Abstract. We extend to the not necessarily simply laced case the study [8] of quantum groups whose parameter is a root of 1.

The universal enveloping algebra of a semisimple complex Lie algebra can be naturally deformed to a Hopf algebra over the formal power series over \(\mathbb{C}\) (Drinfeld) or over the field of rational functions over \(\mathbb{C}\) (Jimbo). This deformation is called a quantum algebra, or a quantum group. With some care, it can be regarded as a family of Hopf algebras defined for any complex parameter \(v\). The case where the parameter \(v\) is a root of 1 is particularly interesting since it is related with the theory of semisimple groups over fields of positive characteristic (see [8]) and (conjecturally, see [7]) with the representation theory of affine Lie algebras.

This case has been studied in [8] in the simply laced case; several results of [8] will be extended here to the general case. For example, we define a braid group action on the quantum algebra (not compatible with the comultiplication) and use it to construct suitable 'root vectors' and a basis.

Assuming that \(l\) is odd (and not divisible by 3, if there are factors \(G_2\)) we construct a surjective homomorphism of the quantum algebra in the ordinary enveloping algebra; this is a Hopf algebra homomorphism whose kernel is the two-sided ideal generated by the augmentation ideal of a remarkable finite dimensional Hopf subalgebra. (This construction appeared in [6] in the simply laced case, in relation with a 'tensor product theorem'.) Thus, the quantum algebra 'differs' from the ordinary enveloping algebra only by a finite dimensional Hopf algebra.

In this paper, we have generally omitted those proofs which do not differ essentially from the simply laced case, or those which involve only mechanical computations.

1. Notations

1.1. In this paper we assume, given an \(n \times n\) matrix with integer entries \(a_{ij}\) (\(1 \leq i, j \leq n\)) and a vector \((d_1, \ldots, d_n)\) with integer entries \(d_i \in \{1, 2, 3\}\) such

* Supported in part by National Science Foundation Grant DMS 8702842.
that the matrix \((d_id_{ij})\) is symmetric, positive definite, \(a_{ii} = 2\) and \(a_{ij} \leq 0\) for \(i \neq j\). (Thus \((a_{ij})\) is a Cartan matrix.)

Let \(v\) be an indeterminate and let \(\mathcal{A} = \mathbb{Z}[v, v^{-1}]\), with quotient field \(\mathbb{Q}(v)\). For \(h \in \mathbb{N}\), let \(\lfloor h \rfloor = (v^h - v^{-h})/(v - v^{-1})\).

Given integers \(N, M, d \geq 0\), we define, following Gauss,

\[
[N]_d = \prod_{h=1}^{N} \frac{v^{dh} - v^{-dh}}{v^d - v^{-d}} \in \mathcal{A}, \quad \left[ \begin{array}{c} M + N \\ N \end{array} \right]_d = \left[ \begin{array}{c} M + N \\ [M]_d [N]_d \end{array} \right] \in \mathcal{A}.
\]

(We omit the subscript \(d\) when \(d = 1\).) Following Drinfeld [2] and Jimbo [3] we consider the \(\mathbb{Q}(v)\)-algebra \(U\) defined by the generators \(E_i, F_i, K_i, K_i^{-1} (1 \leq i \leq n)\) and the relations

\[
\begin{align*}
(a1) & \quad K_iK_j = K_jK_i, \quad K_iK_i^{-1} = K_i^{-1}K_i = 1, \\
(a2) & \quad K_iE_j = v^{d_{ij}}E_jK_i, \quad K_iF_j = v^{-d_{ij}}F_jK_i, \\
(a3) & \quad E_iF_j = F_jE_i - \delta_{ij} \frac{K_i - K_i^{-1}}{v^{d_i} - v^{-d_i}}, \\
(a4) & \quad \sum_{r+s=1-a_{ij}} (-1)^s \begin{bmatrix} 1 - d_{ij} \\ s \end{bmatrix}_{d_i} E_i^r E_j^s F_i^s = 0 \quad \text{if } i \neq j, \\
(a5) & \quad \sum_{r+s=1-a_{ij}} (-1)^s \begin{bmatrix} 1 - d_{ij} \\ s \end{bmatrix}_{d_i} F_i^r F_j^s E_i^s = 0 \quad \text{if } i \neq j.
\end{align*}
\]

If \(E_i^{(N)}, F_i^{(N)}\) denote \(E_i^N, F_i^N\) divided by \([N]_d\), \(N \geq 0\) (cf. [5], [6]), we can rewrite (a4), (a5) in the form:

\[
\begin{align*}
\sum_{r+s=1-a_{ij}} (-1)^s E_i^{(r)} E_j E_i^{(s)} &= 0 \quad \text{if } i \neq j, \\
\sum_{r+s=1-a_{ij}} (-1)^s F_i^{(r)} F_j F_i^{(s)} &= 0 \quad \text{if } i \neq j.
\end{align*}
\]

\(U\) is a Hopf algebra with comultiplication \(\Delta\), antipode \(S\) and counit \(\varepsilon\) defined by

\[
\begin{align*}
(b) & \quad \Delta E_i = E_i \otimes 1 + K_i \otimes E_i, \quad \Delta F_i = F_i \otimes K_i^{-1} + 1 \otimes F_i, \\
& \quad \Delta K_i = K_i \otimes K_i, \\
(c1) & \quad S E_i = -K_i^{-1} E_i, \quad S F_i = -F_i K_i, \quad S K_i = K_i^{-1}, \\
(c2) & \quad \varepsilon E_i = \varepsilon F_i = 0, \quad \varepsilon K_i = 1.
\end{align*}
\]

By iterating \(\Delta\) we obtain as usual an algebra homomorphism \(\Delta^{(N)} : U \to U \otimes U^{(N)}\).
Let $\Omega, \Psi : U \to U^{\text{opp}}$ be the $\mathbb{Q}$-algebra homomorphisms defined by

(d1) $\Omega E_i = F_i, \quad \Omega F_i = E_i, \quad \Omega K_i = K_i^{-1}, \quad \Omega v = v^{-1},$

(d2) $\Psi E_i = E_i, \quad \Psi F_i = F_i, \quad \Psi K_i = K_i^{-1}, \quad \Psi v = v.$

1.2. Let $X$ (resp. $Y$) be the free abelian group with basis $\sigma_i$ (resp. $\tilde{\sigma}_i$), $1 \leq i \leq n$. Let $\langle \cdot, \cdot \rangle : Y \times X \to \mathbb{Z}$ be the bilinear pairing such that $\langle \tilde{\sigma}_i, \sigma_j \rangle = \delta_{ij}$ and let $\sigma_i \in X$ be defined by $\langle \sigma_i, \sigma_j \rangle = a_{ij}$. Define $s_i : X \to X, \quad s_i : Y \to Y$ by $s_i(x) = x - \langle \sigma_i, x \rangle \sigma_i, \quad s_i(y) = y - \langle y, \sigma_i \rangle \tilde{\sigma}_i$. We identify $\text{GL}(X) = \text{GL}(Y)$ using the pairing above and we let $W$ be its (finite) subgroup generated by $s_1, \ldots, s_n$. Let $\Pi$ be the set consisting of $\sigma_1, \ldots, \sigma_n$, let $R = W\Pi \subset X$ and let $R^+ = R \cap (N\sigma_1 + \cdots + N\sigma_n)$.

1.3. Let $U$ be the $\mathcal{A}$-subalgebra of $U$ generated by the elements

$$E_i^{(N)}(\sigma_i), F_i^{(N)}(\sigma_i), K_i, K_i^{-1} \quad (1 \leq i \leq n, N \geq 0).$$

We have

(a) $\Delta(E_i^{(N)}) = \sum_{b=0}^{N} v^{d_{i,b}(N-b)} E_i^{(N-b)} K_i^{b} \otimes E_i^{(b)},$

(b) $\Delta(F_i^{(N)}) = \sum_{a=0}^{N} v^{-d_{i,a}(N-a)} F_i^{(a)} K_i^{-a} \otimes F_i^{(N-a)}.$

1.4. Let $U^+$ (resp. $U^-$) be the subalgebra of $U$ generated by the elements $E_i$ (resp. $F_i$) for all $i$. Let $U^0$ be the subalgebra of $U$ generated by the elements $K_i, K_i^{-1}$ for all $i$.

Let $U^+(\text{resp. } U^-)$ be the $\mathcal{A}$-subalgebra of $U$ generated by the elements $E_i^{(N)}$ (resp. $F_i^{(N)}$) for $N \geq 0$ and all $i$.

