algebra $\mathfrak{S}$. The above decomposition gives rise to the *quantized Harish-Chandra homomorphism*

$$\mathfrak{H}_\xi : \mathfrak{U}_\xi \to \mathfrak{U}_\xi^o,$$

by projecting on the second factor.

Just as in §3.1, define the *Shapovalov bilinear form*

$$S_\xi : \mathfrak{U}_\xi^- \times \mathfrak{U}_\xi^- \to \mathfrak{U}_\xi^o \quad \text{by}$$
$$S_\xi(v, w) = \mathfrak{H}_\xi(\Omega(v)w),$$

where Ω is the $\mathbb{Q}$-algebra anti-automorphism of $\mathfrak{U}_\xi$ (cf. [**L2**, §1.1]), defined by

$$\Omega(E_i) = F_i, \quad \Omega(F_i) = E_i, \quad \Omega(K_i) = K_i^{-1}, \quad \text{and } \ \Omega(\xi) = \xi^{-1}.$$

The elements $\{E_{\beta_j}^p, F_{\beta_j}^p; 1 \leq j \leq N\}$ are central in $\mathfrak{U}_\xi$ (cf. [**DK**, Corollary 3.1]). Let $\mathfrak{u}_\xi$ be the quotient algebra $\mathfrak{U}_\xi / \langle E_{\beta_j}^p,\ F_{\beta_j}^p;\ 1 \leq j \leq N\rangle$. Similarly define

$$\mathfrak{u}_\xi^+ = \mathfrak{U}_\xi^+ / \langle E_{\beta_j}^p; 1 \leq j \leq N\rangle, \quad \mathfrak{u}_\xi^- = \mathfrak{U}_\xi^- / \langle F_{\beta_j}^p; 1 \leq j \leq N\rangle,$$

and

$$\mathfrak{b}_\xi = \mathfrak{B}_\xi / \langle E^p_{\beta_j}; 1 \leq j \leq N \rangle, \quad \mathfrak{b}^-_\xi = \mathfrak{B}^-_\xi / \langle F^p_{\beta_j}; 1 \leq j \leq N \rangle,$$

where $\mathfrak{B}_\xi$ (resp. $\mathfrak{B}^-_\xi$) is the subalgebra $\mathfrak{U}^o_\xi \mathfrak{U}^+_\xi$ (resp. $\mathfrak{U}^o_\xi \mathfrak{U}^-_\xi$) of $\mathfrak{U}_\xi$. Observe that

$$\text{(1)} \qquad \mathfrak{b}_\xi \simeq \mathfrak{u}^+_\xi \otimes \mathfrak{U}^o_\xi \quad \text{and} \quad \mathfrak{b}^-_\xi \simeq \mathfrak{u}^-_\xi \otimes \mathfrak{U}^o_\xi.$$

From Proposition 4.4(a), we obtain that $\mathfrak{u}^+_\xi$ (resp. $\mathfrak{u}^-_\xi$) is a free $\mathbb{Q}_\xi$-module with basis $\{E^t\}$ (resp. $\{F^t\}$), where $t = (t_1, \dots, t_N)$ ranges over those elements of $\mathbb{Z}^N_+$ such that $0 \leq t_j < p$, for all j.

It is easy to see that the bilinear form S_ξ factors through $\mathfrak{u}^-_\xi$ to give rise to the bilinear form

$$s_\xi : \mathfrak{u}^-_\xi \times \mathfrak{u}^-_\xi \longrightarrow \mathfrak{U}^o_\xi.$$

For any $\eta \in Q^+$, define

$$\det{}_\eta(s_\xi) = \det(s_\xi(F^\varphi, F^\psi))_{\varphi,\psi \in \mathcal{P}_{\text{res}}(\eta)} \in \mathfrak{U}^o_\xi.$$

Now the following is the quantized analog of Theorem (3.2) factoring $\det_\eta(s_\xi)$.

Theorem 3.4. *With the notation as above,*

$$\det{}_\eta(s_\xi) = c \prod_{\beta \in \Delta^+} \prod_{0<m<p} \left[K_\beta - \xi^{2(m-(\rho,\beta^\vee))d_\beta} K_\beta^{-1} \right]^{P(\eta, m\beta)},$$

for some non-zero $c \in \mathbb{Q}_\xi$; where for $\beta = \sum m_i \alpha_i, K_\beta := K_1^{m_1} \cdots K_n^{m_n}$, and $d_\beta := \frac{(\beta,\beta)}{2}$.

The following result follows immediately from Theorems (3.2) and (3.4). This result in the modular case is classical (cf. [**H2**, §5.5]) and in the quantum case due to Andersen-Polo-Wen [**APW**, Corollary 7.6 and Theorem 9.8].

Corollary 3.5. *The Steinberg module $M_{\mathbf{F}_p}((p-1)\rho)$ (resp. $M_{\mathbb{Q}_\xi}(\xi^{(p-1)\rho})$) is an irreducible module for $\mathfrak{u}_p$ (resp. $\mathfrak{u}_\xi$), where for any $\lambda \in \mathfrak{h}^*_\mathbb{Z}$, $M_{\mathbf{F}_p}(\lambda)$ and $M_{\mathbb{Q}_\xi}(\xi^\lambda)$ are defined in §10.*

4. Proof of the main theorems – Some preliminary work.

The following two lemmas allow us to move one element pass another. The first is more general and will be applied to the modular case.

Lemma 4.1. *Let a, b be two elements in a ring R. Write $(\overline{\mathrm{ad}}\, a)b$ for $ab - ba$. We have*

$$a^m b = \sum_{0 \le j \le m} \binom{m}{j} \left(\left(\overline{\mathrm{ad}}\, a\right)^j b \right) a^{m-j}. \tag{1}$$

Proof. If two elements x, y in a ring R commute, then of course $(x+y)^m = \sum_{0 \le j \le m} \binom{m}{j} x^j y^{m-j}$. Applying this to the ring End (R) (of all $\mathbb{Z}$-linear maps of R to itself) with $x = \overline{\mathrm{ad}}\, a$ and $y = R_a$ (where $R_a : R \to R$ is given by $r \mapsto ra$), we get the lemma. □

We need a Hopf algebra analog of the above lemma for the Hopf algebra $U_q(\mathfrak{g})$. Rather than stating the result for general Hopf algebras, we will confine ourselves to the Hopf algebra $U_q(\mathfrak{g})$ in the following lemma. We remark that the definition of $\overline{\mathrm{ad}}$ is available for any ring, in contrast to the definition of ad given in (11) of §2 for Hopf algebras. Observe that the two definitions do not coincide in general for Hopf algebras. Set $F = F_i$, $K = K_i$, and $\alpha = \alpha_i$ in the following lemma.

Lemma 4.2. *For any $m \ge 1$ and any $b \in U_q(\mathfrak{g})$,*

$$F^m b = \sum_{0 \le j \le m} \begin{bmatrix} m \\ j \end{bmatrix}_{q^{d_i}} q^{-d_i(j^2 - jm)} \left((\mathrm{ad}\ \ F)^j b \right) F^{m-j} K^{-j}, \tag{1}$$

where $\begin{bmatrix} m \\ j \end{bmatrix}_{q^{d_i}} := \frac{[m]!_{d_i}}{[j]!_{d_i} [m-j]!_{d_i}}$.

Proof. By (12) of §2,

$$Fb = bF + ((\mathrm{ad}\ \ F)b)K^{-1}, \tag{2}$$

which proves (1) for $m = 1$. Assume (1) holds for $m - 1$. Then using (2), we get

$$\begin{aligned} &F(F^{m-1}b) \\ &= \sum_{0 \le j \le m-1} \begin{bmatrix} m-1 \\ j \end{bmatrix} q^{-d_i(j^2 - j(m-1))} ((\mathrm{ad}\ \ F)^j b) F^{m-1-j} K^{-j} F \end{aligned}$$

$$
\begin{aligned}
&+\sum_{0\le j\le m-1}\begin{bmatrix} m-1\\ j\end{bmatrix} q^{-d_i(j^2-j(m-1))}(\text{ad }\ F)(((\text{ad }\ F)^j b)F^{m-1-j}K^{-j})K^{-1}\\
&=\sum_{0\le j\le m-1}\begin{bmatrix} m-1\\ j\end{bmatrix} q^{-d_i(j^2-j(m-1))}((\text{ad }\ F)^j b)F^{m-j}K^{-j}\\
&+\sum_{1\le j\le m}\begin{bmatrix} m-1\\ j-1\end{bmatrix} q^{-d_i((j-1)^2-(j-1)(m-1))+2d_i(m-j)}((\text{ad }\ F)^j b)F^{m-j}K^{-j},
\end{aligned}
$$

where we have dropped the q-binomial coefficient subscript of q^{d_i}. The lemma now follows from the identity

$$\begin{bmatrix} m-1\\ j-1\end{bmatrix}_v v^{m-j}+\begin{bmatrix} m-1\\ j\end{bmatrix}_v v^{-j}=\begin{bmatrix} m\\ j\end{bmatrix}_v .$$

□

Lemma 4.3. *Let $a, b_1, \dots, b_r$ be elements in a ring R of char. 0. Then for any $m \geq 0$*

$$\frac{(\overline{\text{ad}}\, a)^m}{m!}(b_1\dots b_r)=\sum_{\ell\in S_m}\frac{(\overline{\text{ad}}\, a)^{\ell_1}}{\ell_1!}(b_1)\frac{(\overline{\text{ad}}\, a)^{\ell_2}}{\ell_2!}(b_2)\dots\frac{(\overline{\text{ad}}\, a)^{\ell_r}}{\ell_r!}(b_r)\ ,$$

where S_m is the set of r-tuples $\ell = (\ell_1, \dots, \ell_r) \in \mathbb{Z}_+^r$ such that $\sum_{i=1}^r \ell_i = m$.

Proof. The lemma follows immediately from [**H1**, p. 152, Proof of Lemma A]. □

Recall the definition of the subring $\mathcal{B} \subset \mathbb{Q}(q)$ from §2. Observe that $\Omega(\mathcal{B}) = \mathcal{B}, \Omega(\mathfrak{U}_\mathcal{B}) = \mathfrak{U}_\mathcal{B}$ and $\Omega(\mathfrak{U}_\mathcal{B}^+) = \mathfrak{U}_\mathcal{B}^-$ (where Ω is as in §3.3). We have

Proposition 4.4.

(a) $\mathfrak{U}_\mathcal{B}^+$ *(resp. $\mathfrak{U}_\mathcal{B}^-$) is a free $\mathcal{B}$-module with basis $\{E^t\}$ (resp. $\{F^t\}$), where $t = (t_1, \dots, t_N)$ runs over $\mathbb{Z}_+^N$.*

(b) $\mathfrak{U}_\mathcal{B}^0$ *is generated (as a $\mathcal{B}$-algebra) by $\{K_i, [K_i; 1]; 1 \leq i \leq n\}$, where $[K_i; 1] := \frac{K_i - K_i^{-1}}{q^{d_i} - q^{-d_i}}$, and moreover $\mathfrak{U}_\mathcal{B}^0$ is a free $\mathcal{B}$-module with basis $\{(\prod_i K_i^{\delta_i})[K; 1]^m\}$, where m runs over $\mathbb{Z}_+^n$ and $\delta_i \in \{0, 1\}$. (The notation $[K; 1]^m$ is defined below in the proof.)*

(c) *We have a $\mathcal{B}$-module isomorphism*

$$\mathfrak{U}_\mathcal{B}^- \otimes_\mathcal{B} \mathfrak{U}_\mathcal{B}^0 \otimes_\mathcal{B} \mathfrak{U}_\mathcal{B}^+ \cong \mathfrak{U}_\mathcal{B}$$

under the (canonical) multiplication map.

Proof. Any T_i (cf. §2) clearly keeps $\mathfrak{U}_{\mathcal{B}}$ stable. In particular, $E^t, F^t \in \mathfrak{U}_{\mathcal{B}}$. Further $[E_i, F_i] = [K_i; 1] \in \mathfrak{U}_{\mathcal{B}}$. Define

$$\widehat{\mathfrak{U}_{\mathcal{B}}} = \sum \mathcal{B} F^t K^m [K; 1]^{m'} E^{t'} \subset U_q(\mathfrak{g}),$$

where t, t' run over $\mathbb{Z}_+^N, m'$ runs over $\mathbb{Z}_+^n$, and m runs over $\mathbb{Z}^n$; and where $K^m := K_1^{m_1} \cdots K_n^{m_n}$ (for $m = (m_1, \ldots, m_n)$) and $[K;1]^m := [K_1;1]^{m_1} \cdots [K_n;1]^{m_n}$. Clearly $\widehat{\mathfrak{U}_{\mathcal{B}}} \subset \mathfrak{U}_{\mathcal{B}}$. We next prove that $\widehat{\mathfrak{U}_{\mathcal{B}}}$ is an algebra.

It suffices to show that the following elements belong to $\widehat{\mathfrak{U}_{\mathcal{B}}}$.

$$(1)\, E^{t'} F^t \quad (2)\, E^{t'} E^t \quad (3)\, F^{t'} F^t \quad (4)\, E^{t'} [K;1]^{m'} \quad (5)\, [K;1]^{m'} F^t.$$

The proof that the elements (3) belong to $\widehat{\mathfrak{U}_{\mathcal{B}}}$ is similar to that for (2). Moreover, the elements (4) and (5) belong to $\widehat{\mathfrak{U}_{\mathcal{B}}}$ follows from [**L2**, §6.5, Identities (a5) and (a6)]. The assertion that the elements (2) belong to $\widehat{\mathfrak{U}_{\mathcal{B}}}$ follows by repeated use of the relations [**L2**, §5.2] for rank-2 Lie algebras, and the degree function d introduced in [**DK**, §1.7]. The elements (1) belong to $\widehat{\mathfrak{U}_{\mathcal{B}}}$ follows from the same argument as in [**DK**, Proof of Proposition 1.7]. This completes the proof that $\widehat{\mathfrak{U}_{\mathcal{B}}}$ is an algebra.

We next show that $\mathfrak{U}_{\mathcal{B}} \subset \widehat{\mathfrak{U}_{\mathcal{B}}}$. For this it suffices to show that $E_i, F_i \in \widehat{\mathfrak{U}_{\mathcal{B}}}$, for all $1 \leq i \leq n$.

Fix a simple root α_i and let $1 \leq j \leq N$ be such that $\beta_j = \alpha_i$. Let $U_{\mathcal{B}}$ be the Lusztig's $\mathcal{B}$-form of $U_q(\mathfrak{g})$. Then since $U_{\mathcal{B}}^+ := U_{\mathcal{B}} \cap U_q^+$ is generated by $E_l^{(m)}$ $(1 \leq l \leq n, m \geq 0)$, the α_i-weight space W_{α_i} (cf., e.g., [**K**, Definition 2.8] for the definition of weight) of $U_{\mathcal{B}}^+$ is equal to $\mathcal{B} E_i$. Further, by [**L2**, Theorem 6.7], $W_{\alpha_i} = \mathcal{B} E_{\beta_j}$. In particular, $E_i \in \mathcal{B} E_{\beta_j}$. This proves that $E_i \in \widehat{\mathfrak{U}_{\mathcal{B}}}$. A similar argument gives that $F_i \in \widehat{\mathfrak{U}_{\mathcal{B}}}$. Hence $\widehat{\mathfrak{U}_{\mathcal{B}}} = \mathfrak{U}_{\mathcal{B}}$. This, in particular, gives that $\mathfrak{U}_{\mathcal{B}}^+ = \sum_{t \in \mathbb{Z}_+^N} \mathcal{B} E^t, \mathfrak{U}_{\mathcal{B}}^- = \sum_{t \in \mathbb{Z}_+^N} \mathcal{B} F^t$, and $\mathfrak{U}_{\mathcal{B}}^0 = \sum_{m \in \mathbb{Z}^n, m' \in \mathbb{Z}_+^n} \mathcal{B} K^m [K;1]^{m'}$. But E^t (resp. F^t) are linearly independent over $\mathbb{Q}(q)$ (cf. [**L2**, Proposition 4.2]), hence (a) follows.