1.5. We shall regard $\mathbb{Q}$ as a $\mathbb{Q}(v)$-algebra, with $v$ acting as 1. Tensoring $U, U^+, U^-, U^0$ with $\mathbb{Q}$ over $\mathbb{Q}(v)$ we obtain the $\mathbb{Q}$-algebras $U_\mathbb{Q}, U_+^\mathbb{Q}, U_-^\mathbb{Q}, U^0_\mathbb{Q}.$

Similarly, we regard $\mathbb{Z}$ and $\mathbb{F}_p$ (the field with $p$ elements) as $\mathcal{A}$-algebras, with $v$ acting as 1. Tensoring $U$ with $\mathbb{Z}$ (resp. $\mathbb{F}_p$) over $\mathcal{A}$, we obtain the ring $U_\mathbb{Z}$ (resp. the $\mathbb{F}_p$-algebra $U_{\mathbb{F}_p}$).

1.6. For any $j = (j_1, \ldots, j_n) \in \mathbb{N}^n$, let $U_j^+$ be the subspace of $U^+$ spanned by all monomials in $E_1, \ldots, E_n$ in which $E_i$ appears exactly $j_i$ times, for each $i$. We have clearly a direct sum decomposition $U^+ = \bigoplus_j U_j^+$.

We shall denote the subalgebra $U_0^0 U^+$ of $U$ by $U^+_{\geq 0}$. We have a direct sum decomposition $U_{\geq 0} = \bigoplus_j U_j^{\geq 0}$ where, by definition, $U_j^{\geq 0} = U_0^0 U_j^+.$
2. THE U-MODULE $M$

2.1. Let $M$ be the $\mathbb{Q}(v)$-vector space with basis $X_\alpha (\alpha \in R), t_i (1 \leq i \leq n)$. Define endomorphisms $E_i, F_i, K_i$ of $M$ by

$$E_i X_\alpha = [h] X_{\alpha + \varepsilon_i},$$
if $\alpha + \varepsilon_i \in R, \alpha \in R, \ldots, \alpha - (h - 1) \varepsilon_i \in R, \alpha - h \varepsilon_i \notin R$ ($h \geq 1$),

$$E_i X_{-\varepsilon_i} = t_i, \quad E_i X_\alpha = 0 \text{ for all other } \alpha \in R,$$

$$E_i t_i = (v^{d_i} + v^{-d_i}) X_{\varepsilon_i}, \quad E_i t_j = [-a_{ij}] X_{\varepsilon_i} \text{ if } i \neq j.$$

$$F_i X_\alpha = [h] X_{\alpha - \varepsilon_i},$$
if $\alpha - \varepsilon_i \in R, \alpha \in R, \ldots, \alpha + (h - 1) \varepsilon_i \in R, \alpha + h \varepsilon_i \notin R$ ($h \geq 1$),

$$F_i X_{-\varepsilon_i} = t_i, \quad F_i X_\alpha = 0 \text{ for all other } \alpha \in R,$$

$$F_i t_i = (v^{d_i} + v^{-d_i}) X_{-\varepsilon_i}, \quad F_i t_j = [-a_{ij}] X_{-\varepsilon_i} \text{ if } i \neq j,$$

$$K_i X_\alpha = v^{d_i(\varepsilon_i, \alpha)} X_\alpha, \quad K_i t_k = t_k.$$

PROPOSITION 2.2. The endomorphisms in 2.1 define a $U$-module structure on $M$ and a $U$-module structure on $M$, the $\mathcal{A}$-submodule of $M$ generated by the canonical basis of $M$. (Compare [7].)

2.3. Since $U$ is a Hopf algebra, the $U$-module structure on $M$ gives rise, in a standard way (using $\Delta^{(N)}$ in 1.1) to a $U$-module structure on $M \otimes^N$ for any $N \geq 0$. Moreover, using 1.3(a), (b), we see that $M \otimes^N$ is a $U$-submodule of $M \otimes^N$.

3. BRAID GROUP ACTION ON $U$

THEOREM 3.1. For any $i \in [1, n]$ there is a unique algebra automorphism $T_i$ of $U$ such that

$$T_i E_i = -F_i K_i,$$

$$T_i E_j = \sum_{r+s=-a_{ij}} (-1)^r v^{-d_{is}} E_i^{(r)} E_j E_i^{(s)} \text{ if } i \neq j,$$

$$T_i F_i = -K_i^{-1} E_i,$$

$$T_i F_j = \sum_{r+s=-a_{ij}} (-1)^r v^{d_{is}} F_i^{(r)} F_j F_i^{(s)} \text{ if } i \neq j,$$

$$T_i K_j = K_j K_i^{-a_{ij}}.$$

It commutes with $\Omega$ and its inverse is $T_i' = \Psi T_i \Psi$. 

THEOREM 3.2. Let \( w \in W \) and let \( s_{i_1} s_{i_2} \cdots s_{i_n} \) be a reduced expression of \( w \) in \( W \). Then the automorphism \( T_w = T_{i_1} T_{i_2} \cdots T_{i_n} \) of \( U \) depends only on \( w \) and not on the choice of reduced expression for it. Hence the \( T_i \) define a homomorphism of the braid group of \( W \) in the group of automorphisms of the algebra \( U \).

These results are proved by computations which will be omitted.

4. A BASIS OF \( U \)

4.1. According to [9], multiplication defines an isomorphism of \( \mathbb{Q}(v) \)-vector spaces

\[ U^- \otimes U^0 \otimes U^+ \cong U; \]

moreover, the monomials \( K^\varphi = \Pi_i K_{i^\varphi(i)} \) (with \( \varphi \) running over all functions \([1, n] \to \mathbb{Z}\)) form a basis for \( U^0 \).

Let us choose for each \( \beta \in R^+ \) an element \( w_\beta \in W \) such that for some index \( i_\beta \in [1, n] \) we have \( w_\beta^{-1}(\beta) = \alpha_{i_\beta} \). Let \( N^{R^+} \) be the set of all functions \( R^+ \to \mathbb{N} \). We fix a total order on \( R^+ \) and define for any \( \psi, \psi' \in N^{R^+} \):

\[ E^\psi = \prod_{\beta \in R^+} T_{w_\beta}(E^\psi(\beta)), \quad F^\psi = \Omega(E^\psi), \]

where the factors in \( E^\psi \) are written in the given order of \( R^+ \).

PROPOSITION 4.2. The elements \( E^\psi \) (resp. \( F^\psi \)) form a basis of the \( \mathbb{Q}(v) \)-vector space \( U^+ \) (resp. \( U^- \)). Hence the elements \( F^\psi K^\varphi E^\psi \) for various \( \psi, \psi', \varphi \) as above, form a basis of the \( \mathbb{Q}(v) \)-vector space \( U \).

4.3. In Section 7 we will construct an \( \mathcal{A} \)-basis of \( U \). For this we will need some particular (pre)orders on \( R^+ \).

A simple root \( \alpha \in \Pi \) is said to be special if the coefficient with which \( \alpha \) appears in any \( \beta \in R^+ \) (expressed as \( \mathbb{N} \)-linear combination of simple roots) is \( \leq 1 \). A simple root \( \alpha \in \Pi \) is said to be semispecial if the coefficient with which \( \alpha \) appears in any \( \beta \in R^+ \) is \( \leq 1 \), except for a single root \( \beta \), for which the coefficient is necessarily 2. If \( R \) is irreducible, then it has a unique semispecial simple root in types \( \neq A, C \), and none in types \( A, C \). Hence if \( n \geq 1 \), there is at least one simple root which is special or semispecial.

The numbering of the rows and columns of the Cartan matrix (or, equivalently, of \( \Pi \)) has been, so far, arbitrary. We say that this numbering is good if for any \( i \in [1, n] \), \( \alpha_i \) is special or semispecial when considered as a simple root of the root system \( R \cap (\mathbb{Z} \alpha_1 + \cdots + \mathbb{Z} \alpha_i) \). We can always choose a good numbering for the rows and columns of the Cartan matrix; we shall assume it fixed from now on.
For \( \beta \in R^+ \) we can write uniquely \( \beta = \sum_{j=1}^{l} c_j \alpha_j \) with \( c_j \geq 0 \), \( c_1 > 0 \). We then set \( g(\beta) = i, \ c_i = c_1. \) Let \( R_1^+ = \{ \beta \in R^+ \mid g(\beta) = i \}. \)

We define \( h' : R_1^+ \to \mathbb{Q} \) by \( h'(\beta) = c_{\beta^{-1}} \cdot \text{height}(\beta) \) (an integer or half of an odd integer). We define a preorder on \( R^+ \) as follows. If \( \alpha, \beta \in R^+ \), we say that \( \alpha \leq \beta \) if \( g(\alpha) \geq g(\beta) \) and \( h'(\alpha) \leq h'(\beta) \). The corresponding equivalence classes are called boxes.

One verifies that there is a unique function \( R^+ \to [1, n], (\beta \to i_\beta) \) such that the following three properties hold. First, \( s_i, s_j \) commute in \( W \) whenever \( \alpha, \beta \) are in the same box; hence, for any box \( B \), the product of all \( s_\alpha \) with \( \alpha \in B \) is a well defined element \( s(B) \in W \), independent of the order of factors. Second, we have \( i_\alpha = j. \) Finally, if \( \beta \in R_1^+ \) and \( B_1, \ldots, B_k \) are the boxes in \( R_1^+ \) preceding strictly \( \beta \), in increasing order (for \( \leq \)), then \( s(B_1) \cdots s(B_k)(x_\beta) = \beta \); we then set \( w_\beta = s(B_1) \cdots s(B_k). \)

If we now choose a total order on \( R^+ \) which refines the preorder above, then we may apply 4.2 to this order and to the functions \( i_\beta, w_\beta \) just defined and we obtain a basis of \( U \) which is independent of the choice of order; it depends only on the choice of good numbering. Note also that the function \( \beta \to w_\beta \) considered above does not coincide with that in [8, 3.5]; however, it leads to the same basis of \( U \) when both are defined.

5. **Integrality Properties in Rank 2**

5.1. In this section we assume that \( n = 2, a_{12} = \mu, \mu = 1, 2 \) or \( 3, a_{21} = -1. \) Then \( v = |R^+| = 3, 4 \) or 6. Consider the sequence consisting of the following \( v \) elements of \( U \):

\[
E_2, T_2(E_1), T_2T_1(E_2) \quad \text{if } \mu = 1, \\
E_2, T_2(E_1), T_2T_1(E_2), T_2T_1T_2(E_1) \quad \text{if } \mu = 2, \\
E_2, T_2(E_1), T_2T_1(E_2), T_2T_1T_2(E_1), \\
T_2T_1T_2T_1(E_2), T_2T_1T_2T_1T_2(E_1) \quad \text{if } \mu = 3.
\]

(The last term in the sequence is equal to \( E_1 \).) We shall also write the terms of this sequence in the following form \((a_\mu)\):

\[
(a1) \quad E_2, E_{12}, E_{12}, \\
(a2) \quad E_2, E_{12}, E_{112}, E_{12}, \\
(a3) \quad E_2, E_{12}, E_{112}, E_{12}, E_{112}, E_{1}.
\]

(The subscripts correspond to the various positive roots; for example, \( 1122 \) corresponds to \( 3\alpha_1 + 2\alpha_2 \). The order on \( R^+ \) suggested by the previous
sequence coincides with the preorder defined in 4.3.) We shall also need the divided powers $E^{(N)}$ of any term $E$ in the sequence $(a_μ)$ for $N ∈ N$; they are defined as $E^{d}/[N]_d$ where $d = d_1$ (resp. $d = d_2$) if $E$ is the second, fourth, ..., (resp. first, third, ...) term of the sequence.

5.2. The following commutation formulas are verified by direct computations. If $μ = 1$, we have

$$E_{12}E_2 = v^{-d}E_2E_{12}, \quad E_1E_{12} = v^{-d}E_{12}E_1,$$

$$E_1E_{2} = v^dE_2E_1 + v^dE_{12}$$

and $d = d_1 = d_2$. If $μ = 2$, we have

$$E_{12}E_2 = v^{-2}E_2E_{12}, \quad E_{112}E_{12} = v^{-2}E_{12}E_{112},$$
$$E_1E_{112} = v^{-2}E_{112}E_1,$$
$$E_{112}E_2 = E_2E_{112} + v(v^{-1} - v)E_{12}, \quad E_1E_{12} = E_{12}E_1 + [2]E_{112},$$
$$E_1E_2 = v^2E_2E_1 + v^2E_{12}.$$  

If $μ = 3$, we have

$$E_{12}E_2 = v^{-3}E_2E_{12}, \quad E_{1112}E_{12} = v^{-3}E_{12}E_{1112},$$
$$E_{112}E_{1112} = v^{-3}E_{1112}E_{112},$$
$$E_{1112}E_{112} = v^{-3}E_{112}E_{1112}, \quad E_1E_{112} = v^{-3}E_{112}E_1,$$
$$E_{1112}E_2 = v^{-3}E_2E_{1112} + (v^{-1} - v)(v^{-2} - v^2)E_{12}^{(3)},$$
$$E_{112}E_{12} = v^{-1}E_{12}E_{112} + v^{-1}[3]E_{1112},$$
$$E_{1112}E_{1112} = v^{-3}E_{1112}E_{1112} + (v^{-1} - v)(v^{-2} - v^2)E_{112}^{(3)},$$
$$E_1E_{112} = v^{-1}E_{112}E_1 + v^{-1}[3]E_{1112},$$
$$E_{112}E_2 = E_2E_{112} + v(v^{-2} - v^2)E_{12}^{(2)},$$
$$E_{1112}E_{12} = E_{12}E_{1112} + v(v^{-2} - v^2)E_{112}^{(2)},$$
$$E_1E_{112} = E_{112}E_1 + v(v^{-2} - v^2)E_{112}^{(2)},$$
$$E_{1112}E_2 = v^3E_2E_{1112} + (v^{-4} - v^2 + 1)E_{1112}$$
$$+ (v^2 - v^4)E_{12},$$
$$E_1E_{12} = vE_{12}E_1 + v[2]E_{112}, \quad E_1E_2 = v^3E_2E_1 + v^3E_{12}.$$  

5.3. The commutation formulas in 5.2 give rise, by induction, to commutation formulas between the generators of $U^+$. We shall make them explicit in
the case where \( \mu = 1 \) or 2. If \( \mu = 1 \), hence \( d_1 = d_2 = d \), we have:

(a) \[ E_1^{(r)} E_2^{(s)} = v^{-dr} E_2^{(s)} E_1^{(r)}, \]

(b) \[ E_1^{(r)} E_1^{(s)} = v^{-ds} E_1^{(s)} E_1^{(r)}, \]

(c) \[ E_1^{(r)} E_2^{(s)} = \sum_{r \geq 0, s \geq 0, r+s=k} v^{d(r+s)} E_2^{(r)} E_1^{(s)} E_1^{(r)}, \]

If \( \mu = 2 \), hence \( (d_1, d_2) = (1, 2) \), the relations are:

(d) \[ E_1^{(r)} E_2^{(s)} = v^{-2rs} E_1^{(s)} E_2^{(r)}, \]

(e) \[ E_1^{(r)} E_1^{(s)} = v^{-2rs} E_1^{(s)} E_1^{(r)}, \]

(f) \[ E_1^{(r)} E_2^{(s)} = v^{-2rs} E_1^{(s)} E_1^{(r)}, \]

(g) \[ E_1^{(r)} E_2^{(s)} = \sum_{r \geq 0, s \geq 0, r+s=k} v^{-2sr-2st+2s} \left( \prod_{i=1}^{s} \left( v^2 - 4i - 1 \right) \right) E_2^{(r)} E_1^{(s)} E_1^{(r)}, \]

(h) \[ E_1^{(r)} E_1^{(s)} = \sum_{r \geq 0, s \geq 0, r+s=k} v^{-sr-st+2s} \left( \prod_{i=1}^{s} \left( v^2 + 1 \right) \right) E_1^{(r)} E_1^{(s)} E_1^{(r)}, \]

(i) \[ E_1^{(r)} E_2^{(s)} = \sum_{r \geq 0, s \geq 0, r+s=k, r+s+t=k} v^{2ru+2rt+us+2s+2t} E_2^{(r)} E_1^{(s)} E_1^{(t)} E_1^{(u)}, \]

5.4. In the case where \( \mu = 3 \) we have the commutation formula:

(a1) \[ E_1^{(r)} E_2^{(s)} = \sum_{r \geq 0, s \geq 0, r+s=k} v^{f(p, q, r, s, t, u)} E_2^{(r)} E_1^{(s)} E_1^{(r)}, \]

where the sum is taken over the set

\[ \{(p, q, r, s, t, u) \in \mathbb{N}^6 \mid p + q + 2r + s + t = k', q + 3r + 2s + 3t + u = k\}, \]

and

\[ f(p, q, r, s, t, u) = 3up + 2uq + 3ur + us + 6tp + 3tq + 3tr \]
\[ + 3sp + sq + 3rp + 3q + 6r + 4s + 3t. \]

We shall not make explicit the commutation formulas between other pairs of generators of \( U^+ \) except in the following special cases.