By using the relation

$$(1) \qquad K_i^2 = (q^{d_i} - q^{-d_i}) K_i [K_i; 1] + 1,$$

it is easy to see that $\mathfrak{U}_{\mathcal{B}}^0$ is a free $\mathcal{B}$-module with basis $\{(\prod_i K_i^{\delta_i})[K;1]^m\}$, where m runs over $\mathbb{Z}_+^n$ and $\delta_i \in \{0, 1\}$. This proves (b) and also proves (c), since $\widehat{\mathfrak{U}_{\mathcal{B}}} = \mathfrak{U}_{\mathcal{B}}$. □

The next two lemmas will allow us to do some of the necessary computations in $\mathfrak{U}_{\mathcal{B}}$. Recall the relation (12) of §2 determining ad E_i and ad F_i.

Lemma 4.5. *For all $m \geq 0$ and $i \neq j$,*
(a) (ad $E_i^{(m)}$)$E_j \in \mathfrak{U}_{\mathcal{B}}^+$, (ad $F_i^{(m)}$)$F_j K_j \in \mathfrak{U}_{\mathcal{B}}^- K_i^m K_j$.

(b) $(\text{ad } E_i^{(m)})E_j = (\text{ad } F_i^{(m)})F_jK_j = 0$, *for* $m \geq -a_{ij}+1$.

Proof. Note that $(\text{ad } E_i^{(-a_{ij}+1)})E_j = 0$ for $i \neq j$ (see [**L2**, §§1.1 and 1.3] or [**JL1**]; this is just the quantized Serre relation). Hence (to prove the assertion regarding E's), we need only show that

$$\left(\text{ad } E_i^{(m)}\right) E_j \in \mathfrak{U}_{\mathcal{B}}^+ \qquad \text{for } 1 \leq m \leq -a_{ij}. \tag{1}$$

Since $-a_{ij} \leq a$ (cf. §2 for the definition of a), we have

$$([m]!_{d_l})^{-1} \in \mathcal{B} \qquad \text{for each } 1 \leq m \leq -a_{ij} \text{ and } 1 \leq l \leq n. \tag{2}$$

Now (1) follows from (2) and [**L2**, §1.3]. A similar argument proves the assertions regarding F's. □

Lemma 4.6. *Let $b \in \mathfrak{U}_{\mathcal{B}}^+$ be a weight vector of weight $\sum m_j\alpha_j$. Then*

$$\left(\text{ad } E_i^{(k)}\right)(bK_i^{-m_i}) \in \mathfrak{U}_{\mathcal{B}}^+K_i^{-m_i},$$

for all $k \geq 0$ and $1 \leq i \leq n$. Moreover, there is an integer $k_o \geq 0$ depending on b such that (ad $E_i^{(k)}$)$(bK_i^{-m_i}) = 0$ for all $k \geq k_o$.

Similarly, if $c \in \mathfrak{U}_{\mathcal{B}}^-$ is of weight $-\sum m_j\alpha_j$, then

$$\left(\text{ad } F_i^{(k)}\right)(cK^mK_i^{-m_i}) \in \mathfrak{U}_{\mathcal{B}}^-K^mK_i^{-m_i}K_i^k,$$

for all $k \geq 0$ and there is an integer k_o depending on c such that $(\text{ad } F_i^{(k)})(cK^mK_i^{-m_i}) = 0$ *for all $k \geq k_o$, where $K^m := K_1^{m_1}\cdots K_n^{m_n}$.*

Proof. Let b_1 (resp. b_2) be an element of $\mathfrak{U}_{\mathcal{B}}^+$ of weight $\alpha = \sum_j n_j\alpha_j$ (resp. $\beta = \sum_j r_j\alpha_j$). By [**L2**, §1.3] and [**JL1**, §2.2], we have

$$\begin{aligned}&\left(\text{ad } E_i^{(k)}\right)(b_1K_i^{-n_i}b_2K_i^{-r_i})\\ &= \sum_{l=0}^{k} q^{d_il(k-l)}\left(\text{ad } E_i^{(k-l)}\right)\left(q^{l(\alpha_i,\alpha)}b_1K_i^{-n_i}\right)\left(\text{ad } E_i^{(l)}\right)(b_2K_i^{-r_i}).\end{aligned}$$

This calculation shows that if the lemma is true for the elements b_1, $b_2 \in \mathfrak{U}_{\mathcal{B}}^+$ then it is also true for the product b_1b_2. So it suffices to prove that $(\text{ad } E_i^{(k)})E_j \in \mathfrak{U}_{\mathcal{B}}^+$ for $i \neq j$ and $(\text{ad } E_i^{(k)})E_j = 0$ for $i \neq j$ and for all $k \gg 0$, and also $(\text{ad } E_i)(E_iK_i^{-1}) = 0$. The first two assertions follow from Lemma (4.5), and the third is a straightforward computation. This proves the lemma for $b \in \mathfrak{U}_{\mathcal{B}}^+$. The proof for $c \in \mathfrak{U}_{\mathcal{B}}^-$ is similar. □

Definition 4.7. Given a finite subset $V \subset \mathfrak{b}^-(\mathfrak{u}_p)$ (cf. §3.1), define the $V \times V$- matrix

$$M_V(s_p) = (\mathfrak{H}_p(\omega(v)w))_{v,w\in V} \qquad \text{and} \tag{1}$$

$$\det_V(s_p) = \det M_V(s_p). \tag{2}$$

Similarly, for $V \subset \mathfrak{b}_\xi^-$,

$$\det_V(s_\xi) = \det(\mathfrak{H}_\xi(\Omega(v)w))_{v,w\in V}. \tag{3}$$

The next lemma will be crucial in factoring the Shapovalov determinant. Much of the rest of this paper will be devoted to finding suitable elements g and $b_1, \dots , b_r$ that satisfy the conditions of this lemma. Being a Laurent polynomial ring, $\mathfrak{U}_\xi^0$ is a unique factorization domain.

Lemma 4.8. *Fix $\eta \in Q^+$. Let g be an irreducible polynomial in $U(\mathfrak{h}_p)$ (resp. $\mathfrak{U}_\xi^0$). Suppose there exist elements $b_1, \dots , b_r$ in $\mathfrak{b}^-(\mathfrak{u}_p)$ (resp. $\mathfrak{b}_\xi^-$) of weight $-\eta$ such that*

(i) *The elements $\{b_j;\ 1 \le j \le r\}$ are linearly independent considered as elements of the right $U(\mathfrak{h}_p)/\langle g\rangle$-module $\mathfrak{u}_p^- \otimes (U(\mathfrak{h}_p)/\langle g\rangle)$ (resp. $\mathfrak{U}_\xi^0/\langle g\rangle$-module $\mathfrak{u}_\xi^- \otimes (\mathfrak{U}_\xi^0/\langle g\rangle)$) (cf. (2) of §3.1 and (1) of §3.3),*

(ii) *$\mathfrak{H}_p(vb_j) \in U(\mathfrak{h}_p)g$ (resp. $\mathfrak{H}_\xi(vb_j) \in \mathfrak{U}_\xi^0 g$) for all $v \in \mathfrak{u}_p^+$ (resp. $\mathfrak{u}_\xi^+$) of weight η.*

Then g^r divides $\det_\eta(s_p)$ (resp. $\det_\eta(s_\xi)$).

Proof. We prove the lemma for $\det_\eta(s_p)$. (The proof in the case of $\det_\eta(s_\xi)$ is similar.) Choose elements $\{b_{r+1}, \dots , b_s\}$ in $\mathfrak{u}_p^-$ of weight $-\eta$ such that the set $R = \{b_1, \dots , b_r, b_{r+1}, \dots , b_s\}$ is an L-basis for the $-\eta$ weight space of $\mathfrak{u}_p^- \otimes L$, where L is the quotient field of the integral domain $U(\mathfrak{h}_p)/\langle g\rangle$. We may write (for $1 \le j \le s$)

$$b_j = \sum_{t\in\mathcal{P}_{\mathrm{res}}(\eta)} f^t c_{jt},$$

where $\mathcal{P}_{\mathrm{res}}(\eta)$ is as in (4) of §3.1 and $c_{jt} \in U(\mathfrak{h}_p)$. Set C as the matrix $[c_{jt}]$. Since C is the transformation matrix between the two bases of the $-\eta$ weight space of $\mathfrak{u}_p^- \otimes L$ (over L), we obtain

$$\det C \notin U(\mathfrak{h}_p)g. \tag{1}$$

It is straightforward to check that

$$M_R(s_p) = C^t M_{R_o}(s_p)C,$$

where $R_o = \{f^t; t \in \mathcal{P}_{\mathrm{res}}(\eta)\}$; and hence $\det_R(s_p) = (\det C)^2 \det_\eta(s_p)$. Now assumption (ii) forces g^r to divide $\det_R(s_p)$. Since g is irreducible, by (1), $\det C$ and g must be relatively prime. Hence g^r divides $\det_\eta(s_p)$. This proves the lemma. □

We close this section with some properties of Δ^+ which will be needed for the factorization of the Shapovalov determinant in the next sections.

Lemma 4.9. *If p is an odd prime which is not equal to three if G_2 is a component of $\mathfrak{g}$, then the following are satisfied.*

(a) *If $\sum m_i\alpha_i$ and $\sum l_i\alpha_i$ are distinct elements of Δ^+, then $m_i \not\cong l_i (\mathrm{mod}\ p)$ for at least one $1 \leq i \leq n$.*

(b) *If $\beta \in \Delta^+$, then β is not zero* mod p *with respect to the weight lattice.*

(c) *No two distinct positive* ***coroots*** *are equal* mod p (*in the sense of* (a)).

Proof. Assertions (a) and (c) follow from the explicit knowledge of the roots and coroots as given in [B].

For the (b) part, write $\alpha \in \Delta^+$ as $\alpha = \sum n_i\chi_i$ where the χ_i are the fundamental weights. Thus $\langle \alpha, \check{\alpha}_i\rangle = n_i$. Write $\check{\alpha} = \sum m_i\check{\alpha}_i$, where $m_i \in \mathbb{Z}$. Then $\langle \alpha, \check{\alpha}\rangle = 2 = \sum_i m_i n_i$. So if α is zero $\mod p$ (i.e. every n_i is zero $\mod p$), then 2 is divisible by p. This contradicts the choice of p and hence proves the (b)-part. Observe that for the (b)-part, we just need $p \neq 2$. □

5. Special elements in $U(\mathfrak{g}_\mathbb{Z})$.

In [S], Shapovalov defined certain elements of $U(\mathfrak{g})$ (corresponding to any positive root and a positive integer) that produced highest weight vectors in certain Verma modules. These elements were then used to determine the factors and multiplicities of the classical Shapovalov determinant by applying a version of Lemma 4.8. In this section, we make a careful choice of these elements in order to specialize them to $U(\mathfrak{g}_p)$, and in a later section, use them to factor the modular Shapovalov determinant.

Definition 5.1. A reflection $s \in W$ induces an affine automorphism $\tilde{s}$ of $U(\mathfrak{h})$ as follows. Given a simple positive root α, define $\tilde{s}(H_\alpha) = H_{s\alpha} + (\rho, s\check{\alpha}) - (\rho, \check{\alpha})$ and extend this to an algebra homomorphism of $U(\mathfrak{h})$. Since s preserves the coroot lattice (i.e., the lattice $\mathfrak{h}_\mathbb{Z} = \sum_i \mathbb{Z}H_i$), it follows that $\tilde{s}(U(\mathfrak{h}_\mathbb{Z})) \subseteq U(\mathfrak{h}_\mathbb{Z})$.

For $\gamma \in \Delta^+$ and $m > 0$ let $I_{\gamma,m}$ denote the ideal in $U(\mathfrak{h})$ generated by $(H_\gamma + \rho(H_\gamma) - m)$.

The next proposition is a strengthened version of [S, Lemma 1] (cf. also [F]). We write $\deg a$ to denote the total degree of a considered as an element of $U(\mathfrak{g})$ using the standard filtration. Recall the definition of $\mathfrak{n}_{\mathbb{Z}}^-$ from (3) of §2.

Proposition 5.2. *For any integer $m > 0$ and $\gamma \in \Delta^+$, there exists a non-zero element $\Theta_{\gamma,m} \in U(\mathfrak{n}_{\mathbb{Z}}^-)U(\mathfrak{h}_{\mathbb{Z}})$ of weight $-m\gamma$ such that*

(i) $[e_\beta, \Theta_{\gamma,m}] \in U(\mathfrak{n}^-)I_{\gamma,m} + U(\mathfrak{g})\mathfrak{n}^+$, *for all $\beta \in \Delta^+$, and*

(ii) $\deg \Theta_{\gamma,m}$ *is precisely equal to $\sum_i m\ell_i$, where $\gamma = \sum_{i=1}^n \ell_i\alpha_i$.*

Proof. If $\rho(H_\gamma) = 1$, then γ is a simple positive root, say α_i. In this case, as in [**S**, Lemma 1], we may take $\Theta_{\gamma,m} = f_i^m \in U(\mathfrak{n}_{\mathbb{Z}}^-)$, which clearly satisfies (i) and (ii).

So assume $\rho(H_\gamma) > 1$. There exists a simple root ϵ and $\gamma_1 \in \Delta^+$ such that $\gamma_1 = s_\epsilon\gamma$ and $\rho(H_{\gamma_1}) < \rho(H_\gamma)$. Note that $\gamma - \gamma_1 = r\epsilon$ where $r = (\gamma, \check{\epsilon}) > 0$.

Consider the hyperplane

$$L_{\gamma,m} = \{\chi \in \mathfrak{h}^*;\ \chi(H_\gamma) = m\} \tag{1}$$

in $\mathfrak{h}^*$ and the subset

$$B_\epsilon := \{\lambda \in \mathfrak{h}_{\mathbb{Z}}^* \cap L_{\gamma,m}; (\lambda, \check{\epsilon}) < 0\}. \tag{2}$$

It is easy to see that B_ϵ is dense in $L_{\gamma,m}$ in the Zariski topology (cf., e.g., [**BGG**]).

Fix $\lambda \in B_\epsilon$ and set $\psi = s_\epsilon\lambda$. We have the following inclusions of Verma modules

$$M(\psi - \rho) \supset M(\lambda - \rho) \supset M(\lambda - m\,\gamma - \rho), \tag{3}$$

$$M(\psi - \rho) \supset M(\psi - m\gamma_1 - \rho) \supset M(\lambda - m\,\gamma - \rho). \tag{4}$$

Let v be a highest weight vector for $M(\psi - \rho)$ (of weight $\psi - \rho$). By induction on $(\rho, \check{\gamma})$, there exists $\Theta_{\gamma_1,m} \in U(\mathfrak{n}_{\mathbb{Z}}^-)U(\mathfrak{h}_{\mathbb{Z}})$ which satisfies (i) and (ii). Write $\Theta_{\gamma_1,m} = \sum_{t\in\mathcal{P}(m\gamma_1)} f^t p_t$, where $p_t \in U(\mathfrak{h}_{\mathbb{Z}})$. Inclusion (4) implies that

$$f_\epsilon^{-(\lambda,\check{\epsilon})+mr} \sum_{t\in\mathcal{P}(m\gamma_1)} f^t(\psi - \rho)(p_t) \tag{5}$$

applied to v is a highest weight vector for $M(\lambda - m\gamma - \rho)$. Now $(\psi - \rho, \check{\gamma}) = (\lambda - \rho, s_\epsilon\check{\gamma}) + (\rho, s_\epsilon\check{\gamma}) - (\rho, \check{\gamma})$. Hence $(\psi - \rho)p_t = (\lambda - \rho)(\tilde{s}_\epsilon(p_t))$. Combined with Lemma 4.1, this shows that (5) equals

$$\sum_{t,j} \left(\frac{(\mathrm{ad}\ f_\epsilon)^j}{j!} f^t \right) f_\epsilon^{-(\lambda,\check{\epsilon})+mr-j}(\lambda - \rho)(P_{j,t}), \tag{6}$$

where t runs through the elements in $\mathcal{P}(m\gamma_1)$, j runs through the integers $\{0, 1, \dots, -(\lambda, \check{\epsilon}) + mr\}$, and $P_{j,t} = \left(\prod_{1\le \ell\le j}(-H_\epsilon + mr - \ell)\right) \tilde{s}_\epsilon(p_t)$. (Observe that for the Hopf algebra $U(\mathfrak{g})$, $(\mathrm{ad}\ X)a = (\overline{\mathrm{ad}}\ X)a$, for any $X \in \mathfrak{g}$, and $a \in U(\mathfrak{g})$.)

By [H1, Corollary 26.3], $\frac{(\mathrm{ad}\, f_\epsilon)^j}{j!} U(\mathfrak{n}^-_{\mathbb{Z}}) \subseteq U(\mathfrak{n}^-_{\mathbb{Z}})$. Furthermore, $(\mathrm{ad}\, f_\epsilon)^j f^t = 0$ for $j \gg 0$, and so the above sum (6) has the same number of terms for $(-\lambda, \check{\epsilon}) \gg 0$. By assumption, $p_t \in U(\mathfrak{h}_{\mathbb{Z}})$ and hence $P_{j,t} \in U(\mathfrak{h}_{\mathbb{Z}})$. Set

$$\bar{\Theta}_{\gamma,m} = \sum_{t\in\mathcal{P}(m\gamma_1)} \sum_{0\le j} \left(\frac{(\mathrm{ad}\, f_\epsilon)^j}{j!} f^t \right) f_\epsilon^{mr-j} P_{j,t}.$$

This is a finite sum and each summand is contained in $U(\mathfrak{n}^-_{\mathbb{Z}})[f_\epsilon^{-1}]U(\mathfrak{h}_{\mathbb{Z}})$. (Note that $\bar{\Theta}_{\gamma,m}$ is not necessarily an element of $U(\mathfrak{n}^-_{\mathbb{Z}})U(\mathfrak{h}_{\mathbb{Z}})$.) Furthermore one easily checks (using expression (6)) that for $\lambda \in B_\epsilon$ such that $(-\lambda, \check{\epsilon}) \gg 0$

$$\bar{\Theta}_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v = f_\epsilon^{-(\lambda,\check{\epsilon})+mr} \Theta_{\gamma_1,m} v. \tag{7}$$

Fix an ordering of Δ^+ as in (13) of §2 such that ϵ is the smallest element. Given an element a in $U(\mathfrak{n}^-_{\mathbb{Z}})[f_\epsilon^{-1}]U(\mathfrak{h}_{\mathbb{Z}})$, write a in terms of the PBW basis thus obtained (cf. (2) of §2), and let $[a]^+_\epsilon$ denote the sum of those terms with non-negative powers of f_ϵ. Set

$$\Theta_{\gamma,m} = \sum_{t\in\mathcal{P}(m\gamma_1)} \sum_{0\le j} \left[\left(\frac{(\mathrm{ad}\, f_\epsilon)^j}{j!} f^t \right) f_\epsilon^{mr-j} \right]^+_\epsilon P_{j,t}. \tag{8}$$

Of course, $\Theta_{\gamma,m}$ is an element of $U(\mathfrak{n}^-_{\mathbb{Z}})U(\mathfrak{h}_{\mathbb{Z}})$. We prove that for $\lambda \in B_\epsilon$, $(-\lambda, \check{\epsilon}) \gg 0$

$$\bar{\Theta}_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v = \Theta_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v. \tag{9}$$

Write

$$\bar{\Theta}_{\gamma,m} = \sum_{J,k\ge(\lambda,\check{\epsilon})} f^J f_\epsilon^k a_{J,k},$$

where $a_{J,k} \in U(\mathfrak{h}_{\mathbb{Z}})$ and $J = (j_2, \dots, j_N)$ is an $(N-1)$-tuple of non-negative integers. Then

$$\bar{\Theta}_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v = \sum_{J,k\ge(\lambda,\check{\epsilon})} f^J f_\epsilon^k a_{J,k} f_\epsilon^{-(\lambda,\check{\epsilon})} v. \tag{10}$$

Inclusion (3) (resp. (7)) implies that $f_\epsilon^{-(\lambda,\check{\epsilon})} v$ (resp. $\bar{\Theta}_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v$) is annihilated by all the positive root vectors. In particular, by the uniqueness of the embeddings in (3) and (4), we get that there exists $f = \sum_{t\in\mathcal{P}(m\gamma)} b_t f^t \in U(\mathfrak{n}^-) \neq 0$ (for some $b_t \in \mathbb{Q}$) such that $f f_\epsilon^{-(\lambda,\check{\epsilon})} v$ is a highest weight vector of $M(\lambda - m\gamma - \rho)$. Hence

$$(11) \qquad a f f_\epsilon^{-(\lambda,\check{\epsilon})} v = \bar{\Theta}_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v, \qquad \text{for some } \; a \in \mathbb{Q}.$$

We have (by (10))

$$\begin{aligned} a f f_\epsilon^{-(\lambda,\check{\epsilon})} v &= \sum_{J,k\geq(\lambda,\check{\epsilon})} f^J f_\epsilon^k a_{J,k} f_\epsilon^{-(\lambda,\check{\epsilon})} v \\ &= \sum_{J,k} f^J f_\epsilon^{k-(\lambda,\check{\epsilon})} (\lambda-\rho)(a_{J,k}) v. \end{aligned}$$

This forces $(\lambda-\rho)(a_{J,k}) = 0$, unless $k - (\lambda,\check{\epsilon}) \geq -(\lambda,\check{\epsilon})$, i.e., $k \geq 0$. Hence by (10),

$$(12) \qquad \bar{\Theta}_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v = \sum_{J,k\geq 0} f^J f_\epsilon^k a_{J,k} f_\epsilon^{-(\lambda,\check{\epsilon})} v.$$

But the right hand side of this equation is exactly $\Theta_{\gamma,m} f_\epsilon^{-(\lambda,\check{\epsilon})} v$. This proves (9).

Now let v_λ be a non-zero highest weight generating vector for $M(\lambda-\rho)$. We can take $v_\lambda = f_\epsilon^{-(\lambda,\check{\epsilon})} v$. Then by (7) and (9), $\Theta_{\gamma,m} v_\lambda$ is annihilated by all e_β $(\beta \in \Delta^+)$, for each $\lambda \in B_\epsilon$ with $-(\lambda,\check{\epsilon}) \gg 0$. The density of B_ϵ in $L_{\gamma,m}$ implies that $\Theta_{\gamma,m}$ satisfies (i).

To prove assertion (ii), recall that $\gamma_1 = s_\epsilon\gamma = \gamma - r\epsilon$. Hence $\gamma = \sum_{i=1}^n \ell_i\alpha_i$ implies that $\gamma_1 = \sum_{i=1}^n \ell_i\alpha_i - r\epsilon$. By the inductive hypothesis, $\Theta_{\gamma_1,m}$ has degree $(\sum_{i=1}^n m\ell_i) - mr$. Note that the degree function on $U(\mathfrak{n}^-)U(\mathfrak{h})$ may be extended to a degree function on $U(\mathfrak{n}^-)[f_\epsilon^{-1}]U(\mathfrak{h})$ by defining $\deg f_\epsilon^\ell = \ell$ for all $\ell \in \mathbb{Z}$. Since the adjoint action and $\tilde{s}_\epsilon$ both preserve degrees, it follows from (8) that $\deg \Theta_{\gamma,m} \leq \sum_{i=1}^n m\ell_i$. One obtains equality by showing (using induction as in [**S**, Lemma 1]) that $\Theta_{\gamma,m} = \prod_{i=1}^n f_{\alpha_i}^{m\ell_i} + \sum_k a_k b_k$, where $b_k \in U(\mathfrak{h}_\mathbb{Z})$ and $a_k \in U(\mathfrak{n}_\mathbb{Z}^-)$ of weight $-m\gamma$ and $\deg a_k < \sum_{i=1}^n m\ell_i$. (See Proposition 5.6 as well.) □

Observe that $\Theta_{\gamma,m}$ in the above proposition are not unique. We will make a particular choice for $\Theta_{\gamma,m}$ in the sequel.

Definition 5.3. Let ϵ and β be two positive roots. The ϵ-string through β is the set of those roots which are of the form $\beta + k\epsilon$, for some $k \in \mathbb{Z}$. By [**H1**, §9.4], there exist non-negative integers ℓ and s with $\ell + s \leq 3$ such that the ϵ-string through β is precisely the set $\{\beta + k\epsilon;\ -\ell \leq k \leq s\}$.

Lemma 5.4. *Let $\alpha, \beta \in \Delta^+$ and ϵ a simple (positive) root such that $\beta = s_\epsilon \alpha = \alpha + r\epsilon$, for some $r > 0$. Then*

$$\frac{(\operatorname{ad} f_\epsilon)^r}{r!} f_\alpha = \begin{cases} \pm f_\beta, & \text{if } \alpha - \epsilon \notin \Delta^+ \\ \pm 2 f_\beta, & \text{if } \alpha - \epsilon \in \Delta^+. \end{cases}$$

Furthermore, the second possibility occurs only in the case where $\mathfrak{g}$ contains a component of type G_2.

Proof. The proof follows from [**H1**, Theorem 25.2]. Let $\alpha - \ell\epsilon, \dots, \alpha + s\epsilon$ be the ϵ-string through α. Then $r = s - \ell$ and

$$(1) \qquad \frac{(\operatorname{ad} f_\epsilon)^r}{r!} f_\alpha = \pm \frac{(\ell+1)(\ell+2)\dots(\ell+r)}{r!} f_\beta.$$

If $\alpha - \epsilon \notin \Delta^+$, then $\ell = 0$ and the right hand side of (1) is just $\pm f_\beta$. Since $\ell + s \leq 3$, in the case when $\ell \neq 0$ we have $\ell + s = 3$, $\ell = 1$, and $r = 1$; and this can only happen if $\mathfrak{g}$ contains a component of type G_2. Hence if $\alpha - \epsilon \in \Delta^+$, then the right hand side of (1) is $\pm 2 f_\beta$. □

Definition 5.5 (A particular choice for $\Theta_{\gamma,m}$). Fix $\gamma \in \Delta^+$ and $m > 0$. We want to make a particular choice for $\Theta_{\gamma,m}$. Let us choose simple reflections $s_0, \dots, s_v$ (corresponding to simple roots $\epsilon_0, \dots, \epsilon_v$ respectively), and a simple (positive) root γ_{v+1} such that $s_0 \cdots s_v \gamma_{v+1} = \gamma$. Set $\gamma_k = s_k \cdots s_v \gamma_{v+1}$, in particular, $\gamma_0 = \gamma$. Assume further that $s_0, \dots, s_v$ are chosen so that $(\rho, \check{\gamma}_k) > (\rho, \check{\gamma}_{k+1})$ for $0 \leq k \leq v$. Set $r_k = (\gamma_k, \check{\epsilon}_k)$. The assumption on $(\rho, \check{\gamma}_k)$ implies that $r_k > 0$. Note that

$$(1) \qquad \gamma_k = s_k \gamma_{k+1} = \gamma_{k+1} + r_k \epsilon_k.$$

We define elements $\Theta_k = \Theta_{\gamma_k, m}$, $0 \leq k \leq v+1$, in $U(\mathfrak{n}_{\mathbb{Z}}^-)U(\mathfrak{h}_{\mathbb{Z}})$ inductively as follows. Set $\Theta_{v+1} = f_{\gamma_{v+1}}^m$. Assume we have defined Θ_{k+1} and that $\Theta_{k+1} = \sum_{t \in \mathcal{P}(m\gamma_{k+1})} f^t p_t$, where $p_t \in U(\mathfrak{h}_{\mathbb{Z}})$. Define Θ_k by (cf. (8) of §5.2)

$$(2) \quad \Theta_k = \sum_{t,j} \left[\left(\frac{(\operatorname{ad} f_{\epsilon_k})^j}{j!} f^t \right) f_{\epsilon_k}^{m r_k - j} \right]_{\epsilon_k}^+ \left(\prod_{1 \leq \ell \leq j} (-H_{\epsilon_k} + m r_k - \ell) \right) \tilde{s}_k(p_t),$$

where t runs over the elements in $\mathcal{P}(m\gamma_{k+1})$, j runs over the non-negative integers, and $[\quad]_{\epsilon_k}^+$ is as in the proof of Proposition (5.2). By the proof of Proposition 5.2, Θ_k belongs to $U(\mathfrak{n}_{\mathbb{Z}}^-)U(\mathfrak{h}_{\mathbb{Z}})$, is of weight $m\gamma_k$, and satisfies (i) and (ii) of Proposition (5.2).

We now prove the following strengthened version of Proposition (5.2).

Proposition 5.6. *Assume $\mathfrak{g}$ to be simple. Fix $\gamma \in \Delta^+$ and $m > 0$. Let $s_0, \dots, s_v;\ \ \epsilon_0, \dots, \epsilon_v;$ and $\gamma_0, \dots, \gamma_{v+1}$ be as in the above section. Then there exists $\Theta_{\gamma,m} \in U(\mathfrak{n}_{\mathbb{Z}}^-)U(\mathfrak{h}_{\mathbb{Z}})$ of weight $-m\gamma$ such that*

(i) *$[e_\beta, \Theta_{\gamma,m}] \in U(\mathfrak{g})I_{\gamma,m} + U(\mathfrak{g})\mathfrak{n}^+$, for all $\beta \in \Delta^+$.*

(ii) *Write $\Theta_{\gamma,m}$ in terms of any PBW basis for $U(\mathfrak{n}^-)$:*

$$\Theta_{\gamma,m} = f_\gamma^m \otimes a_\gamma + \sum_{f^J \neq f_\gamma^m} f^J \otimes a_J,$$

where $a_\gamma, a_J \in U(\mathfrak{h}_{\mathbb{Z}})$. Then $a_\gamma \in U(\mathfrak{h}_{\mathbb{Z}})$ is of degree $m\sum_{\ell=0}^v r_\ell$ and its top homogeneous component is

$$\pm \prod_{0 \le \ell \le v} (H_{s_0 \dots s_{\ell-1}\epsilon_\ell})^{mr_\ell},$$

with only one exception when $\mathfrak{g} = G_2$ and $\gamma = 2\alpha_1 + \alpha_2$. In this case it is $\pm H_1^m (H_1 + H_2)^m$ (cf. §6 for the notation).
Moreover, $\deg(f^J \otimes a_J) \le \deg(f_\gamma^m \otimes a_\gamma) = m(1 + \sum_{\ell=0}^v r_\ell) = \sum_i ml_i$, where l_i is as in Proposition (5.2).

Proof. Note that $\gamma_k = \gamma_{v+1} + \sum_{k \le \ell \le v} r_\ell \epsilon_\ell$. Hence, by Proposition 5.2, $\deg \Theta_k = m(1 + \sum_{k \le \ell \le v} r_\ell)$. We prove the proposition under the assumption that $\mathfrak{g} \neq G_2$, in particular by Lemma (5.4), $\gamma_{\ell+1} - \epsilon_\ell \notin \Delta^+$ for any $0 \le \ell \le v$. (The next section will be devoted to handling the case $\mathfrak{g} = G_2$.)

Fix $\beta \in \Delta^+$ and $m \ge 1$. For any $a \neq 0 \in U(\mathfrak{n}^-) \otimes U(\mathfrak{h})$, write $a = f_\beta^m \otimes b_\beta + \sum_{f^J \neq f_\beta^m} f^J \otimes b_J$, where $b_\beta, b_J \in U(\mathfrak{h})$. Let us denote the top homogeneous component of b_β by $[a]^0_{f_\beta^m}$, if $\deg(f_\beta^m \otimes b_\beta) = \deg a$. If $\deg(f_\beta^m \otimes b_\beta) < \deg a$, we set $[a]^0_{f_\beta^m} = 0$.

Assume, by induction, that

$$[\Theta_{k+1}]^0_{f^m_{\gamma_{k+1}}} = \pm \prod_{k+1 \le \ell \le v} (H_{s_{k+1} \dots s_{\ell-1}\epsilon_\ell})^{mr_\ell}, \tag{1}$$

and prove (1) for Θ_k.