(a2) \[ E_1^{(r)} E_2^{(s)} = v^{3r} E_2^{(r)} E_1^{(s)} + v^3 E_2^{(s)} E_1^{(r)}, \]

(a3) \[ E_1^{(r)} E_1^{(s)} = v^{r} E_1^{(r)} E_1^{(s)} + v(v + v^{-1}) E_1^{(r)} E_1^{(s)} + v^{r-1} E_1^{(r)} E_1^{(s)} + (v^2 - 1 + v^{-2}) E_1^{(s)} E_1^{(r)} + (v^2 - 2) E_1^{(s)} E_1^{(r)}. \]
(a4) \[ E_1 E_{1112}^{(k)} = v^{-k'} E_{1112}^{(k')} E_1 + v^{-2k'+1}(v^2 + 1 + v^{-2})E_{1112}^{(k'-1)} E_{1112}, \]

(a5) \[ E_1 E_{1112}^{(k')} = E_{1112}^{(k')} E_1 + v^{-3k'+2}(1 - v^2)E_{1112}^{(k'-1)} E_{1112}, \]

(a6) \[ E_1^{(k)} E_2 = v^{3k} E_2 E_1^{(k)} + v^{2k+1} E_1 E_1^{(k-1)} + v^{k+2} E_{1112} E_1^{(k-2)} + v^3 E_{1112} E_1^{(k-3)}, \]

(a7) \[ E_{1112}^{(k')} E_2 = v^{-3k} E_{2} E_{1112}^{(k')-1} + v^{-6k+3}(v^2 - 1)(v^4 - 1)E_{1112}^{(3)} E_{1112}^{(k'-1)}, \]

(a8) \[ E_{1112}^{(k)} E_2 = E_2 E_{1112}^{(k)} + v^{-2k+2}(v^3 - v^3)E_{1112} E_{1112}^{(k-2)} E_{1112}^{(k-3)} + v^{-2k+2}(v^2 - v^2)E_{1112}^{(k-1)}, \]

(a9) \[ E_{1112}^{(k)} E_2 = v^{3k} E_2 E_{1112}^{(k)} + (-v^4 - v^2 + 1)E_{1112} E_{1112}^{(k-1)} + v^{-2k+2}(v^3 - v^3)E_{1112} E_{1112}^{(k-1)} + v^{-3k+6}(v^4 - 1)E_{1112} E_{1112}^{(k-2)}, \]

(a10) \[ E_{1112}^{(k)} E_{12} = v^{-k} E_{12} E_{1112}^{(k)} + v^{-2k-1}(1 + v^2 + v^4)E_{1112} E_{1112}^{(k-1)}, \]

(a11) \[ E_{1112}^{(k)} E_{12} = E_{12} E_{1112}^{(k)} + v^{-3k+4}(v^{-2} - v^2)E_{1112} E_{1112}^{(k-1)}. \]

5.5. We have:

\[ E_{12}^{(k)} = \sum_{i=0}^{k} (-1)^{k-i} v^{-i} E_{12}^{(k-i)} E_{12}^{(k)}. \]

Furthermore, \( E_{12}^{(k)} \) (when \( \mu = 1 \)), \( E_{1112}^{(k)} \) (when \( \mu = 2 \)) and \( E_{1112}^{(k)} \) (when \( \mu = 3 \)) are given by:

\[ \sum_{k=0}^{d_2 k'} (-1)^{d_2 k'} v^{-k} E_{12}^{(k)} E_{12}^{(d_2 k'-k)}. \]

These formulas can be deduced from 5.3(c), 5.3(i), 5.4(a1).

5.6. The divided powers (see 5.1) of the elements in the sequence 5.1(a\( \mu \)) belong to \( U^+ \). This follows from 5.5 for all elements except for \( E_{1112}, E_{1112} \) in the case \( \mu = 3 \). For these, we use the following argument. Writing 5.4(a1) for \( (k, k') = (2q, q) \) and \( (k, k') = (3p, 2p) \), we see that \( v^{4q} E_{1112}^{(q-1)} - E_{12}^{(2q)} E_{12}^{(q)} \) is a sum of terms of form \( u_1 E_{1112}^{(b)} E_{1112}^{(c)} u_2 \) with \( b \leq q/2, c < q \), while \( v^{6p} E_{1112}^{(3p)} E_{1112}^{(2p)} \) is a sum of terms of form \( u_3 E_{1112}^{(b')} E_{1112}^{(c')} u_4 \) with \( b_1 < p, c_1 < 3p/2 \); here, \( u_1, u_2, u_3, u_4 \) are elements of \( U^+ \). These two facts imply by induction the desired result.

**PROPOSITION 5.7.** The elements \( E^\# \) defined in 4.1 and 4.3 form an \( \mathcal{A} \)-basis of \( U^+ \).

From 5.6, we see that these elements are contained in \( U^+ \). Let \( u \in U^+ \). By 4.2, we can write \( u \) uniquely as a \( Q(v) \)-linear combination of our basis.
elements, and it remains to show that the coefficients are in \( \mathcal{A} \). When \( \mu = 1 \) or 2, this follows easily by a repeated application of the commutation formulas in 5.3. In the rest of the proof we assume that \( \mu = 3 \). We shall adapt a method from Kostant's paper \([4]\) (see also the exposition in \([11, \text{section 2, Lemma 8}]\)).

We define a lexicographic order on \( \mathbb{N}^6 \) as follows. If \( n = (n_1, \ldots, n_6) \), \( n' = (n'_1, \ldots, n'_6) \) belong to \( \mathbb{N}^6 \), we say that \( n < n' \) if there exists an index \( j \) such that \( n_j < n'_j \) and \( n_h = n'_h \) for all \( h \) such that \( h > j \). We say that \( n \preceq n' \) if \( n < n' \) or \( n = n' \).

For \( n \in \mathbb{N}^6 \), let \( L(n) \) be the \( 2 \times N \) matrix:

\[
\left( \begin{array}{cccccc}
1 & \cdots & 1 & 3 & \cdots & 3 \\
0 & \cdots & 0 & 1 & \cdots & 1
\end{array} \right)
\]

which contains \( n_1 \) columns \( (1, 0) \), \( n_2 \) columns \( (3, 1) \), \( n_3 \) columns \( (2, 1) \), \( n_4 \) columns \( (3, 2) \), \( n_5 \) columns \( (1, 1) \) and \( n_6 \) columns \( (0, 1) \). (We have \( N = \sum j n_j \).)

To each of the following six column vectors we associate a set of column vectors (said to be its subordinates) as shown:

\[
\begin{align*}
(1, 0) & \Rightarrow \emptyset; \\
(3, 1) & \Rightarrow \{(1, 0), (2, 0), (3, 0)\}; \\
(2, 1) & \Rightarrow \{(1, 0), (2, 0)\}; \\
(3, 2) & \Rightarrow \{(1, 0), (2, 0), (3, 1), (3, 1)\}; \\
(1, 1) & \Rightarrow \{(1, 0), (0, 1)\}; \\
(0, 1) & \Rightarrow \emptyset.
\end{align*}
\]

**ASSERTION A.** Assume given \( n, n' \in \mathbb{N}^6 \) with \( \Sigma j n_j = \Sigma j n'_j = N \). Assume also given \( N \) matrices \( \Lambda_1, \ldots, \Lambda_N \) with two rows and \( N \) columns each, with entries in \( \mathbb{N} \). Assume that the sum of these \( N \) matrices is the matrix \( L(n') \). We assume that, for each \( k \in [1, N] \), at least one entry of \( \Lambda_k \) is non-zero and that the last non-zero column \( C_k \) of \( \Lambda_k \) is equal to the \( k \)th column \( D_k \) of \( L(n) \) or to one of its subordinates. Then \( n \preceq n' \). If we have \( n = n' \), then \( C_k = D_k \) for all \( k \).

(We leave the easy verification to the reader.) Recall from 1.6 that \( U^{>0} \) has been decomposed in a direct sum of subspaces \( U_j^{>0} \) indexed by pairs \( j \) of natural numbers. It will be convenient to write such a pair as a column \( j = \left( \begin{array}{c} j_1 \\ j_2 \end{array} \right) \). A vector in the subspace \( U_j^{>0} \) is said to have degree \( j \). If \( \alpha \in \mathbb{R}^+ \), then
the degree \( j \) of \( E_a \) is well defined; it is one of \( \left( \begin{array}{c} 1 \\ 0 \end{array} \right), \left( \begin{array}{c} 3 \\ 1 \end{array} \right), \left( \begin{array}{c} 2 \\ 1 \end{array} \right), \left( \begin{array}{c} 3 \\ 2 \end{array} \right), \left( \begin{array}{c} 1 \\ 1 \end{array} \right), \left( \begin{array}{c} 0 \\ 1 \end{array} \right) \) and we have:

**ASSERTION B.** (i) \( \Delta(E_a) = E_a \otimes 1 + \kappa_a \otimes E_a \) plus a sum of terms of form \( u_1 \otimes u_2 \) where \( u_1, u_2 \in U^{>0} \) have well-defined degrees and the degree of \( u_2 \) is subordinate to \( j \) (\( \kappa_a \) is a monomial in \( K_1, K_2 \)). (ii) \( \Delta^{ln}(E_a) \in (U^{>0})^{\otimes N} \) is equal to the sum over \( k \in [1, N] \) of the terms (said to be principal) \( K \otimes \cdots \otimes K \otimes E_a \otimes 1 \cdots \otimes 1 \) with \( K \) a fixed monomial in \( K_1, K_2 \), and \( E_a \) in the \( k \)th position, plus a sum of terms (said to be subordinate) of form \( u_1 \otimes \cdots \otimes u_{n-1} \otimes u_n \otimes 1 \otimes \cdots \otimes 1 \), where \( u_1, \ldots, u_n \) are elements of \( U^{>0} \) with well-defined degrees and the degree of \( u_n \) is subordinate to \( j \).