Since $\Theta_{v+1} = f^m_{\gamma_{v+1}}$, (1) is trivially true in this case. Write

$$\Theta_{k+1} = \pm f^m_{\gamma_{k+1}} \otimes \prod_{k+1 \le \ell \le v} (H_{s_{k+1} \dots s_{\ell-1}}\epsilon_\ell)^{mr_\ell} + \sum f^t \otimes a_t \tag{2}$$
$$+ \text{ lower degree terms},$$

for $a_t \in U(\mathfrak{h}_{\mathbb{Z}})$; where the summation is taken over $t \in \mathcal{P}(m\gamma_{k+1})$ subject to $f^t \neq f^m_{\gamma_{k+1}}$, and $\deg(f^t a_t) = \deg \Theta_{k+1}$. Set

(3)

$$z_j = \left[\left(\frac{(\operatorname{ad} f_{\epsilon_k})^j}{j!} f^m_{\gamma_{k+1}}\right) f_{\epsilon_k}^{mr_k - j}\right]^+_{\epsilon_k} (-H_{\epsilon_k})^j \left(\prod_{k+1 \le \ell \le v} H_{s_k \cdots s_{\ell-1}\epsilon_\ell}\right)^{mr_\ell}$$

and

(4)
$$z_j^t = \left[\left(\frac{(\mathrm{ad}\, f_{\epsilon_k})^j}{j!} f^t\right) f_{\epsilon_k}^{mr_k - j}\right]_{\epsilon_k}^+ \tilde{s}_k(p_t)(-H_{\epsilon_k})^j.$$

Since ad and $\tilde{s}_k$ both preserve degrees, it follows that $\deg z_j \leq \deg \Theta_{k+1} + mr_k = \deg \Theta_k$ and similarly $\deg z_j^t \leq \deg \Theta_k$. Set $S_1 = \{j \geq 0;\ \deg z_j = \deg \Theta_k\}$ and $S_2 = \{(j,t);\ j \geq 0,\ t \in \mathcal{P}(m\gamma_{k+1}),\ f^t \neq f_{\gamma_{k+1}}^m$, and $\deg z_j^t = \deg \Theta_k\}$. Then (2) of §5.5 and (2) imply that

$$\Theta_k = \pm \sum_{j \in S_1} z_j + \sum_{(j,t) \in S_2} z_j^t + \text{ lower degree terms.} \tag{5}$$

Since $\gamma_{k+1} - \epsilon_k \notin \Delta^+$, by the proof of Lemma (5.4) and (1) of §5.5, it follows that $\gamma_k + \epsilon_k \notin \Delta^+$ and so $(\mathrm{ad}\ f_{\epsilon_k})^{r_k+1} f_{\gamma_{k+1}} = 0$. Therefore $z_j = 0$ for $j > mr_k$. Furthermore, by Lemmas (4.3) and (5.4), we have

$$\frac{(\mathrm{ad}\, f_{\epsilon_k})^{mr_k}}{(mr_k)!} f_{\gamma_{k+1}}^m = \pm f_{\gamma_k}^m.$$

On the other hand $j < mr_k$ implies that $z_j \in U(\mathfrak{n}^-) f_{\epsilon_k} U(\mathfrak{h})$, and so $[z_j]^0_{f^m_{\gamma_k}} = 0$ (when $j < mr_k$). Let us abbreviate $[a]^0_{f^m_{\gamma_k}}$ by $[a]^0$ till the end of this proof. Therefore

$$\sum_{j \in S_1} [z_j]^0 = [z_{mr_k}]^0 = \pm \prod_{k \leq \ell \leq v} (H_{s_k \dots s_{\ell-1}\epsilon_\ell})^{mr_\ell}.$$

To complete the proof, we argue that for any $(j,t) \in S_2$ we have $[z_j^t]^0 = 0$. We have

$$\deg\left(\left[\left(\frac{(\mathrm{ad}\, f_{\epsilon_k})^j}{j!} f^t\right) f_{\epsilon_k}^{mr_k - j}\right]_{\epsilon_k}^+\right) = \deg f^t + mr_k - j. \tag{6}$$

Now by (4),

$$[z_j^t]^0 = \left[\left[\left(\frac{(\mathrm{ad}\, f_{\epsilon_k})^j}{j!} f^t\right) \cdot f_{\epsilon_k}^{mr_k - j}\right]_{\epsilon_k}^+\right]^0 (-H_{\epsilon_k})^j \tilde{s}_k(p_t). \tag{7}$$

Assume, if possible, $[z_j^t]^0 \neq 0$. Then (7) implies that

$$\left[\left[((\mathrm{ad}\ f_{\epsilon_k})^j f^t)\, f_{\epsilon_k}^{mr_k - j}\right]_{\epsilon_k}^+\right]^0 \neq 0. \tag{8}$$

Hence by (6), we have

$$\deg f^t + mr_k - j = \deg(f_{\gamma_k}^m) = m. \tag{9}$$

Let $t = (t_1, \dots, t_N)$. Then

$$f^t = f_{\beta_N}^{t_N} \cdots f_{\beta_2}^{t_2} f_{\epsilon_k}^{t_1} = f_{\lambda_1} \cdots f_{\lambda_s} f_{\epsilon_k}^{t_1},$$

where $\lambda_1 = \lambda_2 = \cdots = \lambda_{t_N} = \beta_N, \lambda_{t_{N+1}} = \cdots = \lambda_{t_N + t_{N-1}} = \beta_{N-1}, \dots,$ $\lambda_{t_N + \cdots + t_3 + 1} = \cdots = \lambda_{t_N + \cdots + t_2} = \beta_2$. In particular, let $s = t_2 + t_3 + \cdots + t_N$. By (8) (since $\epsilon_k \neq \gamma_{k+1}$), we must have $t_1 = j - mr_k$. This forces (by (9))

$$s = \deg f^t - (j - mr_k) = m. \tag{10}$$

Furthermore, $\left[\frac{(\operatorname{ad} f_{\epsilon_k})^j}{j!} f_{\lambda_1} \dots f_{\lambda_s}\right]^0 \neq 0$. So there exist non-negative integers $c_1, \dots, c_s$ such that $\lambda_l + c_l \epsilon_k = \gamma_k$ and $\sum_{l=1}^s c_l = j$. Since $j \geq mr_k$ and $\gamma_{k+1} - \epsilon_k$ is not a positive root, it follows that $\lambda_1 = \cdots = \lambda_s = \gamma_{k+1},\ j = mr_k$ and $c_1 = \cdots = c_s = r_k$, i.e., $f^t = f_{\gamma_{k+1}}^m$. But, by the definition of S_2, $f^t \neq f_{\gamma_{k+1}}^m$. This contradiction shows that $[z_j^t]^0 = 0$.

This completes the proof of the proposition for any $\mathfrak{g} \neq G_2$. (The case of G_2 will be handled in the next section.) □

6. Proof of Proposition (5.6) for $\mathfrak{g}$ of type G_2.

Throughout this section, we assume that $\mathfrak{g}$ is of type G_2.

Let α_1, α_2 be the positive simple roots with

$$(\alpha_1, \alpha_2) = -3, \qquad (\alpha_1, \alpha_1) = 2, \qquad (\alpha_2, \alpha_2) = 6.$$

Then $\Delta^+ = \{\alpha_1, \alpha_2, \alpha_1 + \alpha_2, 2\alpha_1 + \alpha_2, 3\alpha_1 + \alpha_2, 3\alpha_1 + 2\alpha_2\}$. Let r_i be the reflection corresponding to α_i. Set $f_1 = f_{\alpha_1},\ f_2 = f_{\alpha_2},\ f_3 = f_{\alpha_1+\alpha_2},\ f_4 = f_{2\alpha_1+\alpha_2},\ f_5 = f_{3\alpha_1+\alpha_2},\ f_6 = f_{3\alpha_1+2\alpha_2},\ H_1 = H_{\alpha_1},$ *and* $H_2 = H_{\alpha_2}$. We can choose $f_k' s$ so that the following relations are satisfied.

$$\begin{aligned} f_3 &= [f_1, f_2], \\ f_4 &= \tfrac{1}{2}[f_1, [f_1, f_2]], \\ f_5 &= \tfrac{1}{6}[f_1, [f_1, [f_1, f_2]]], \text{ and} \\ f_6 &= \tfrac{1}{6}[f_2, [f_1, [f_1, [f_1, f_2]]]]. \end{aligned}$$

A straightforward checking shows that the only positive roots α, β for which the second possibility of Lemma (5.4) occurs is $\beta = 2\alpha_1 + \alpha_2$ and $\alpha = \alpha_1 + \alpha_2$ (and in this case, in the notation of Lemma 5.4, $\epsilon = \alpha_1$ and $r = 1$). Now $r_1\beta = \alpha$ and $r_2\alpha = \alpha_1$. In the notation of §5.5, take $v = 1$, $\gamma_2 = \alpha_1$, $s_0 = r_1$, and $s_1 = r_2$ (so that $\gamma_1 = \alpha$ and $\gamma_0 = \beta$). Fix $m > 0$, and let Θ_2, Θ_1, and Θ_0 be the associated elements in $U(\mathfrak{n}_{\mathbb{Z}}^-)U(\mathfrak{h}_{\mathbb{Z}})$ as in §5.5. In particular,

$$\Theta_2 = f_1^m \tag{1}$$

and

$$(2)\qquad \Theta_1 = \sum_{0\le j\le m} \left(\frac{(\operatorname{ad} f_2)^j}{j!} f_1^m\right) f_2^{m-j} \left(\prod_{1\le \ell\le j} (-H_2 + m - \ell)\right).$$

Note that $(\operatorname{ad} f_2)^j f_1^m = 0$, for $j > m$. By §5.5, Θ_2 (resp. Θ_1) is an element of weight $m\alpha_1$ (resp. $m\alpha$) and it satisfies the requirements of Proposition (5.6) for $\gamma = \alpha_1$ (resp. $\gamma = \alpha$). We now want to construct $\Theta_{\beta,m}$.

Define

$$(3)\qquad \overline{\Theta}_1 = \sum_{0\le j\le m} (-1)^j \binom{m}{j} f_3^j f_1^{m-j} f_2^{m-j} \left(\prod_{1\le \ell\le j} (-H_2 + m - \ell)\right).$$

Then by Lemma (4.3), Θ_1 and $\overline{\Theta}_1$ have the same highest degree terms. Write $\overline{\Theta}_1 = \sum_{t\in\mathcal{P}(m\alpha)} f^t p_t$, with $p_t \in U(\mathfrak{h}_{\mathbb{Z}})$, and following (2) of §5.5 set

$$(4)\quad \overline{\Theta}_0 = \sum_t \sum_{k\ge 0} \left[\left(\frac{(\operatorname{ad} f_1)^k}{k!} f^t\right) f_1^{m-k}\right]^+_{\alpha_1} \left(\prod_{1\le \ell\le k} (-H_1 + m - \ell)\right) \tilde{r}_1(p_t),$$

where the first sum runs over t in $\mathcal{P}(m\alpha)$. Then again Θ_0 and $\overline{\Theta}_0$ have the same highest degree terms. In particular,

$$[\Theta_0]^0_{f_4^m} = \left[\overline{\Theta}_0\right]^0_{f_4^m}.$$

We now compute $[\overline{\Theta}_0]^0_{f_4^m}$.

Note that $\deg(f_3^j f_1^{m-j} f_2^{m-j}(-H_2)^j) = 2m = \deg\Theta_1$. We have $\tilde{r}_1(H_2) = H_2 + H_1 + 1$. Hence by (3) and (4) we have

(5)

$$\overline{\Theta}_0 = \sum_{(k,j)\in S} (-1)^j \binom{m}{j} \left(\frac{(\operatorname{ad} f_1)^k}{k!} \left(f_3^j f_2^{m-j} f_1^{m-j}\right) f_1^{m-k} (-H_1)^k (-H_1 - H_2)^j\right)$$
$$+ \quad \text{lower degree terms,}$$

where

$$S = \{(k,j);\ 0 \le j \le m,\ k \ge 0,\ 2m \ge j + k\}.$$

So we must compute the coefficient of f_4^m in

$$X(k,j) := (\operatorname{ad} f_1)^k \left(f_3^j f_2^{m-j} f_1^{m-j}\right) f_1^{m-k} (-H_1)^k (-H_1 - H_2)^j,$$

for $(k, j) \in S$. If $2m - j - k > 0$, then $X(k, j) \in U(\mathfrak{n}_{\mathbb{Z}}^-)f_1$; and hence the coefficient of f_4^m in $X(k, j)$ is zero. So, we may assume that $2m - j - k = 0$, i.e., $j = 2m - k$. Since $m \geq j \geq 0$, we must have $m \leq k \leq 2m$. Clearly,

$$\text{(6)} \qquad \frac{(\operatorname{ad} f_1)^k}{k!}\left(f_3^{2m-k} f_2^{k-m} f_1^{k-m}\right) f_1^{m-k} = \frac{(\operatorname{ad} f_1)^k}{k!}\left(f_3^{2m-k} f_2^{k-m}\right).$$

By virtue of Lemma (4.3), it is easy to see that the coefficient of f_4^m in the expression (6) is equal to 2^{2m-k}. Hence

$$\begin{aligned}\left[\overline{\Theta}_0\right]^0_{f_4^m} &= \sum_{m \leq k \leq 2m} \left((-1)^{2m-k}\binom{m}{2m-k} 2^{2m-k}(-H_1)^k(-H_1 - H_2)^{2m-k}\right)\\ &= (-H_1)^m(H_1 + 2H_2)^m.\end{aligned}$$

This proves Proposition (5.6) for $\mathfrak{g} = G_2$, thereby finishing its proof for arbitrary $\mathfrak{g}$. □

7. Special elements in $\mathfrak{U}_{\mathcal{B}}$.

We are now ready to mimic the construction in Section 5 for the quantum case. Given $\beta = \sum m_i\alpha_i$, set $K_\beta = K_1^{m_1} \cdots K_n^{m_n}$ and $d_\beta = (\beta, \beta)/2$. For $\gamma \in \Delta^+$ and $m > 0$, define the ideal $I^q_{\gamma,m}$ in $\mathfrak{U}^0_{\mathcal{B}}$ by

$$I^q_{\gamma,m} = \mathfrak{U}^0_{\mathcal{B}} \cap \left(U_q^0\left(K_\gamma^2 - q^{2(m-(\rho,\check{\gamma}))d_\gamma}\right)\right)$$

where U_q^0 is the $\mathbb{Q}(q)$-subalgebra of $U_q(\mathfrak{g})$ as in §2. It is easy to see that

$$I^q_{\gamma,m} = \mathfrak{U}^0_{\mathcal{B}}\left(\frac{K_\gamma^2 - q^{2(m-(\rho,\check{\gamma}))d_\gamma}}{q^{d_\gamma} - q^{-d_\gamma}}\right).$$

A reflection $s \in W$ induces a $\mathcal{B}$-algebra automorphism $\tilde{s} = \tilde{s}_q$ of $\mathfrak{U}^0_{\mathcal{B}}$ defined as follows.

$$\tilde{s}(K_i) = q^{(\rho, s\alpha_i) - (\rho, \alpha_i)} K_{s\alpha_i}.$$

(Note that here we are using the assumption that $[a]!^{-1}_{q^{d_i}} \in \mathcal{B}$ for each $1 \leq i \leq n$.)

The following is a quantized version of Proposition (5.2).