One verifies (i) directly; (ii) is deduced from (i). (Note that in the classical case of enveloping algebras, there are no subordinate terms. The presence of subordinate terms is the main reason for the present proof to be more complicated than in the classical case.)

Let \( L \) be a \( 2 \times N \) matrix with entries in \( N \). Then \( L \) defines a subspace \( U_{j_1}^{>0} \otimes \cdots \otimes U_{j_N}^{>0} \) of \( (U^{>0})^{\otimes N} \), where \( j_1, \ldots, j_N \) are the first, \( \ldots \), \( \)Nth column of \( L \). The vectors in this subspace are said to have multidegree \( L \). When \( L \) varies, these subspaces form a direct sum decomposition of \( (U^{>0})^{\otimes N} \). Let \( n, n' \in N^6 \) be such that \( \Sigma_j n_j = \Sigma_j n'_j = N \). Let \( E(n) = E_{n_1}^1 E_{n_2}^{112} E_{n_3}^{1112} E_{n_4}^{11122} \times E_{n_5}^{12} E_{n_6}^{2} \in U^{>0} \). Let \( \tau_{nn'} \) be the projection of \( \Delta^{ln}(E(n)) \) onto the subspace of vectors of multidegree \( L(n') \) (in the direct sum decomposition above).

For each \( j \in [1, 6] \) define a subset \( S_j(n) \) of the set \( \{1, 2, \ldots, N\} \) as follows: \( S_1(n) \) consists of the first \( n_1 \) elements in this set, \( S_2(n) \) consists of the next \( n_2 \) elements, \( \ldots \), \( S_6(n) \) consists of the last \( n_6 \) elements.

Let \( E(n) \in (U^{>0})^{\otimes N} \) be defined as \( x_1 \otimes \cdots \otimes x_N \), where \( x_k = E_1 \) for \( k \in S_1(n) \), \( x_k = E_{1112} \) for \( k \in S_2(n) \), \( x_k = E_{112} \) for \( k \in S_3(n) \), \( x_k = E_{12} \) for \( k \in S_4(n) \), \( x_k = E_2 \) for \( k \in S_5(n) \), \( x_k = E_2 \) for \( k \in S_6(n) \). Let \( c(n) = [n_1][n_2][n_3][n_4][n_5][n_6] \in \mathcal{A} \).

**ASSERTION C.** (i) If \( \tau_{nn'} \neq 0 \), then \( n \preceq n' \).

(ii) For \( n = n' \) we have
\[
\tau_{nn} = c(n) \nu \kappa E(n);
\]
here \( \nu \) is some integer, \( \kappa = \kappa_1 \otimes \cdots \otimes \kappa_N \) and \( \kappa_j \) are certain monomials in \( K_1, K_2 \).

Since \( \Delta^{ln} \) is an algebra homomorphism, we can express \( \Delta^{ln}(E(n)) \) as a product of factors \( \Delta^{ln}(E_a) \); each of these factors can be written as a sum of terms as in Assertion A(ii). Let us select one such term \( \xi_k \) in the \( k \)th factor such
that the product $\xi_1 \cdots \xi_N$ is non-zero, of multidegree $L(n')$. (Then $r_{n,n'}$ is the sum of all such products). Let $\Lambda_k$ be the multidegree of $\xi_k$. We have $\Sigma_k \Lambda_k = L(n')$. We can apply Assertion A (its assumptions are satisfied by Assertion B(ii)). Assertion C(i) follows; moreover, in the case where $n = n'$, it follows that the terms $\xi_k$ are necessarily principal terms (in the terminology of Assertion B(ii)). Assertion C(ii) then follows essentially as in the classical case of enveloping algebras.

**Assertion D.** The $U$-module $M$ (see 2.2) has the following property. Let $t(\alpha) = E_2X_{-\alpha}$, ($\alpha \in R^+$). Then $t(\alpha)$ is an indivisible element of the $\mathcal{A}$-lattice $M$.

Indeed, we have $t(\alpha_1) = t_1$, $t(3\alpha_1 + \alpha_2) = v^{-1}t_1 - t_2$, $t(2\alpha_1 + \alpha_2) = -v^{-2}[2]t_1 + [3]t_2$, $t(3\alpha_1 + 2\alpha_2) = -v^{-3}[2]t_1 + v^{-3}[2]t_2$, $t(\alpha_1 + \alpha_2) = v^{-3}t_1 - [3]t_2$, $t(\alpha_2) = t_2$.

Assume that there exists an element $u \in U^+$ which is a $\mathbb{Q}(v)$ linear combination of basis elements $E^\phi$ with at least one coefficient not in $\mathcal{A}$. We will show that this leads to a contradiction. For $u' \in U^+$, we can write uniquely $u' = \sum b(n, u')E(n)$ with $b(n, u') \in \mathbb{Q}(v)$. Using our assumption and the fact that $\Psi(U^+) = U^+$ we see that $b(n, u') \notin c(n)^{-1}\mathcal{A}$ for some $n$, where $u' = \Psi(u)$. Moreover, we can choose $n$ so that we also have $b(n', u') \notin c(n')^{-1}\mathcal{A}$ for all $n' < n$. Let $N = n_1 + \cdots + n_6$.

In the $U$-module $M \otimes \mathbb{N}$ (see 2.3) we consider the elements $X(n) = x_1 \otimes \cdots \otimes x_N$, $t(n) = y_1 \otimes \cdots \otimes y_N$, where $x_k = X_{-\alpha_1}$, $y_k = t(\alpha_1)$ for $k \in S_1(n)$; $x_k = X_{-3\alpha_1 - \alpha_2}$, $y_k = t(3\alpha_1 + \alpha_2)$ for $k \in S_2(n)$; $x_k = X_{-2\alpha_1 - \alpha_2}$, $y_k = t(2\alpha_1 + \alpha_2)$ for $k \in S_3(n)$; $x_k = X_{-3\alpha_1 - 2\alpha_2}$, $y_k = t(3\alpha_1 + 2\alpha_2)$ for $k \in S_4(n)$; $x_k = X_{-\alpha_1 - \alpha_2}$, $y_k = t(\alpha_1 + \alpha_2)$ for $k \in S_5(n)$; $x_k = X_{-\alpha_1}$, $y_k = t(\alpha_1)$ for $k \in S_6(n)$. Let $M_0$ (resp. $M_0$) be the $\mathbb{Q}(v)$- (resp. $\mathcal{A}$-) submodule of $M$ (resp. $M$) generated by $t_1$, $t_2$. Consider the projection $M \to M_0$ which takes $t_i$ to $t_i$ ($i = 1, 2$) and all other basis elements to zero. Taking a tensor power, we get a $\mathbb{Q}(v)$-linear projection $M \otimes \mathbb{N} \to M_0 \otimes \mathbb{N}$ which is denoted by $\pi$. We have clearly $\pi(M \otimes \mathbb{N}) \subset M_0 \otimes \mathbb{N}$. In particular,

$$\pi(u'X(n)) \in M_0 \otimes \mathbb{N}.$$ 

If $n'' \in \mathbb{N}^6$, then from the definitions, we have

$$\pi(E(n'')X(n)) = \pi(E(n')X(n)).$$

Hence, if this is non-zero, we have $n'' \leq n$ (by Assertion C). Since $u''$ is a linear combination of $E(n')$ with $n' \geq n$, it follows that

$$\pi(u''X(n)) = b(n, u'')\pi(E(n)X(n)) = b(n, u'')\pi(r_{n,n}X(n)) = b(n, u'')c(n)u''E((n))X(n) = b(n, u'')c(n)u''t(n),$$

where $c(n)u''E((n))X(n) = b(n, u'')c(n)u''t(n)$.
where $f$ is some integer. It follows that the last expression is contained in $M_0^{\otimes N}$. From Assertion D, it follows that $b(n)$ is an indivisible element of the lattice $M^{\otimes N}$ hence also of its direct summand $M_0^{\otimes N}$. It follows that $b(n, u^t)c(n)u^f$ is contained in $\mathcal{A}$. This is a contradiction; the proposition is proved.

5.8. Let us write the sequence 5.1(a) in the form:

(a) $e_1, e_2, e_3, \ldots, e_v$

(In particular, $e_1 = E_2$, $e_v = E_1$.) From the formulas in 5.2, it follows easily, by induction, that for any $i < j$ in $[1, v]$, and any $k, k' \in \mathbb{N}$ we have

(b) $e_j^{(k)}e_j^{(k')} = \sum_{\zeta} c_{\zeta, i, j, k, k'} e_j^{(\zeta(0))} e_j^{(\zeta(i + 1))} \cdots e_j^{(\zeta(0))}$

where $\zeta$ runs over all maps of the interval $\{z \in \mathbb{N}: i \leq z \leq j\}$ to $\mathbb{N}$, and all but finitely many of the coefficients $c_{\zeta, i, j, k, k'} \in \mathbb{Q}(t)$ are zero. These coefficients are uniquely determined and belong to $\mathcal{A}$, by 5.7. Hence these are some universal quantities. We can define an abstract $\mathcal{A}$-algebra (with 1) $V^+(d_1, d_2)$ with generators $e_i^{(N)}(1 \leq i \leq v, N \in \mathbb{N})$ with $e_i^{(0)} = 1$ for all $i$ and relations given by (b) above and

(c) $e_i^{(N)} e_i^{(M)} = \left[ \begin{array}{c} M + N \\ N \end{array} \right]_d e_i^{(M + N)}$

where $d = d_1$ if $i$ is even and $d = d_2$ if $i$ is odd. (Note that $d_1 = d_2$ if $v = 3$, $(d_1, d_2) = (1, 2)$ if $v = 4$ and $(d_1, d_2) = (1, 3)$ if $v = 6$.) We shall also need some variants of this algebra. We can replace the multiplication by the opposite one, or we can keep the original generators but change the original relations by applying $v \to v^{-1}$ to their coefficients, or we can change the multiplication in the last algebra to the opposite one. We thus get three new $\mathcal{A}$ algebras $V^+_v(d_1, d_2), V^-_v(d_1, d_2), V^+_v(d_1, d_2)$. We have $\mathcal{A}$-algebra homomorphisms

$V^+_v(d_1, d_2) \to U^+, \quad V^+_v(d_1, d_2) \to U^+$,

$V^-_v(d_1, d_2) \to U^-, \quad V^-_v(d_1, d_2) \to U^-$;

the first two map $e_1$ to $E_2$, $e_v$ to $E_1$ and the last two map $e_1$ to $F_2$, $e_v$ to $F_1$. They are actually algebra isomorphisms. (Compare [8, 4.5].)

6. SOME PROPERTIES OF $U$

6.1. We now return to the general case. Consider a two-dimensional subspace $P$ of $X \otimes Q$ such that $R_p = R \cap P$ generates $P$ over $Q$; let $R^+_p = R_p \cap R^+$. We say that $P$ is an admissible plane if one of the conditions
(a)–(f) below is satisfied.

(a) \( R^+_P = \{x, x_i\} \) with \( i < g(x) \),

(b) \( R^+_P = \{x, x + x_i, x_i\} \) with \( i < g(x) \),

(c) \( R^+_P = \{x', x' + x, x\} \) with \( h'(x) = l, h'(x') = l + 1, \)

\[ h'(x' + x) = \frac{2l + 1}{2}, g(x) = g(x'). \]

(d) \( R^+_P = \{x, x + x_i, x + 2x_i, x_i\} \) with \( i < g(x) \)

(e) \( R^+_P = \{x_j, x_j + x, x_j + 2x, x\} \)

with \( h'(x) = l, h'(x_j + 2x) = \frac{2l + 1}{2}, j < g(x) \)

(f) \( R^+_P = \{x_j, x_i + x_j, 3x_i + 2x_j, 2x_i + x_j, 3x_i + x_j, x_i\} \).

Given \( P \) as in (b)–(f), we define \((d', d'')\) to be \((1, 3)\) in case (f); \((1, 2)\) in cases (d), (e); \((d_k, d_k)\) in cases (b), (c), where \( x \) is in the \( W \)-orbit of \( x_k \).

6.2. We define an \( \mathcal{A} \)-algebra \( V^+ \) (with 1) by generators and relations as follows. The generators are

(a) \( E^{(N)}_\alpha (\alpha \in R^+, N \in \mathbb{N}) \)

with \( E^{(0)}_\alpha = 1 \). For each admissible plane \( P \) (see 6.1) we impose a set of relations among the generators \( E^{(N_1)}_{e[i]_1}, E^{(N_2)}_{e[i]_2}, \ldots, E^{(N_v)}_{e[i]_v} \) (where the subscripts are the elements of \( R^+ \) arranged in order as in 6.1(a)–(f)) as follows.

If \( P \) is as in 6.1(a), these generators commute. If \( P \) is as in 6.1(b), (d), (f), these generators are required to satisfy the relations of the algebra \( V^+_{+}(d', d'') \). If \( P \) is as in 6.1(c), (e), these generators are required to satisfy the relations of the algebra \( V^+_{+}(d', d'') \). (Here, \((d', d'')\) is as in 6.1.)

6.3. Similarly, we define an \( \mathcal{A} \)-algebra \( V^- \) by generators and relations as follows. The generators are

(a) \( F^{(N)}_\alpha (\alpha \in R^+, N \in \mathbb{N}) \)

with \( F^{(0)}_\alpha = 1 \). For each admissible plane \( P \) we impose a set of relations among the generators \( F^{(N_1)}_{e[i]_1}, F^{(N_2)}_{e[i]_2}, \ldots, F^{(N_v)}_{e[i]_v} \) (where the subscripts are the elements of \( R^- \) arranged in order as in 6.1(a)–(f)) as follows.

If \( P \) is as in 6.1(a), these generators commute. If \( P \) is as in 6.1(b), (d), (f), these generators are required to satisfy the relations of the algebra \( V^-_{+}(d', d'') \). If \( P \) is as in 6.1(c), (e), these generators are required to satisfy the relations of the algebra \( V^-_{+}(d', d'') \). (Here, \((d', d'')\) is as in 6.1.)
6.4. We define an $\mathfrak{g}$-algebra $V^0$ (with 1) by generators and relations as follows. The generators are:

(a) $K_i, K_i^{-1}, \left[ \begin{array}{c} K_i; c \\ t \end{array} \right]$ (for $i \in [1, n], c \in \mathbb{Z}, t \in \mathbb{N}$).

The relations are:

(b1) the generators (a) commute with each other,

(b2) $K_i K_i^{-1} = 1, \left[ \begin{array}{c} K_i; c \\ 0 \end{array} \right] = 1$,

(b3) $\left[ \begin{array}{cc} K_i; 0 \\ t \\ K_i; -t \\ t' \end{array} \right] = \left[ \begin{array}{cc} t + t' \\ t \end{array} \right] \left[ \begin{array}{c} K_i; 0 \\ t \end{array} \right], \quad (t, t' \geq 0),$

(b4) $\left[ \begin{array}{c} K_i; c \\ t \end{array} \right] - v^{-d_i} \left[ \begin{array}{c} K_i; c + 1 \\ t \end{array} \right] = -v^{-d_i(c+1)} K_i^{-1} \left[ \begin{array}{c} K_i; c \\ t - 1 \end{array} \right], \quad (t \geq 1),$

(b5) $(v^{d_i} - v^{-d_i}) \left[ \begin{array}{c} K_i; 0 \\ 1 \end{array} \right] = K_i - K_i^{-1}.$

6.5. Let $V$ be the $\mathfrak{g}$-algebra (with 1) defined by the generators 6.2(a), 6.3(a), 6.4(a), subject to the relations of $V^+, V^-, V^0$ and the following additional relations:

(a1) $E_{ai}^{(N)} F_{aj}^{(M)} = F_{aj}^{(M)} E_{ai}^{(N)}$ if $i \neq j$

(a2) $E_{ai}^{(N)} F_{aj}^{(M)} = \sum_{i \geq 0, i \leq N, j \leq M} F_{aj}^{(M-i)} \left[ \begin{array}{c} K_i; 2t - N - M \\ t \end{array} \right] E_{ai}^{(N-i)}$

(a3) $K_i^{\pm 1} E_{aj}^{(N)} = v^{\pm d_{ai} N} E_{aj}^{(N)} K_i^{\pm 1}$,

(a4) $K_i^{\pm 1} F_{aj}(N) = v^{\pm d_{ai} N} F_{aj}(N) K_i^{\pm 1}$,

(a5) $\left[ \begin{array}{c} K_i; c \\ t \end{array} \right] E_{aj}(N) = E_{aj}(N) \left[ \begin{array}{c} K_i; c + N a_{ij} \\ t \end{array} \right],$

(a6) $\left[ \begin{array}{c} K_i; c \\ t \end{array} \right] F_{aj}(N) = F_{aj}(N) \left[ \begin{array}{c} K_i; c - N a_{ij} \\ t \end{array} \right].$

The following result provides a presentation of $U^+, U^-, U$ by generators and relations.

THEOREM 6.6. (i) There are unique homomorphisms of $\mathfrak{g}$-algebras with the indicated properties:

(a) $V^+ \to U^+ (E_{ai}^{(N)} \to E_i^{(N)} \quad \forall i, N)$
The braid group action on $U$ restricts to a braid group action on $U$.

Under (a) and (c), $E_{\beta}^{(N)}$ is carried to $T_{w_{\beta}^*}(E_{\beta}^{(N)})$ for all $\beta \in \mathbb{R}^+$, (notations of 4.3). Similarly, under (b) and (c), $F_{\beta}^{(N)}$ is carried to $T_{w_{\beta}^*}(F_{\beta}^{(N)})$ for all $\beta \in \mathbb{R}^+$.