Proposition 7.1. *For any $\gamma \in \Delta^+$ and $m \geq 1$, there exists $\Theta^q_{\gamma,m} \in \mathfrak{U}^-_{\mathcal{B}}\mathfrak{U}^0_{\mathcal{B}}$ of weight $-m\gamma$ satisfying*

(a) *Writing $\Theta^q_{\gamma,m} = \sum_{t \in \mathbb{Z}_+^N} F^t a_t$ with $a_t \in \mathfrak{U}^0_{\mathcal{B}}$, there exists $r \in \mathbb{Z}^n$ (not depending upon t) such that $a_t \in K^r U_q^{0,\text{even}}$,*

(b) $\Theta^q_{\gamma,m} \notin \mathfrak{U}^-_{\mathcal{B}} I^q_{\gamma,m}$,

(c) $[E_i, \Theta^q_{\gamma,m}] \in \mathfrak{U}^-_{\mathcal{B}} I^q_{\gamma,m} + \mathfrak{U}_{\mathcal{B}}\mathcal{I}(\mathfrak{U}^+_{\mathcal{B}})$, *for all* $1 \leq i \leq n$,

where $\mathcal{I}(\mathfrak{U}^+_{\mathcal{B}})$ *denotes the augmentation ideal of* $\mathfrak{U}^+_{\mathcal{B}}$, *and* $U_q^{0,\mathrm{even}} \subset U_q^0$ *is the* $\mathbb{Q}(q)$*-subalgebra generated by* $\{K_1^{\pm 2}, \dots, K_n^{\pm 2}\}$.

Definition 7.2. For any $\lambda \in \mathfrak{h}^*_{\mathbb{Z}}$, define the $\mathbb{Q}(q)$-algebra homomorphism $\hat{\lambda} : U_q^0 \to \mathbb{Q}(q)$ by $\hat{\lambda}(K_i) = q^{(\lambda,\alpha_i)}$.

The following lemma (which can be proved by a standard density type argument) will be needed in the proof of the above proposition.

Lemma 7.3. *Let* ϵ *be a simple root and let* $\gamma, \gamma_1 \in \Delta^+$ *be such that* $\gamma = \gamma_1 + r\epsilon$ *for some* $r \neq 0$. *Fix* $m \in \{1, 2, 3, \dots\}$ *and let* $a \in \mathfrak{U}^0_{\mathcal{B}}$ *be an element such that* $\widehat{\lambda - \rho}(a) = 0$ *for all* $\lambda \in L_{\gamma,m} \cap \mathfrak{h}^*_{\mathbb{Z}}$ *satisfying* $(\mathrm{sign}\ r)(\lambda, \check{\epsilon}) \ll 0$ *(where* $L_{\gamma,m}$ *is defined by* (1) *of Proposition* (5.2) *and* sign r *denotes the sign of* r*). Assume further that* $K^s a \in U_q^{0,\mathrm{even}}$*, for some* $s \in \mathbb{Z}^n$*. Then* $a \in I^q_{\gamma,m}$.

Proof of Proposition 7.1. The proof is very similar to the proof of Proposition 5.2. If $(\rho, \check{\gamma}) = 1$, then $\gamma = \alpha_i$ for some $1 \leq i \leq n$ and we may take $\Theta^q_{\gamma,m} = F_i^m$. So assume $(\rho, \check{\gamma}) > 1$. Let ϵ, γ_1, and r be as in the proof of Proposition 5.2, i.e., ϵ is a simple root such that $\gamma_1 := s_\epsilon \gamma$ belongs to Δ^+ and $(\rho, \check{\gamma}_1) < (\rho, \check{\gamma})$. Moreover $\gamma - \gamma_1 = r\epsilon$ where $r := (\gamma, \check{\epsilon}) > 0$. Recall the definition of B_ϵ from (2) of the proof of Propostion 5.2.

For $\lambda \in B_\epsilon$ we have the following inclusions of Verma modules for $U_q(\mathfrak{g})$ (where $\psi = s_\epsilon \lambda$).

$$(1) \qquad M\left(\widehat{\psi - \rho}\right) \supset M\left(\widehat{\lambda - \rho}\right) \supset M\left(\lambda - \widehat{m\gamma} - \rho\right)$$

$$(2) \qquad M\left(\widehat{\psi - \rho}\right) \supset M\left(\psi - \widehat{m\gamma_1} - \rho\right) \supset M\left(\lambda - \widehat{m\gamma} - \rho\right).$$

Let v be the highest weight generating vector for $M(\widehat{\psi - \rho})$.

By induction on $(\rho, \check{\gamma})$, there exists $\Theta^q_{\gamma_1,m} \in \mathfrak{U}^-_{\mathcal{B}}\mathfrak{U}^0_{\mathcal{B}}$ as in the proposition. Let $\{w_\phi\}$ be a $\mathcal{B}$-basis for the $-m\gamma_1$ weight space of $\mathfrak{U}^-_{\mathcal{B}}$. Write $m\gamma_1 = \sum m_i\alpha_i$ and set $m_\epsilon = m_{i_o}$ where $\epsilon = \alpha_{i_o}$. We can write

$$(3) \quad \Theta_{\gamma_1,m} = \sum_t w_\phi p_\phi = \sum_\phi \left(w_\phi K_1^{m_1} \cdots K_n^{m_n} K_\epsilon^{-m_\epsilon}\right) K_1^{-m_1} \cdots K_n^{-m_n} K_\epsilon^{m_\epsilon} p_\phi,$$

where $p_\phi \in \mathfrak{U}^0_{\mathcal{B}}$. For $\lambda \in B_\epsilon$

$$(4) \qquad F_\epsilon^{-(\lambda,\check{\epsilon})+mr} \sum_\phi w_\phi \left(\widehat{\psi - \rho}\right)(p_\phi)$$

applied to v is a highest weight generating vector for $M(\widehat{\lambda-\rho-m\gamma})$, or else is 0 (see [**L2**, Identity (a_2) on page 103]). It can be easily seen that $(\widehat{\psi-\rho})(a) = (\widehat{\lambda-\rho})(\tilde{s}_\epsilon a)$, for all $a \in U_q^0$. We use Lemma 4.2 to construct $\Theta^q_{\gamma,m}$.

Set $B = K_1^{m_1} \dots K_n^{m_n} K_\epsilon^{-m_\epsilon}$ and $l = mr - (\lambda, \check{\epsilon})$. By Lemma 4.2, and [**JL1**, Lemma 2.2]

(5)
$$\sum_\phi \left(F_\epsilon^l w_\phi B\right) B^{-1} \left(\widehat{\lambda-\rho}\right)(\tilde{s}_\epsilon p_\phi)$$
$$= \sum_\phi \sum_{0\le j\le l} \begin{bmatrix} l \\ j \end{bmatrix}_{q^{d_\epsilon}} q^{-(j^2-jl)d_\epsilon} \left((\text{ad } F_\epsilon^j)(w_\phi B)\right) F_\epsilon^{l-j} K_\epsilon^{-j} B^{-1} \left(\widehat{\lambda-\rho}\right)(\tilde{s}_\epsilon p_\phi).$$

By definition,

$$\frac{[l]!_{q^{d_\epsilon}}}{[l-j]!_{q^{d_\epsilon}}} = \prod_{t=l-j+1}^{l} \frac{q^{td_\epsilon} - q^{-td_\epsilon}}{q^{d_\epsilon} - q^{-d_\epsilon}}. \tag{6}$$

A straightforward computation shows that (6) equals $q^{(\lambda-\rho, j\epsilon)}(\widehat{\lambda-\rho})(C_j)$ where
$$C_j := \prod_{0\le s\le j-1} \frac{q^{(mr-1-s)d_\epsilon} K_\epsilon^{-2} - q^{-(mr-1-s)d_\epsilon}}{q^{d_\epsilon} - q^{-d_\epsilon}}.$$

Substituting C_j back into (5) and noting that $jl - j^2 + (\lambda-\rho, j\check{\epsilon}) = jmr - j - j^2$, we get that (5) equals

(7)
$$\sum_\phi \sum_{0\le j\le l} q^{(jmr-j-j^2)d_\epsilon} \left(\left(\text{ad } F_\epsilon^{(j)}\right)(w_\phi B)\right) F_\epsilon^{l-j} K_\epsilon^{-j} B^{-1} \left(\widehat{\lambda-\rho}\right)[C_j(\tilde{s}_\epsilon p_\phi)].$$

By Lemma 4.6, $(\text{ad } F_\epsilon^{(j)})(w_\phi B) \in \mathfrak{U}_{\mathcal{B}}^- B K_\epsilon^j$ and equals zero for $j \gg 0$. It follows that the above sum has the same number of terms for different choices of λ as long as $(-\lambda, \check{\epsilon}) \gg 0$. Note that $C_j(\tilde{s}_\epsilon p_\phi) \in \mathfrak{U}_{\mathcal{B}}^0$.

Set

$$\bar{\Theta}^q_{\gamma,m} = \sum_\phi \sum_{0\le j} q^{(-j^2+j+jmr)d_\epsilon} B(j,\phi) K_\epsilon^{-j} B^{-1} K_\epsilon^{2j-mr-2m_\epsilon} C_j(\tilde{s}_\epsilon p_\phi),$$

as an element of $\mathfrak{U}_{\mathcal{B}}[F_\epsilon^{-1}]$, where $B(j,\phi) = ((\text{ad } F_\epsilon^{(j)})(w_\phi B))F_\epsilon^{mr-j}$. Note that the definition of $\bar{\Theta}^q_{\gamma,m}$ differs from expression (7) in the powers of q and K_ϵ. We now show that $\bar{\Theta}^q_{\gamma,m}$ satisfies the following identity in the Verma module $M(\widehat{\psi-\rho})$ (for $\lambda \in B_\epsilon$ such that $(\lambda, \check{\epsilon}) << 0$).

$$q^{(mr+2m_\epsilon)d_\epsilon} F_\epsilon^{-(\lambda,\check{\epsilon})+mr} \Theta^q_{\gamma_1,m} v = \bar{\Theta}^q_{\gamma,m} F_\epsilon^{-(\lambda,\check{\epsilon})} v. \tag{8}$$

First of all, $\bar{\Theta}^q_{\gamma,m} F_\epsilon^{-(\lambda,\check{\epsilon})} v$ equals

$$(9)\qquad \sum_{\phi, 0\leq j} q^{(-j^2+j+jmr)d_\epsilon} B(j,\phi) B^{-1} K_\epsilon^{j-mr-2m_\epsilon} F_\epsilon^{-(\lambda,\check{\epsilon})} \left(\widehat{\lambda-\rho}\right)(C_j \tilde{s}_\epsilon(p_\phi))v.$$

We show that

$$(10)\qquad B^{-1} K_\epsilon^{j-mr-2m_\epsilon} F_\epsilon^{-(\lambda,\check{\epsilon})} v = q^{(mr+2m_\epsilon-2j)d_\epsilon} F_\epsilon^{-(\lambda,\check{\epsilon})} K_\epsilon^{-j} B^{-1} v.$$

Since $F_\epsilon^{-(\lambda,\check{\epsilon})} v$ has weight $\lambda-\rho$, the left hand side of (10) is equal to $q^s F_\epsilon^{-(\lambda,\check{\epsilon})} v$, where

$$\begin{aligned} s &= (\lambda-\rho, -m\gamma_1 + m_\epsilon \epsilon) + (\lambda-\rho,\epsilon)(j-mr-2m_\epsilon) \\ &= (\lambda-\rho,-m\gamma_1) + d_\epsilon(\lambda,\check{\epsilon})(j-mr-m_\epsilon) - d_\epsilon(j-mr-m_\epsilon). \end{aligned}$$

Now since v has weight $\psi-\rho$ and $\psi = s_\epsilon\lambda = \lambda - (\lambda,\check{\epsilon})\epsilon$, the right hand side of (10) equals $q^{s'} F_\epsilon^{-(\lambda,\check{\epsilon})} v$ where

$$\begin{aligned} s' &= (\lambda-(\lambda,\check{\epsilon})\epsilon-\rho, -m\gamma_1 + (m_\epsilon - j)\epsilon) + d_\epsilon(mr+2m_\epsilon-2j) \\ &= (\lambda-\rho,-m\gamma_1) - mrd_\epsilon(\lambda,\check{\epsilon}) - d_\epsilon(m_\epsilon-j)(\lambda,\check{\epsilon}) - d_\epsilon(j-mr-m_\epsilon). \end{aligned}$$

This proves Identity (10). Expression (9) and Identity (10) imply that $\bar{\Theta}^q_{\gamma,m} F_\epsilon^{-(\lambda,\check{\epsilon})} v$ equals

$$q^{d_\epsilon(mr+2m_\epsilon)} \sum_{\phi,j} q^{jd_\epsilon(mr-j-1)} B(j,\phi) F_\epsilon^{-(\lambda,\check{\epsilon})} K_\epsilon^{-j} B^{-1} \left(\widehat{\lambda-\rho}\right)(C_j \tilde{s}_\epsilon(p_\phi))v.$$

Identity (8) now follows from the fact that the left hand side of (8) is equal to the Expression (7) applied to $q^{d_\epsilon(mr+2m_\epsilon)}v$.

By Lemma 4.6, $B(j,\phi)K_\epsilon^{-j}B^{-1} \in \mathfrak{U}_{\mathcal{B}}^-[F_\epsilon^{-1}]$. Set

$$\Theta^q_{\gamma,m} = \sum_\phi \sum_{0\leq j} \left[q^{(-j^2+j+jmr)d_\epsilon} B(j,\phi) K_\epsilon^{-j} B^{-1}\right]_\epsilon^+ K_\epsilon^{2j-mr-2m_\epsilon} C_j(\tilde{s}_\epsilon p_\phi),$$

where the notation $[\;]_\epsilon^+$ is formally defined exactly as was done in the modular case (cf. the proof of Proposition 5.2).

The same argument used in the proof of Proposition 5.2 shows that for $\lambda \in B_\epsilon$ with $(\lambda,\check{\epsilon}) \ll 0$,

$$(11)\qquad \Theta^q_{\gamma,m} F_\epsilon^{-(\lambda,\check{\epsilon})} v = \bar{\Theta}^q_{\gamma,m} F_\epsilon^{-(\lambda,\check{\epsilon})} v.$$

The assertion (a) is easy to prove in view of the explicit construction of $\Theta^q_{\gamma,m}$. We now show that $\Theta^q_{\gamma,m}$ satisfies assertion (c) of the proposition. By (8),

$$(12)\qquad E_i \bar{\Theta}^q_{\gamma,m} F_\epsilon^{-(\lambda,\check{\epsilon})} v = 0,$$

for all i. Hence Identities (11) and (12) imply that $E_i\Theta^q_{\gamma,m}F_\epsilon^{-(\lambda,\check{\epsilon})}v = 0 = E_iF_\epsilon^{-(\lambda,\check{\epsilon})}v$, for all i. Therefore, $[E_i,\Theta^q_{\gamma,m}]F_\epsilon^{-(\lambda,\check{\epsilon})}v = 0$ for all i. Write $[E_i,\Theta^q_{\gamma,m}] = a + \sum_t F^t a_t$ for some $a_t \in \mathfrak{U}^0_{\mathcal{B}}$ and $a \in \mathfrak{U}^-_{\mathcal{B}}\mathfrak{U}^0_{\mathcal{B}}\mathcal{I}(\mathfrak{U}^+_{\mathcal{B}})$. Then, we get $\sum_t F^t a_t F_\epsilon^{-(\lambda,\check{\epsilon})}v = 0$. This implies that $\sum_t F^t F_\epsilon^{-(\lambda,\check{\epsilon})}(\widehat{\lambda-\rho})(a_t)v = 0$. Thus $(\widehat{\lambda-\rho})(a_t) = 0$ for all t and for all $\lambda \in B_\epsilon$ such that $(\lambda,\check{\epsilon}) \ll 0$. Hence (c) follows from Lemma 7.3.