The obvious homomorphism $V^0 \rightarrow V$ composed with (c) is an injective algebra homomorphism

We have

$$E_{\beta}^{(N)} \in U^+, \quad F_{\beta}^{(N)} \in U^- (\beta \in \mathbb{R}^+), \quad \left[ K_i; c \atop t \right] \in U^0.$$

We have

$$\left[ K_i; c \atop t \right] = \prod_{s=1}^{i} \frac{K_i^{d_i(\epsilon - s + 1)} - K_i^{-1}v^{d_i(\epsilon + s - 1)}}{v^{d_i s} - v^{- d_i s}}.$$

**THEOREM 6.7.** (i) The elements

(a) $\prod_{\alpha \in \mathbb{R}^+} E_{\alpha}^{(N_{\alpha})} \quad (N_{\alpha} \in \mathbb{N} \, \forall \alpha)$

form a $\mathcal{A}$-basis of $U^+$; the elements

(b) $\prod_{\alpha \in \mathbb{R}^+} F_{\alpha}^{(N_{\alpha})} \quad (N_{\alpha} \in \mathbb{N} \, \forall \alpha)$

form a $\mathcal{A}$-basis of $U^-$. (The product in (a) is taken in an order as in 4.3, while that in (b) is taken in the opposite order.) The elements

(c) $\prod_{i=1}^{n} \left( K_i^{\delta_i} \begin{bmatrix} K_i; 0 \\ t_i \end{bmatrix} \right) \quad (t_i \geq 0, \, \delta_i = 0 \, \text{or} \, 1)$

form a $\mathcal{A}$-basis of $U^0$.

(ii) Multiplication defines an isomorphism of $\mathcal{A}$-modules

(d) $U^- \otimes U^0 \otimes U^+ \cong U$.

Hence the elements $FKE$ with $F$ as in (b), $K$ as in (c), $E$ as in (a), form a $\mathcal{A}$-basis.
of $U$. They also form a $\mathbb{Q}(v)$-basis of $U$. Hence the natural homomorphism

$$U \otimes \mathbb{Q}(v) \to U$$

is an isomorphism of $\mathbb{Q}(v)$-algebras.

The proof is essentially the same as that in [8, 4.5].

7. THE QUANTUM COORDINATE ALGEBRA

7.1. In [1], Chevalley constructed a $\mathbb{Z}$-form of the coordinate algebra of a simply connected semisimple algebraic group. Another approach to it has been given by Kostant [4] by taking a suitable dual of the enveloping algebra. We shall adapt Kostant's procedure to quantum groups.

Let $\mathcal{F}$ be the set of all two-sided ideals $I$ in $U$ such that:

(a) $I$ has finite codimension in $U$ and
(b) there exists some $r \in \mathbb{N}$ such that for any $i \in [1, n]$ we have

$$\Pi_{h = -r}(K_i - v^{ab}) \in I.$$

Let $\mathcal{A}_0 = \mathbb{Q}[v, v^{-1}]$ and let $U_{\mathcal{A}_0} = U \oplus_{\mathcal{A}_0} \mathcal{A}_0$. For $I \in \mathcal{F}$ we set $I_0 = I \cap U_{\mathcal{A}_0}$. Let $U^*$ be the set of $\mathbb{Q}(v)$-linear maps $U \to \mathbb{Q}(v)$ and let $O$ be the set of all $f \in U^*$ such that $f|_I = 0$ for some $I \in \mathcal{F}$. Similarly, let $U_{\mathcal{A}_0}^*$ be the set of all $\mathcal{A}_0$-linear maps $U_{\mathcal{A}_0} \to \mathcal{A}_0$ and let $O = O \cap U_{\mathcal{A}_0}^*$ (We identify $U_{\mathcal{A}_0}^*$ with a subset of $U^*$, using 6.7.) We can regard $O$ (resp. $O$) as a Hopf algebra over $\mathbb{Q}(v)$ (resp. $\mathcal{A}_0$): as in loc. cit. we define product and coproduct in $O$, $O$ by taking the transpose of the coproduct and product in $U$, $U$. To see that the coproduct is well defined in $O$, we must check the following statement:

(c) For any $I \in \mathcal{F}$, the $\mathcal{A}_0$-module $U_{\mathcal{A}_0}/I_0$ is free of finite rank.

It is clearly torsion-free, and due to the special nature of $\mathcal{A}_0$, it is enough to verify that it is finitely generated. Now the $U$-module $U/I$ is a direct sum of finitely many simple, finite-dimensional $U$-modules, to which we can apply [5, 4.2], hence we can find an $\mathcal{A}_0$-lattice $\mathcal{L}$ in $U/I$ which is stable under left multiplication by $U_{\mathcal{A}_0}$. Using the $U_{\mathcal{A}_0}$-module structure on $\mathcal{L}$, we find an injective $\mathcal{A}_0$-linear map $U_{\mathcal{A}_0}/I_0 \to \text{End}_{\mathcal{A}_0}(\mathcal{L})$. The last $\mathcal{A}_0$-module is finitely generated; since $\mathcal{A}_0$ is noetherian, it follows that $U_{\mathcal{A}_0}/I_0$ is finitely generated, as required.

7.2. In the last paragraph, we have used the complete reducibility of finite dimensional $U$-modules. This is proved in [10], using a description of the centre of $U$, together with the main result of [5]. However, there is a simpler proof, which still uses [5] but does not use the structure of the centre. By an
argument of Borel (given in [10]) it is enough to prove that any finite dimensional $U$-module $L$ generated by a highest weight vector is simple. Let $L_0$ be the $U_{\mathfrak{g}_0}$-submodule of $L$ generated by $x$. This coincides with the $U_{\mathfrak{g}_0} \cap U^-$-submodule of $L$ generated by $x$ (just as in [5, 4.5]). It follows immediately that $L_0$ is the direct sum of its intersections with the weight spaces of $L$, that these intersections are free $\mathfrak{g}_0$-modules of finite rank and that the natural homomorphism $Q(v) \otimes_{\mathfrak{g}_0} L_0 \to L$ is an isomorphism. Arguing just as in [5, 4.11, 4.12], we see that the dimension of $L$ is given by Weyl's dimension formula; the same proof shows that the simple quotient of $L$ has dimension given by the same formula. Hence, $L$ is simple. (I would like to point out that the proof of Proposition 4.2 in [5] is unnecessarily complicated (we assume that $F = F_0(q)$). In fact, parts (b), (c), (d) of that proposition are almost obvious and 4.6, 4.7, 4.8, and most of 4.9 in loc. cit. are unnecessary. Moreover, that proposition holds for any highest weight module, not just for simple ones.)

7.3. It is easy to see that the inclusion $O < O$ induces an isomorphism of Hopf algebras over $Q(v)$

\[ O \otimes_{\mathfrak{g}_0} Q(v) \cong O. \]

We call $O$ the quantum coordinate algebra and $O$ its $\mathfrak{g}_0$-form.

7.4. Let $\mathcal{M}$ be a $U_{\mathfrak{g}_0}$-module which is free, of finite rank as a $\mathfrak{g}_0$-module. We say that $\mathcal{M}$ is of type 1 if $\mathcal{M} \otimes Q(v)$ is a direct sum of subspaces on which each $K_i$ acts by multiplication by some integral power of $v$. Assume that $\mathcal{M}$ is of type 1. If $x \in \mathcal{M}$ and $\xi \in Hom_{\mathfrak{g}_0}(\mathcal{M}, \mathfrak{g}_0)$, the matrix coefficient $c_{x,\xi}: u \to \xi(ux)$ (an element of $U^*_{\mathfrak{g}_0}$), belongs to $O$. Moreover, it follows from the definitions that $O$ is exactly the $\mathfrak{g}_0$-submodule of $U^*_{\mathfrak{g}_0}$ spanned by the matrix coefficients $c_{x,\xi}$ for various $\mathcal{M}$, $x$, $\xi$ as above.

7.5. The definition of $O$ in terms of matrix coefficients of finite dimensional $U$-modules is suggested by Drinfeld in [2], where he describes $O$ in type $A_n$; for further results on $O$ (or, rather, its variant over formal power series) see [12].

8. Specialization to a root of 1

8.1. We fix an integer $l \geq 1$. Let $B$ be the quotient ring of $Q[v, v^{-1}]$ by the ideal generated by the $l$th cyclotomic polynomial. We denote the image of $v$ in $B$ again by $v$. Then $v$ has order $l$ in $B$.

Let $l_i$ be the order of $v^{2^d_i}$ in $B$ (a divisor of $l$). For any $x \in R^+$ we set $l_x = l_i$.
where $\alpha_i$ is in the $W$-orbit of $\alpha$. We regard $B$ as an $A$-algebra via the natural homomorphism $A \to B$, taking $v$ to $v$, and we form the $B$-algebras $U_B = U \otimes A B$, $U_B = U^+ \otimes A B$, $U^+_B = U^- \otimes A B$, $U^0_B = U^0 \otimes A B$. The generators of $U$ are mapped by the canonical homomorphism $U \to U_B$ to generators of $U_B$ denoted by the same letters. Similar conventions apply to the other algebras.