To see that $\Theta^q_{\gamma,m}$ satisfies assertion (b) of the proposition, recall that (cf. (3))

$$\Theta^q_{\gamma_1,m} = \sum w_\phi p_\phi.$$

Write

$$\Theta^q_{\gamma,m} = \sum_t F^t b_t,$$

for some (unique) $b_t \in \mathfrak{U}^0_{\mathcal{B}}$. Rewriting (8) (in view of (11)), we get

$$\begin{aligned}(13)\quad q^{(mr+2m_\epsilon)d_\epsilon}F_\epsilon^{-(\lambda,\check{\epsilon})+mr}\sum_\phi w_\phi\left(\widehat{\psi-\rho}\right)(p_\phi)v \\ = \sum_t F^tF_\epsilon^{-(\lambda,\check{\epsilon})}\left(\widehat{\lambda-\rho}\right)(b_t)v.\end{aligned}$$

Now by Lemma 7.3 and induction, there exists $\lambda \in B_\epsilon$ with $(\lambda,\check{\epsilon}) \ll 0$ such that $(\widehat{\psi-\rho})(p_\phi) \neq 0$ for some ϕ. This gives that the left hand side of (13) is non-zero, in particular, there exists a t_0 such that $(\widehat{\lambda-\rho})(b_{t_0}) \neq 0$. This forces $b_{t_0} \notin I^q_{\gamma,m}$. This proves assertion (b), thus completing the proof of Proposition 7.1. □

Definition 7.5 (A particular choice of $\Theta^q_{\gamma,m}$). We now use the above inductive construction to make a particular choice for $\Theta^q_{\gamma,m}$ (following the modular case as in §5.5). Fix $\gamma \in \Delta^+$ and $m > 0$. Let $s_k, \epsilon_k, \gamma_k, \gamma_{v+1}, r_k$; $0 \leq k \leq v$ be as in §5.5. Define elements Θ^q_k, $0 \leq k \leq v+1$, in $\mathfrak{U}^-_{\mathcal{B}}\mathfrak{U}^0_{\mathcal{B}}$ inductively as follows. Set $\Theta^q_{v+1} = F^m_{\gamma_{v+1}}$. Assume that we have defined Θ^q_{k+1} of weight $m\gamma_{k+1}$. Write $\Theta^q_{k+1} = \sum_{t\in\mathcal{P}(m\gamma_{k+1})} F^tp_t$, for $p_t \in \mathfrak{U}^0_{\mathcal{B}}$.

Write $m\gamma_{k+1} = \sum m_{k+1,i}\alpha_i$ and set $B(k) = K_1^{m_1}\cdots K_n^{m_n}K_s^{-m_s}$ where $m_i := m_{k+1,i}$ and α_s is the simple root such that $\epsilon_k = \alpha_s$. For any $j \geq 0$, let

$$C(k,j) = K_{\epsilon_k}^{j-mr_k-2m_s}\prod_{0\leq l\leq j-1}\frac{q^{(mr_k-l-1)d_{\epsilon_k}}K_{\epsilon_k}^{-1} - q^{-(mr_k-l-1)d_{\epsilon_k}}K_{\epsilon_k}}{q^{d_{\epsilon_k}} - q^{-d_{\epsilon_k}}}.$$

Now define Θ^q_k to be

$$\sum_{t,j} q^{(-j^2+j+jmr_k)d_{\epsilon_k}}\left[\left(\mathrm{ad}\,F^{(j)}_{\epsilon_k}\right)(F^tB(k))F^{mr_k-j}_{\epsilon_k}K^{-j}_{\epsilon_k}B(k)^{-1}\right]^+_{\epsilon_k}C(k,j)\tilde{s}_{\epsilon_k}(p_t),$$

where t runs through the elements in $\mathcal{P}(m\gamma_{k+1})$, and j runs through the non-negative integers.

8. Highest degree term.

We compute the highest degree terms of $\det_\eta(s_p)$ and $\det_\eta(s_\xi)$. We consider the two cases separately since the arguments are different.

Lemma 8.1. *The highest degree term of* $\det_\eta(s_p)$ *is*

$$a_\eta \prod_{\beta\in\Delta^+} \prod_{p>m>0} H_\beta^{P(\eta,m\beta)},$$
$$\textit{where}\ \ a_\eta = \prod_{t=(t_1,\cdots,t_N)\in\mathcal{P}_{res}(\eta)} \prod_{1\le j\le N} t_j!$$

Proof. By [**S**, Lemma 4],

$$\det_\eta(s_p) = \left(\prod_{t\in\mathcal{P}_{\mathrm{res}}(\eta)} \mathfrak{H}_p\left(e^t f^t\right)\right) + \ \text{ lower degree terms in }\ U(\mathfrak{h}_p).$$

Further,

$$\mathfrak{H}_p\left(e^t f^t\right) = \left(\prod_{1\le j\le N} \mathfrak{H}_p\left(e_{\beta_j}^{t_j} f_{\beta_j}^{t_j}\right)\right) + \ \text{ lower degree terms,}$$

and by [**H1**, §26.2],

$$\mathfrak{H}_p\left(e_{\beta_j}^{t_j} f_{\beta_j}^{t_j}\right) = (t_j!)H_{\beta_j}^{t_j} + \ \text{ lower degree terms.}$$

Hence the highest degree term of $\det_\eta(s_p)$ is equal to

$$\prod_{t\in\mathcal{P}_{\mathrm{res}}(\eta)} \left(\prod_{1\le j\le N} (t_j!)H_{\beta_j}^{t_j}\right).$$

Hence, to prove the lemma, we must show that

$$(1) \qquad \prod_{t\in\mathcal{P}_{\mathrm{res}}(\eta)} \left(\prod_{1\le j\le N} H_{\beta_j}^{t_j}\right) = \prod_{\beta\in\Delta^+} \prod_{p>m>0} H_\beta^{P(\eta,m\beta)}.$$

Fix $1 \leq j \leq N$. The multiplicity of H_{β_j} in the left hand side of (1) is $\sum_{t \in \mathcal{P}_{\mathrm{res}}(\eta)} t_j$. We have

$$\begin{aligned}\sum_{t \in \mathcal{P}_{\mathrm{res}}(\eta)} t_j &= \sum_{m=1}^{p-1} m\#\{t \in \mathcal{P}_{\mathrm{res}}(\eta); t_j = m\} \\ &= \sum_{m=1}^{p-1} \#\{t \in \mathcal{P}_{\mathrm{res}}(\eta); t_j \geq m\} \\ &= \sum_{m=1}^{p-1} P(\eta, m\beta_j).\end{aligned}$$

Now $\sum_{m=1}^{p-1} P(\eta, m\beta_j)$ is precisely the multiplicity of H_{β_j} in the right hand side of (1). This proves (1), thereby proving the lemma. □

Recall the definition of K_η from Theorem (3.4).

Lemma 8.2. *For any $\eta \in Q^+, (K_\eta)^{P_{\mathrm{res}}(\eta)} \det_\eta(s_\xi) \in \mathbb{Q}_\xi[K_1, \ldots, K_n]$ and $(K_\eta)^{-P_{\mathrm{res}}(\eta)} \det_\eta(s_\xi) \in \mathbb{Q}_\xi[K_1^{-1}, \ldots, K_n^{-1}]$. Furthermore,*

$$(K_\eta)^{P_{\mathrm{res}}(\eta)} = \prod_{\beta \in \Delta^+} \prod_{p > m > 0} K_\beta^{P(\eta, m\beta)}. \tag{1}$$

Proof. Recall that $\mathfrak{H}_\xi(E_i F_j) = \delta_{ij}[K_i; 1]$(cf. Proposition 4.4 for the notation $[K_i; 1]$). Hence if a is an element in $\mathfrak{u}_\xi^+$ of weight η and b is an element of weight $-\eta$ in $\mathfrak{u}_\xi^-$, the highest possible degree term of $\mathfrak{H}_\xi(ab)$ is K_η and the lowest is K_η^{-1}. Since $det_\eta(s_\xi)$ is a sum of terms each a product of $P_{\mathrm{res}}(\eta)$ elements of the form $\mathfrak{H}_\xi(ab)$, the first assertion of the lemma follows.

Identity (1) follows by an argument as in the proof of Lemma (8.1). □

9. Factoring the Shapovalov determinant.

We are now ready to factor the Shapovalov determinants. The idea is to combine Lemmas (4.8), (8.1), (8.2), (9.1), and (9.4) to determine the factors and their multiplicities.

For $\gamma \in \Delta^+$ and $m > 0$, set $H_{\gamma,m} = H_\gamma + \rho(H_\gamma) - m \in U(\mathfrak{h}_p)$. We will also think of it sometimes as an element of $U(\mathfrak{h}_\mathbb{Z})$.

Lemma 9.1. *For each $\gamma \in \Delta^+$ and $0 < m < p$, there exists $b_{\gamma,m} \in \mathfrak{b}^-(\mathfrak{u}_p)$ (cf. §3.1) of weight $-m\gamma$ such that for each $\eta \in Q^+$ with $P(\eta, m\gamma) \neq 0$, we have*

(i) *the image of the set $\{f^t b_{\gamma,m}; t \in \mathcal{P}(\eta, m\gamma)\}$ in the right $U(\mathfrak{h}_p)/\langle H_{\gamma,m}\rangle$-module $\mathfrak{u}_p^- \otimes (U(\mathfrak{h}_p)/\langle H_{\gamma,m}\rangle)$ is linearly independent.*

(ii) $\mathfrak{H}_p(vf^tb_{\gamma,m}) \in U(\mathfrak{h}_p)H_{\gamma,m}$ *for all* $v \in \mathfrak{u}_p^+$ *of weight* η *and* $t \in \mathcal{P}(\eta, m\gamma)$.

Proof. Choose $\Theta_{\gamma,m}$ using Proposition (5.6), and set $b_{\gamma,m}$ equal to the image of $\Theta_{\gamma,m}$ in $\mathfrak{b}^-(\mathfrak{u}_p)$.

Introduce a new multi-degree function ℓ-degree on $\mathfrak{u}_p^- \otimes U(\mathfrak{h}_p)$ as follows. Choose an ordering of the positive roots $\{\beta_1, \dots, \beta_N\}$ as in (13) of §2 such that $\beta_1 = \gamma$. Define the lexicographic ordering on $\mathbb{Z}_+^{N+1}$ so that

$$(1, 0, \dots, 0) < (0, 1, 0, \dots, 0) < \cdots < (0, \dots, 0, 1).$$

For any $\sum f^t \otimes a_t \in \mathfrak{u}_p^- \otimes U(\mathfrak{h}_p)$, set

$$\ell\text{-deg} \sum_t f^t \otimes a_t = \max_{\{t=(t_1,\dots,t_N)\ \ a_t \neq 0\}} (t_N, \dots, t_1,\ \deg(f^t \otimes a_t)) \in \mathbb{Z}_+^{N+1}.$$

Note that if $\deg a < \deg b$ for $a, b \in \mathfrak{u}_p^- \otimes U(\mathfrak{h}_p)$, then ℓ-deg $a < \ell$-deg b.

By Propositions (5.6), we may write

$$b_{\gamma,m} = f_\gamma^m \otimes a_\gamma + \sum f^J \otimes a_J,$$

such that $|f^J \otimes a_J|_\ell < |f_\gamma^m \otimes a_\gamma|_\ell$, where $|\quad|_\ell$ denotes the ℓ-degree (use the fact that $a_J = 0$ unless $J \in \mathcal{P}(m\gamma)$).

Consider the following equation where $x_t \in U(\mathfrak{h}_p)$ and $b_\phi \in U(\mathfrak{h}_p)H_{\gamma,m}$:

$$(1) \qquad \sum_{t \in \mathcal{P}(\eta, m\gamma)} f^t b_{\gamma,m} x_t = \sum_{\phi \in \mathcal{P}_{res}(\eta)} f^\phi b_\phi.$$

If not all x_t are zero, pick t^o such that x_{t^o} is non-zero and moreover $|f^{t^o}x_{t^o}|_\ell > |f^t x_t|_\ell$, for any $t \neq t^o$ such that $x_t \neq 0$. Now $\sum f^t b_{\gamma,m} x_t = f^{t^o} f_\gamma^m a_\gamma x_{t^o} + \sum f^\phi y_\phi$ with $y_\phi \in U(\mathfrak{h}_p)$ and $|f^\phi y_\phi|_\ell < |f^{t^o} f_\gamma^m a_\gamma x_{t^o}|_\ell$ (as can easily be seen). In view of (1), this forces $a_\gamma x_{t^o} + v = b_{\phi^o}$ for some $v \in U(\mathfrak{h}_p)$ of degree strictly less than that of $a_\gamma x_{t^o}$, where ϕ^o is such that $f^{\phi^o} = f^{t^o} f_\gamma^m$. This implies that the highest degree component of $a_\gamma x_{t^o}$ equals the highest degree component of b_{ϕ^o}. But (by assumption) $H_{\gamma,m}$ divides b_{ϕ^o} and therefore H_γ divides the highest degree component of $a_\gamma x_{t^o}$. Recall from Proposition 5.6 that the top homogeneous component of a_γ is coprime to H_γ, and hence H_γ divides the highest degree component of x_{t^o}. Thus we can find $x' \in U(\mathfrak{h}_p)$ such that

$$(2) \qquad \deg(x_{t^o} - H_{\gamma,m} x') < \deg x_{t^o}.$$

We prove by induction on $\sum_t \deg x_t$ that if

$$\sum_{t \in \mathcal{P}(\eta, m\gamma)} f^t b_{\gamma,m} x_t \in \mathfrak{u}_p^- U(\mathfrak{h}_p) H_{\gamma,m},$$

then $x_t \in U(\mathfrak{h}_p)H_{\gamma,m}$, for all t:

Clearly,

$$\sum_{t \neq t^o \in \mathcal{P}(\eta, m\gamma)} f^t b_{\gamma,m} x_t + f^{t^o} b_{\gamma,m}(x_{t^o} - H_{\gamma,m} x') \in \mathfrak{u}_p^- U(\mathfrak{h}_p) H_{\gamma,m}.$$

Hence by the inductive hypothesis and (2), any $x_t \in U(\mathfrak{h}_p)H_{\gamma,m}$. This proves (i).

We now prove assertion (ii): For any $\beta \in \Delta^+$, writing $[e_\beta, \Theta_{\gamma,m}] \in U(\mathfrak{g}_\mathbb{Z})$, in terms of the PBW basis, we get

$$[e_\beta, \Theta_{\gamma,m}] \in \sum_t f^t p_t + U(\mathfrak{g}_\mathbb{Z})\mathfrak{n}_\mathbb{Z}^+$$

for some $p_t \in U(\mathfrak{h}_\mathbb{Z})$. By Proposition (5.2), we get that p_t is divisible by $H_{\gamma,m}$ in $S(\mathfrak{h}_\mathbb{Q})$, where $S(\mathfrak{h}_\mathbb{Q})$ is the symmetric algebra of $\mathfrak{h}_\mathbb{Q} := \mathfrak{h}_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Q}$. Write $p_t = H_{\gamma,m} p'_t$ where $p'_t \in S(\mathfrak{h}_\mathbb{Q})$. We can take an integral basis $\{h_1, \dots, h_l\}$ of $\mathfrak{h}_\mathbb{Z}$, which contains H_γ (say $h_l = H_\gamma$). Write $p'_t = d_t^{-1} p''_t$, where p''_t is a polynomial in $\{h_1, \dots, h_l\}$ with integral coefficients such that the greatest common divisor of the coefficients is 1 and d_t is a non-zero integer. Then $d_t p_t = H_{\gamma,m} p''_t$. Fix any t such that $p_t \neq 0$. Reducing mod any prime ℓ such that ℓ divides d_t, we get $0 = H_{\gamma,m} p''_t (\text{mod } \ell)$. But both of $H_{\gamma,m}$ and p''_t are non-zero considered as elements of $U(\mathfrak{h}_{\mathbf{F}_\ell})$. This is a contradiction. Hence $p'_t \in U(\mathfrak{h}_\mathbb{Z})$ and assertion (ii) follows. □

We will prove a quantum analog of the above lemma. The proof uses a certain 'specialization', which we explain.

Definition 9.2. Set

$$\bar{\mathcal{B}} = \mathcal{B}/\langle q - 1 \rangle.$$

(Note that $q - 1$ is not invertible in $\mathcal{B}$.) Then $\bar{\mathcal{B}} = \mathbb{Z}[(a!)^{-1}]$, where a is as in §2. A standard argument shows that (as $\bar{\mathcal{B}}$-algebras)

$$\bar{\mathcal{B}} \otimes_\mathcal{B} \mathfrak{U}_\mathcal{B} \cong \bar{\mathcal{B}}_K \otimes_{\bar{\mathcal{B}}} U(\mathfrak{g}_{\bar{\mathcal{B}}}), \tag{1}$$

where $\mathfrak{g}_{\bar{\mathcal{B}}} := \bar{\mathcal{B}} \otimes_\mathbb{Z} \mathfrak{g}_\mathbb{Z}$, $\bar{\mathcal{B}}_K := \bar{\mathcal{B}}[\bar{K}_1, \dots, \bar{K}_n]/\langle \bar{K}_1^2 - 1, \dots, \bar{K}_n^2 - 1\rangle$ is the quotient of the polynomial algebra $\bar{\mathcal{B}}[\bar{K}_1, \cdots, \bar{K}_n]$ in the variables $\bar{K}_1, \dots, \bar{K}_n$ by the ideal $\langle \bar{K}_1^2 - 1, \dots, \bar{K}_n^2 - 1\rangle$, and we put the tensor product algebra structure on the right side (in particular, $\bar{K}_i$ are central elements in this algebra). Moreover, under the isomorphism (1), K_i goes to $\bar{K}_i$. Clearly $\bar{\mathcal{B}}_K/\langle \bar{K}_1 - 1, \dots, \bar{K}_n - 1\rangle \cong \bar{\mathcal{B}}$, and hence we get

$$(\bar{\mathcal{B}} \otimes_\mathcal{B} \mathfrak{U}_\mathcal{B})/\langle K_1 - 1, \dots, K_n - 1\rangle \cong U(\mathfrak{g}_{\bar{\mathcal{B}}}). \tag{2}$$

We will refer to the above isomorphism (2) as the *specialization at* $q = 1$. One can show that $\frac{q^{md_i}K_i^{-1}-q^{-md_i}K_i}{q^{d_i}-q^{-d_i}}$ specializes to $-H_i+m$ (for any $1 \le i \le n$ and $m \in \mathbb{Z}$), while $\tilde{s}(a)$ specializes to $\tilde{s}$ of the specialization of a (for any reflection $s \in W$ and $a \in \mathfrak{U}^0_{\mathcal{B}}$). Also, for any $\beta \in \Delta^+$, E_β (resp. F_β) specializes to the corresponding root vector e_β (resp. f_β) in $U(\mathfrak{g}_{\bar{\mathcal{B}}})$. For any $\gamma \in \Delta^+$ and $m > 0$, from the explicit construction of Θ^q_k (resp. Θ_k) given in §7.5 (resp. §5.5), we see by induction that Θ^q_k specializes to Θ_k, for each $0 \le k \le v+1$.

Let $\mathcal{B}_\xi := \mathcal{B}/\langle \frac{q^p-1}{q-1} \rangle$ and define $\mathfrak{U}_{\mathcal{B}_\xi} = \mathcal{B}_\xi \otimes_{\mathcal{B}} \mathfrak{U}_{\mathcal{B}}$. Similarly define $\mathfrak{U}^0_{\mathcal{B}_\xi} = \mathcal{B}_\xi \otimes_{\mathcal{B}} \mathfrak{U}^0_{\mathcal{B}}$. By Proposition 4.4, $\mathfrak{U}^0_{\mathcal{B}_\xi}$ is a subalgebra of $\mathfrak{U}_{\mathcal{B}_\xi}$. Recall the definitions of $\mathfrak{U}_\xi$ and $\mathfrak{U}^0_\xi$ from (17) of §2, and note that $\mathfrak{U}_\xi \cong \mathbb{Q}_\xi \otimes_{\mathcal{B}_\xi} \mathfrak{U}_{\mathcal{B}_\xi}$ and $\mathfrak{U}^0_\xi \cong \mathbb{Q}_\xi \otimes_{\mathcal{B}_\xi} \mathfrak{U}^0_{\mathcal{B}_\xi}$ (where $\mathbb{Q}_\xi$ is $\mathcal{B}_\xi$-module under the injective ring homomorphism $\mathcal{B}_\xi \hookrightarrow \mathbb{Q}_\xi, q \mapsto \xi$).

There is a ring homomorphism $\bar{\theta} : \mathcal{B}_\xi \to \mathbf{F}_p$, taking $q \to 1$. We will refer to this homomorphism as *reduction* mod p. This induces a ring homomorphism $\theta : \mathfrak{U}_{\mathcal{B}_\xi} \to U(\mathfrak{g}_p)$ (analogous to (2)) taking each $K_i \mapsto 1$. In particular, on restriction, we get a ring homomorphism $\theta^0 : \mathfrak{U}^0_{\mathcal{B}_\xi} \to U(\mathfrak{h}_p)$.

By Proposition (4.4), we get $\mathfrak{U}^0_{\mathcal{B}_\xi} \hookrightarrow \mathbb{Q}_\xi \otimes_{\mathcal{B}_\xi} \mathfrak{U}^0_{\mathcal{B}_\xi} \cong \mathfrak{U}^0_\xi$. Let $\mathfrak{U}^{0,2}_\xi$ (resp. $\mathfrak{U}^{0,\text{even}}_\xi$) be the $\mathbb{Q}_\xi$-subalgebra of $\mathfrak{U}^0_\xi$ generated by $\{K_1^2, \dots, K_n^2\}$ (resp. $\{K_1^{\pm 2}, \dots, K_n^{\pm 2}\}$). Consider the $\mathcal{B}_\xi$-subalgebra $\mathfrak{U}^{0,2}_{\mathcal{B}_\xi} := \mathfrak{U}^0_{\mathcal{B}_\xi} \cap \mathfrak{U}^{0,2}_\xi$ of $\mathfrak{U}^0_{\mathcal{B}_\xi}$.

Lemma 9.3. *The algebra $\mathfrak{U}^{0,2}_{\mathcal{B}_\xi}$ is freely generated (as an algebra over $\mathcal{B}_\xi$) by the elements $\left\{ Z_i := \frac{K_i^2-1}{q^{d_i}-q^{-d_i}} \right\}_{1 \le i \le n}$.*

Proof. By Proposition (4.4)(b), the elements $\prod_{i=1}^n Z_i^{m_i}$ span $\mathfrak{U}^{0,2}_{\mathcal{B}_\xi}$ as a $\mathcal{B}_\xi$-module. Further, the image of $\prod_{i=1}^n Z_i^{m_i}$ in $U(\mathfrak{h}_p)$ under θ^0 is precisely $\prod_{i=1}^n H_i^{m_i}$. In particular, these elements are linearly independent over $\mathcal{B}_\xi$. (Use the fact that given any non-zero element $a \in \mathcal{B}_\xi$, there exists $r \in \mathbb{Z}_+$ such that $a = (q-1)^r b$ with $b \notin \ker\ \bar{\theta}$.) This proves the lemma. □

Recall the definition of $I^q_{\gamma,m}$ from §7. Let $\bar{I}^\xi_{\gamma,m}$ be the $\mathbb{Q}_\xi$-span of the image of $I^q_{\gamma,m}$ inside $\mathfrak{U}^0_\xi$ under the canonical map $\mathfrak{U}^0_{\mathcal{B}} \to \mathfrak{U}^0_\xi$. Set $\mathfrak{U}^{0,\text{even}}_{\mathcal{B}_\xi} = \mathfrak{U}^0_{\mathcal{B}_\xi} \cap \mathfrak{U}^{0,\text{even}}_\xi$. Note that $\mathfrak{U}^{0,\text{even}}_\xi \cong \mathbb{Q}_\xi \otimes_{\mathcal{B}_\xi} \mathfrak{U}^{0,\text{even}}_{\mathcal{B}_\xi}$ and $\mathfrak{U}^{0,2}_\xi \cong \mathbb{Q}_\xi \otimes_{\mathcal{B}_\xi} \mathfrak{U}^{0,2}_{\mathcal{B}_\xi}$.

Lemma 9.4. *For any $\gamma \in \Delta^+$ and $0 < m < p$, there exists $b^q_{\gamma,m} \in \mathfrak{b}^-_\xi$ of weight $-m\gamma$ such that for each $\eta \in Q^+$ with $P(\eta, m\gamma) \neq 0$, we have:*

(1) *The image of $\{F^t b^q_{\gamma,m};\ t \in \mathcal{P}(\eta, m\gamma)\}$ in $\mathfrak{u}^-_\xi \otimes (\mathfrak{U}^0_\xi/\bar{I}^\xi_{\gamma,m})$ is linearly independent over $\mathfrak{U}^{0,\text{even}}_\xi/(\mathfrak{U}^{0,\text{even}}_\xi \cap \bar{I}^\xi_{\gamma,m})$ (under right multiplication).*

(2) *$\mathfrak{H}_\xi(vF^t b^q_{\gamma,m}) \in \bar{I}^\xi_{\gamma,m}$, for any $v \in \mathfrak{u}^+_\xi$ of weight η and $t \in \mathcal{P}(\eta, m\gamma)$.*

Proof. Take for $b^q_{\gamma,m}$ the image of $\Theta^q_{\gamma,m}$ (as in Proposition 7.1) in $\mathfrak{b}^-_\xi$. Assertion (2) follows from Proposition 7.1(c). For assertion (1), note that

$\Theta^q_{\gamma,m}$ specializes to $\Theta_{\gamma,m}$ at $q = 1$ under the isomorphism (2) of Definition (9.2), and moreover $b_{\gamma,m}$ (of Lemma 9.1) is the image of $\Theta_{\gamma,m}$ in $\mathfrak{b}^-(\mathfrak{u}_p)$. Given a set $\{a_t;\ t \in \mathcal{P}(\eta, m\gamma)\}$ contained in $\mathfrak{U}_\xi^{0,\text{even}}$, we can choose $m \in \mathbb{Z}^n$ such that $(K^m)^2 a_t \in \mathfrak{U}_\xi^{0,2}$, for each $t \in \mathcal{P}(\eta, m\gamma)$. By Proposition 7.1(a), there exists $r \in \mathbb{Z}^n$ such that $b^q_{\gamma,m}K^r$ is contained in $\mathfrak{u}_\xi^- \mathfrak{U}_\xi^{0,2}$. Moreover, $\sum F^t b^q_{\gamma,m} a_t \in \mathfrak{u}_\xi^- \bar{I}^\xi_{\gamma,m}$ if and only if $\sum F^t b^q_{\gamma,m} K^r (K^m)^2 a_t \in \mathfrak{u}_\xi^- (\mathfrak{U}_\xi^{0,2} \cap \bar{I}^\xi_{\gamma,m})$. Thus, without loss of generality, we may assume that each a_t is in $\mathfrak{U}_\xi^{0,2}$. Multiplying by an appropriate element of $\mathbb{Q}_\xi$, we may further assume that every $a_t \in \mathfrak{U}_{\mathcal{B}_\xi}^{0,2}$ and moreover at least for one t^o, $\theta^0(a_{t^o}) \neq 0$ (as an element of $U(\mathfrak{h}_p)$), where θ^0 is as defined in §9.2. The lemma now follows by reduction mod p (using Lemma (9.1) and some arguments in its proof). □

Proof of Theorem (3.2). By our assumption on the prime p and Lemma (4.9), the factors $(H_\beta + \rho(H_\beta) - m)$ are relatively prime where β runs over the positive roots and $0 < m < p$. Hence Lemmas (4.8) and (9.1) imply that

$$(1)\qquad \prod_{\beta\in\Delta^+} \prod_{0<m<p} (H_\beta + \rho(H_\beta) - m)^{P(\eta, m\beta)}$$

divides $\det_\eta(s_p)$. A comparison of highest degree terms using Lemma (8.1) proves that (1) equals $\det_\eta(s_p)$ up to a non-zero scalar in $\mathbf{F}_p$. This proves Theorem (3.2). □

Proof of Theorem (3.4). It is easy to see that

$$(1)\qquad \theta^0(\det_\eta(s_\xi)) = \det_\eta(s_p).$$

In particular, $\det_\eta(s_\xi) \neq 0$.

Using Lemmas (4.8) and (9.4), it follows that $(K_\beta^2 - \xi^{2(m-(\rho,\check{\beta}))d_\beta})^{P(\eta,m\beta)}$ divides $\det_\eta(s_\xi)$, for each $\beta \in \Delta^+$, $0 < m < p$. (Actually we need a slight variant of Lemma 4.8, where we replace $\mathfrak{U}_\xi^0$ by $\mathfrak{U}_\xi^{0,\text{even}}$.) Observe that $K_\beta - \xi^{\ell d_\beta}$ and $K_\beta + \xi^{\ell d_\beta}$ are both irreducible as elements of $\mathfrak{U}_\xi^0$ (use the automorphisms $\tilde{s}$ as in the beginning of §7). By our restriction on the prime p, these factors are relatively prime to each other. Hence

$$(2)\qquad \prod_{\beta\in\Delta^+} \prod_{0<m<p} \left(K_\beta^2 - \xi^{2(m-(\rho,\check{\beta}))d_\beta}\right)^{P(\eta,m\beta)}$$

divides $\det_\eta(s_\xi)$ in $\mathfrak{U}_\xi^0$. Hence there exists $R \in \mathfrak{U}_\xi^0$ such that

$$\det_\eta(s_\xi) = (K_\eta)^{-P_{\text{res}}(\eta)} R \prod_{\beta\in\Delta^+} \prod_{0<m<p} \left(K_\beta^2 - \xi^{2(m-(\rho,\check{\beta}))d_\beta}\right)^{P(\eta,m\beta)}$$

$$= R \prod_{\beta \in \Delta^+} \prod_{0<m<p} \left(K_\beta - \xi^{2(m-(\rho,\check{\beta}))d_\beta} K_\beta^{-1} \right)^{P(\eta, m\beta)},$$

by (1) of Lemma 8.2.

Since the constant term of expression (2) is non-zero, by Lemma (8.2), it is easy to see that R is a (non-zero) constant. This proves the theorem. □

10. The Jantzen filtration and the Linkage principle.

One of the standard applications of the Shapovalov determinant is deriving the character-sum formula for the Jantzen filtration. In the modular and root of unity case, Andersen-Jantzen-Soergel [**AJS**, Proposition 6.6] determined this formula by different methods. In this section we derive this character-sum formula as an easy consequence of our Theorems (3.2) and (3.4). We first define the Jantzen filtration for the Verma modules of $\mathfrak{u}_p$ and $\mathfrak{u}_\xi$, which is fairly standard (and follows Jantzen's original construction).

Let us consider the polynomial algebras $R_\xi := \mathbb{Q}_\xi[S]$ and $R_p := \mathbf{F}_p[s]$ where S and s are indeterminates. Let D_ξ (resp. D_p) be the quotient field of R_ξ (resp. R_p). Recall the definition of the algebras $\mathfrak{u}_p$ and $\mathfrak{u}_\xi$ from §3 and let $\mathfrak{u}_{D_p}$ and $\mathfrak{u}_{R_p}$ (resp. $\mathfrak{u}_{D_\xi}$ and $\mathfrak{u}_{R_\xi}$) be obtained from them by extension of scalars from F_p (resp. $\mathbb{Q}_\xi$) to D_p and R_p (resp. D_ξ and R_ξ). Similarly, let $\mathfrak{b}(\mathfrak{u}_{D_p})$ (resp. $\mathfrak{b}_{D_\xi}$) be obtained from $\mathfrak{b}(\mathfrak{u}_p)$ (resp. $\mathfrak{b}_\xi$) by extending the scalars from $\mathbf{F}_p$ (resp. $\mathbb{Q}_\xi$) to D_p (resp. D_ξ).

For any fixed $\lambda \in \mathfrak{h}^*_{\mathbb{Z}}$, consider the one dimensional representation $S^\rho \xi^\lambda$ of $\mathfrak{b}_{D_\xi}$ defined by

$$\left(S^\rho \xi^\lambda\right)(K_i) = S^{(\rho,\alpha_i)} \xi^{(\lambda,\alpha_i)}$$

and

$$(S^\rho \xi^\lambda)(E_i) = 0, \quad \text{for any } \ 1 \leq i \leq n.$$

This gives rise to the Verma module

$$M_{D_\xi} = M_{D_\xi}(S^\rho \xi^\lambda) := \mathfrak{u}_{D_\xi} \otimes_{\mathfrak{b}_{D_\xi}} (S^\rho \xi^\lambda).$$

Similarly, define the one dimensional representation $\lambda + s\rho$ of $\mathfrak{b}(\mathfrak{u}_{D_p})$ by

$$(\lambda + s\rho)(H_i) = \lambda(H_i) + s \quad \text{and} \quad (\lambda + s\rho)(e_i) = 0,$$

and let $M_{D_p} = M_{D_p}(\lambda + s\rho)$ be the associated Verma module for the algebra $\mathfrak{u}_{D_p}$.

Following Jantzen [**J1**, §5], define the contravariant form $\mathcal{F}_\xi(\lambda)$ on M_{D_ξ} with values in D_ξ (resp. $\mathcal{F}_p(\lambda)$ on M_{D_p} with values in D_p) such that

$$\mathcal{F}_\xi(\lambda)(v_\xi, v_\xi) = \mathcal{F}_p(\lambda)(v_p, v_p) = 1,$$

where v_ξ (resp. v_p) is a highest weight vector in M_{D_ξ} (resp. M_{D_p}). The determinant formulas (Theorems 3.2 and 3.4) and the definition of the Coxeter number h of the Lie algebra $\mathfrak{g}$ (see, e.g., [**J2**, Part II, §6.2]) imply that both of these contravariant forms are non-degenerate for $p \geq h$. (In fact, $\mathcal{F}_\xi(\lambda)$ is non-degenerate for any prime p.) Define the Jantzen filtration $\{F_m(\xi^\lambda); m \geq 0\}$ of the Verma module $M(\xi^\lambda) := \mathfrak{u}_\xi \otimes_{\mathfrak{b}_\xi} (\xi^\lambda)$ as follows, where (ξ^λ) is the one dimensional representation of $\mathfrak{b}_\xi$ satisfying

$$(\xi^\lambda)(K_i) = \xi^{(\lambda,\alpha_i)} \quad \text{and} \quad (\xi^\lambda)(E_i) = 0.$$

First, let $M_{R_\xi} = M_{R_\xi}(S^\rho \xi^\lambda)$ be the $\mathfrak{u}_{R_\xi}$- submodule of M_{D_ξ} generated by the highest weight vector v_ξ, and define (for any $m \geq 0$)

$$M^m_{R_\xi} = \{v \in M_{R_\xi} : \mathcal{F}_\xi(\lambda)(v, M_{R_\xi}) \subset R_\xi(S-1)^m\}.$$

Identifying $M_{R_\xi} \otimes_{R_\xi} \mathbb{Q}_\xi$ with $M_{\mathbb{Q}_\xi}(\xi^\lambda)$ (where $R_\xi \to \mathbb{Q}_\xi$ is the $\mathbb{Q}_\xi$-algebra homomorphism which sends S to 1), we define $F_m(\xi^\lambda)$ as the image of $M^m_{R_\xi} \otimes_{R_\xi} \mathbb{Q}_\xi$ in $M_{\mathbb{Q}_\xi}(\xi^\lambda)$.

Using the homomorphism $R_p \to \mathbf{F}_p$ taking $s \mapsto 0$, we can similarly define the filtration $F_m(\lambda)$ of the Verma module $M_{F_p}(\lambda)$ corresponding to the algebra $\mathfrak{u}_p$.

As in the classical case, $M_{\mathbb{Q}_\xi}(\xi^\lambda)/F_1(\xi^\lambda)$ is an irreducible $\mathfrak{u}_\xi$-module. Similarly, $M_{\mathbf{F}_p}(\lambda)/F_1(\lambda)$ is an irreducible $\mathfrak{u}_p$-module.

We define the formal character ch of certain submodules of the Verma modules $M_{\mathbb{Q}_\xi}(\xi^\lambda)$ as an element of the group algebra $\mathbb{Z}[\mathfrak{h}^*_\mathbb{Z}]$ as follows. We first define the weight of the highest weight vector $v_o = 1 \otimes z \in M = M_{\mathbb{Q}_\xi}(\xi^\lambda)$ for $z \in (\xi^\lambda)$ as λ. Now a vector $v \in M$ is said to be of weight $\lambda - \eta$ if we can write $v = \sum a_t F^t v_o$, for some $a_t \in \mathbb{Q}_\xi$, where the summation runs over $t = (t_1, \ldots, t_N) \in \mathbb{Z}^N_+$ such that $\sum t_j \beta_j = \eta$. Define the $(\lambda - \eta)-$ *weight space* of M as

$$M_{\lambda-\eta} = \{v \in M : v \text{ is of weight } \lambda - \eta\}.$$

Then it is easy to see that $M = \oplus_{\eta \in R} M_{\lambda-\eta}$, where $R := \{\sum_{\beta\in\Delta^+} r_\beta \beta; 0 \leq r_\beta < p\} \subset Q^+$.

A submodule $N \subset M$ is said to be a weight module if $N = \oplus_{\eta\in R} N_{\lambda-\eta}$, where $N_{\lambda-\eta} := M_{\lambda-\eta} \cap N$. In this case we define its *formal character* ch $N \in \mathbb{Z}[\mathfrak{h}^*_\mathbb{Z}]$ by

$$\text{ch } N = \sum_\eta \text{ dim } N_{\lambda-\eta} e^{\lambda-\eta}.$$

An exactly parallel definition applies to $M_{\mathbf{F}_p}(\lambda)$ and its submodules. It is easy to see that $F_m(\xi^\lambda)$ (resp. $F_m(\lambda)$) are weight submodules of $M_{\mathbb{Q}_\xi}(\xi^\lambda)$ (resp. $M_{\mathbf{F}_p}(\lambda)$).

Given $\beta \in \Delta^+$, following [**AJS**] let $n_\beta = n_\beta(\lambda)$ be the integer congruent to $(\lambda+\rho)(H_\beta)$ mod p which satisfies $0 \leq n_\beta < p$. For $\lambda \in \mathfrak{h}^*_{\mathbb{Z}}$, define

$$R(\lambda) = \{\beta \in \Delta^+ : 0 < n_\beta < p\}.$$

We derive the following result due to Andersen-Jantzen-Soergel as an immediate consequence of our Theorems (3.2) and (3.4).

Theorem 10.1 ([**AJS**, Proposition 6.6])**.**
(a) *For any $\lambda \in \mathfrak{h}^*_{\mathbb{Z}}$, and $p \geq h$ (where h is the Coxeter number of $\mathfrak{g}$)*

$$\sum_{m>0} \text{ch } F_m(\lambda)$$
$$= \sum_{\beta\in R(\lambda)} \left(\sum_{m\geq 0} \text{ch}\, M_{\mathbf{F}_p}(\lambda - (mp+n_\beta)\beta) - \sum_{m>0} \text{ch}\, M_{\mathbf{F}_p}(\lambda - mp\beta) \right).$$

(b) *Similarly, for any $\lambda \in \mathfrak{h}^*_{\mathbb{Z}}$ and any odd prime p (we assume $p \neq 3$ if G_2 is a factor of $\mathfrak{g}$)*

$$\sum_{m>0} \text{ch } F_m(\xi^\lambda)$$
$$= \sum_{\beta\in R(\lambda)} \left(\sum_{m\geq 0} \text{ch } M_{\mathbb{Q}_\xi}(\xi^{\lambda-(mp+n_\beta)\beta}) - \sum_{m>0} \text{ch } M_{\mathbb{Q}_\xi}(\xi^{\lambda - mp\beta}) \right).$$

Proof. Using the argument in [**J1**, §5.3] and the factorization of the modular Shapovalov determinant (cf. Theorem 3.2), we get

$$\sum_{m>0} \text{ch } F_m(\lambda) = \sum_{\beta\in R(\lambda)} \sum_{\eta \in R} P(\eta, n_\beta \beta) e^{\lambda-\eta}.$$

Now for any $\beta \in R(\lambda)$,

$$\sum_{m\geq 0} \text{ch } M_{\mathbf{F}_p}(\lambda - (mp+n_\beta)\beta) - \sum_{m>0} \text{ch } M_{\mathbf{F}_p}(\lambda - mp\beta)$$
$$= \sum_{m\geq 0}\sum_{\eta\in R} P_{\text{res}}(\eta) e^{\lambda-(mp+n_\beta)\beta-\eta} - \sum_{m>0}\sum_{\eta\in R} P_{\text{res}}(\eta) e^{\lambda-mp\beta-\eta}$$
$$= \sum_{\eta\in Q} \left(\sum_{m\geq 0} P_{\text{res}}(\eta - mp\beta - n_\beta\beta) - P_{\text{res}}(\eta - (m+1)p\beta) \right) e^{\lambda-\eta}.$$

Thus, to prove the theorem, it suffices to show that for any $\beta \in R(\lambda)$,

$$\sum_{m\geq 0} P_{\mathrm{res}}(\eta - mp\beta - n_\beta\beta) - P_{\mathrm{res}}(\eta - (m+1)p\beta) = P(\eta, n_\beta\beta) : \tag{1}$$

Set (for any integers $s_1 < s_2$)

$$N_\beta(s_1, s_2) = \{t = (t_\gamma)_{\gamma\in\Delta^+} \in \mathbb{Z}_+^N;\ s_1 \leq t_\beta < s_2\}.$$

Then it is easy to see that the left hand side of (1) equals

$$\begin{aligned}\sum_{m\geq 0} &\#\left(\{t = (t_\gamma) \in \mathcal{P}(\eta)\,; 0 \leq t_\gamma < p \ \text{ for } \ \gamma \neq \beta\} \cap N_\beta(mp + n_\beta, (m+1)p)\right)\\ &+ \#\left(\{t = (t_\gamma);\ 0 \leq t_\gamma < p \ \text{ for } \ \gamma \neq \beta\} \cap N_\beta((m+1)p, (m+1)p + n_\beta)\right)\\ &- \#\left(\{t = (t_\gamma);\ 0 \leq t_\gamma < p \ \text{ for } \ \gamma \neq \beta\} \cap N_\beta((m+1)p, (m+1)p + n_\beta)\right)\\ &- \#\left(\{t = (t_\gamma);\ 0 \leq t_\gamma < p \ \text{ for } \ \gamma \neq \beta\} \cap N_\beta((m+1)p + n_\beta, (m+2)p)\right).\end{aligned}$$

Clearly, by virtue of cancellations, the above sum reduces to

$$\#\{t = (t_\gamma) \in \mathcal{P}(\eta);\ 0 \leq t_\gamma < p \ \text{ for } \ \gamma \neq \beta \ \text{ and } \ n_\beta \leq t_\beta < p\}. \tag{2}$$

Now (2) equals $P(\eta, n_\beta\beta)$ (by its definition; cf. (6) of §3.1). This proves (1) and hence the first part of the theorem follows. The second part follows by exactly the same argument (using Theorem 3.4). □

Remark. Even though we deduce the above character-sum formula from our factorization of the Shapovalov determinant (Theorems 3.2 and 3.4), Jantzen has pointed out to us that one could work backwards and deduce our Theorems (3.2) and (3.4) by using the character-sum formula as in [**AJS**] for "non-integral" weights.

Definition 10.2. Let $\lambda, \mu \in \mathfrak{h}_{\mathbb{Z}}^*$ be two weights. Then λ *is said to be strongly linked to* μ if there exist $\lambda_1 \leq \cdots \leq \lambda_r \in \mathfrak{h}_{\mathbb{Z}}^*; \beta_1, \ldots, \beta_{r-1} \in \Delta^+$ and $n_1, \ldots, n_{r-1} \in \mathbb{Z}$ such that

$$\lambda_1 = \lambda, \lambda_r = \mu \ \text{ and } \ \lambda_{j+1} = s_{\beta_j}(\lambda_j + \rho) - \rho + n_j p \beta_j, \ \text{ for all } \ 1 \leq j \leq r-1,$$

where s_{β_j} is the reflection throught the root β_j, and $\leq$ denotes the Bruhat partial order on $\mathfrak{h}_{\mathbb{Z}}^*$.

For $\lambda = \sum m_i\alpha_i \in Q^+$, let $|\lambda|$ denote the sum $\sum m_i$.

As in [**AJS**, §6], the following theorem can easily be deduced from Theorem 10.1. Recall that this result in the modular case (in fact for arbitrary p) was proved in general by Andersen [**A**], and in the quantum case by Andersen-Polo-Wen [**APW**].

Theorem 10.3. *Let $p \geq h$ be any odd prime* (*where h is the Coxeter number of $\mathfrak{g}$*)*. Then if $L_{\mathbf{F}_p}(\lambda)$ is a subquotient of $M_{\mathbf{F}_p}(\mu)$ as a $\mathfrak{u}_p$-module, then λ is strongly linked to μ, where $L_{\mathbf{F}_p}(\lambda)$ is the* (*unique*) *irreducible quotient of $M_{\mathbf{F}_p}(\lambda)$.*

Similarly, for any prime p as in (b) *of Theorem* (10.1)*, if $L_{\mathbb{Q}_\xi}(\lambda)$ is a subquotient of $M_{\mathbb{Q}_\xi}(\mu)$ as a $\mathfrak{u}_\xi$-module, then λ is strongly linked to μ.*

References

[A] H.H. Andersen, *The strong linkage principle*, J. Reine Angew Math., **315** (1980), 53-59.

[AJS] H.H. Andersen, J.C. Jantzen and W. Soergel, *Representations of quantum groups at a p-th root of unity and of semisimple groups in characteristic p: Independence of p*, Astérisque, **220** (1994), 1-321.

[APW] H.H. Andersen, P. Polo and K. Wen, *Representations of quantum algebras*, Invent. Math., **104** (1991), 1-59.

[BGG] I.N. Bernshtein, I.M. Gel'fand and S.I. Gel'fand, *Structure of representations generated by vectors of highest weight*, Funct. Anal. Appl., **5** (1971), 1-8.

[B] N. Bourbaki, *Groupes et algèbres de Lie*, Chap. IV-VI, Hermann, Paris, 1968.

[DK] C. DeConcini and V.G. Kac, *Representations of quantum groups at roots of* 1, In: Operator Algebras, Unitary Representations, Enveloping Algebras, and Invariant Theory, Progr. Math., **92** (1990), 471-506.

[F] J. Franklin, *Homomorphisms between Verma modules in characteristic p*, J. of Algebra, **112** (1988), 58-85.

[H1] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.

[H2] ———, *Ordinary and modular representations of Chevalley groups*, LNM, **528**, Springer-Verlag, 1976.

[J1] J.C. Jantzen, *Moduln mit einem höchsten Gewicht*, LNM, **750**, Springer-Verlag, Heidelberg, 1979.

[J2] ———, *Representations of Algebraic Groups*, Pure Appl. Math., **131**, Academic Press, 1987.

[JL1] A. Joseph and G. Letzter, *Local finiteness of the adjoint action for quantized enveloping algebras*, J. of Algebra, **153** (1992), 289-318.

[JL2] ———, *Rosso's form and quantized Kac Moody algebras*, preprint.

[K] S. Kumar, *Representations of quantum groups at roots of unity*, In : Proceedings of the conference on Quantum Topology, World Scientific Press, 1994.

[L1] G. Lusztig, *Finite dimensional Hopf algebras arising from quantized universal enveloping algebras*, J. Amer. Math. Soc., **3** (1990), 257-296.

[L2] ———, *Quantum groups at roots of* 1, Geometriae Dedicata, **35** (1990), 89-113.

[R] M. Rosso, *Groupes Quantiques, representations lineaires et applications*, Thesis, Paris 7, 1990.

[S] N.N. Shapovalov, *On a bilinear form on the universal enveloping algebra of a complex semisimple Lie algebra*, Funct. Anal. Appl., **6** (1972), 307-312.

Receive June 29, 1995. The first author was supported by the NSF grant no. DMS-9203660 and the second author was supported by a NSF postdoctoral fellowship.

University of North Carolina
Chapel Hill, NC 27599-3250
E-mail address: kumar@math.unc.edu

and

Massachusetts Institute of Technology
Cambridge, MA 02139