8.2. Let $u^+$ (resp. $u^-$) be the $B$-subalgebra of $U_B^+$ (resp. $U_B^-$) generated by the elements $E_i^{(N)}$ (resp. $F_i^{(N)}$) with $0 \leq N < l_i$, $\alpha \in R^+$. Similarly, let $u^0$ be the $B$-subalgebra of $U_B^0$ generated by the elements $K_i^{\pm 1}$. Let $u$ be the $B$-subalgebra of $U_B$ generated by the elements $E_i^{(N)}$, $F_i^{(N)}$, $K_i^{\pm 1}$ just considered.

THEOREM 8.3. (i) The elements $F$ (resp. $E$) with $F \in U_B^+$, $E \in U_B^-$ as in 6.7(b), (a), satisfying respectively $N_i < l_i$, $N'_i < l_i$, $\forall \alpha \in R^+$, form a $B$-basis of $u^+$ (resp. $u^-$).

(ii) The elements $K = \prod_{i=1}^n K_i^{N_i} (0 \leq N_i \leq 2l_i - 1)$ form a $B$-basis of $u^0$.

(iii) The elements $FK E$ with $F$, $E$ as in (i), $K$ as in (ii), form a $B$-basis of $u$.

(iv) In particular,

$$\dim_B u = 2^n \prod_{i=1}^n l_i \prod_{\alpha \in R^+} l_i^{2}.$$

In the simply laced case, this is proved in [8, §5]. The same method could be used in general, provided that we could verify the following statement in the setup of Section 5 (when $n = 2$).

Consider a relation 5.8(b) (the prototype of a defining relation for the $A$-algebra $U^+$). Assume that the exponents $k$, $k'$ in the left-hand side of that relation satisfy: $k < l_i$ if $j$ is even, $k < l_2$ if $j$ is odd, $k' < l_i$ if $i$ is even, $k' < l_2$ if $i$ is odd. Then the exponents $\xi(h)$, ($i \leq h \leq j$) in the right-hand side satisfy the analogous inequality $\xi(h) < l_i$ if $h$ is even, $\xi(h) < l_2$ if $h$ is odd, at least when the coefficient $c(\xi, i, j, k, k')$ is non-zero as an element of $B$. (In other words, if we regard the relation 5.8(b) over $B$, then from the fact that the left hand side has small exponents, it should follow that the right-hand side has small exponents.)

Assume first that $\mu = 1$ or 2. Then the relations 5.8(b) are described explicitly in 5.3 and the statement above is easily verified. (In 5.3(g), (h), some coefficients in the right-hand side can be non-zero in $A$ but zero in $B$ and this is crucial for the truth of our statement.) Assume now that $\mu = 3$. Since not all relations 5.8(b) are known explicitly, we argue in a different way. Let $u_1$ be the $B$-subspace of $U_B^+$ spanned by the elements $E$ in (i). It is sufficient to show that $u_1$ is stable under left and right multiplication by a set of algebra generators of $u^+$. 
This can be easily checked using the commutation formulas in 5.4. (Note that we can take as algebra generators for $u^+$ the set $E_1, E_2$ if $l > 6$ or $l = 5$, the set $E_1, E_2, E_{112}$ if $l = 4$, the set $E_1, E_{12}$ if $l = 3$ or 6 and the empty set if $l = 1$ or 2.)

8.4. We shall assume, from now on, that $l$ is odd and that $l$ is prime to 3 whenever the root system has a component of type $G_2$. We then have $l_a = l$ for all $a \in R^+$. Let $\delta_i$ (resp. $\delta'$) be the derivation of the algebra $U_B$ defined by $\delta_i(x) = E_i^{(0)} x - x E_i^{(0)}$ (resp. $\delta'(x) = F_i^{(0)} x - x F_i^{(0)}$).

**Lemma 8.5.** (i) $\delta_i$ leaves $u$ and $u^+$ stable.
(ii) $\delta'_i$ leaves $u$ and $u^-$ stable.

This is trivial for $l = 1$. Assume now that $l > 1$. Then the algebra $u^+$ (resp. $u^-$) is generated by the elements $E_i$ (resp. $F_i$) for $1 \leq i \leq n$; moreover, the algebra $u$ is generated by the elements $E_i, F_i, K_i, K_i^{-1}$ ($1 \leq i \leq n$). It is enough to show that our derivations map these generators into the corresponding subalgebra. We have:

\[
\delta_i(E_j) = \sum_{h \geq 0} \left[ -\frac{a_{ij}}{h} \right] E_i^{(h)} E_j E_i^{(l-h)} \quad \text{if } a_{ji} = -1,
\]
\[
\delta_i(E_j) = -E_i^{(l-1)} E_j E_i \quad \text{if } a_{ij} = -1,
\]
\[
\delta_i(F_j) = \begin{bmatrix} K_i; 1 \\ 1 \end{bmatrix} E_i^{(l-1)}
\]

and $\delta_i$ maps the generators $F_j (j \neq i), E_i$ and $K_i^\pm$ to 0. Similarly,

\[
\delta'_i(F_j) = -\sum_{h \geq 0} \left[ -\frac{a_{ij}}{h} \right] F_i^{(l-h)} F_j F_i^{(h)} \quad \text{if } a_{ji} = -1,
\]
\[
\delta'_i(F_j) = F_i F_j F_i^{(l-1)} \quad \text{if } a_{ij} = -1,
\]
\[
\delta'_i(E_j) = -F_i^{(l-1)} \begin{bmatrix} K_i; 1 \\ 1 \end{bmatrix}
\]

and $\delta'_i$ maps the generators $E_j (j \neq i), F_i$ and $K_i^\pm$ to 0. (These formulas follow from the results for rank 2 in Section 5.)

**Lemma 8.6.** There is a unique $B$-algebra homomorphism $\psi : U_Q^+ \otimes_Q B \to U_B^+$ which takes $E_i$ to $E_i^{(0)}$ for all $i$.

It is enough to check this in the setup of Section 5 (when $n = 2$). Assume for example that $\mu = 2$. Using 5.3(i) we compute in $U_B^+$:
\[ E_1^{(3l-hl)}E_2^{(h)} = \sum_{r+s+t=l \atop s+2t+u=3l-hl} E_2^{(3)}E_1^{(s)}E_1^{(t)}E_1^{(u')}, \]

\[ = \sum_{r+s+t=l \atop s+2t+u=3l} \left[ \begin{array}{c} u \\ hl \end{array} \right] E_2^{(3)}E_1^{(s)}E_1^{(t)}E_2^{(u')} \]

\[(0 \leq h \leq 3); \text{ we use the convention that } \left[ \begin{array}{c} m \\ m' \end{array} \right] = 0 \text{ if } 0 \leq m < m'. \text{ Let} \]

\[ A = \sum_{h=0}^{3} (-1)^h E_1^{(3l-hl)}E_2^{(h)}E_1^{(hl)}. \]

We want to show that \( A = 0 \). By the previous computation it is enough to show that for any integer \( u \geq l \) we have

\[ \sum_{h=0}^{3} (-1)^h \left[ \begin{array}{c} u \\ hl \end{array} \right] = 0 \]

in \( B \). This property of Gaussian binomial coefficients follows immediately from [6, 3.2]. From loc. cit. it follows also that \( E_1^{(hl)} = (E_1^{(h)})^l/(hl)! \). Hence the equation \( A = 0 \) can be written as

\[ \sum_{h=0}^{3} (-1)^h \frac{(E_1^{(l)})^{3-h}}{(3-h)!} E_2^{(h)} E_1^{(hl)} = 0. \]

An entirely similar argument shows that

\[ \sum_{h=0}^{2} (-1)^h \frac{(E_1^{(l)})^{2-h}}{(2-h)!} E_1^{(l)} E_2^{(l)} = 0. \]

This proves the lemma in the case where \( u = 2 \). The proof in the case where \( u = 1 \text{ or } 3 \) is entirely similar.

8.7. Consider the \( B \)-vector space \( \mathcal{V}^+ = (U_Q^+ \otimes Q B) \otimes B u^+ \). We identify \( U_Q^+ \otimes Q B \) (resp. \( u^+ \)) with a subspace of \( \mathcal{V}^+ \) via \( x \rightarrow x \otimes 1 \) (resp. \( y \rightarrow 1 \otimes y \)). From 8.5, 8.6, it follows that there is a unique associative \( B \)-algebra structure on \( \mathcal{V}^+ \) which coincides with the already known structure on \( U_Q^+ \otimes Q B \) (an enveloping algebra of a nilpotent Lie algebra) and on \( u^+ \), and is such that

\[ E_i \cdot y = y \cdot E_i + \delta_i(y) \]

for all \( i \in [1, n] \) and all \( y \in u^+ \); moreover, we see that there is a unique \( B \)-algebra homomorphism \( \gamma: \mathcal{V}^+ \rightarrow U_B^+ \) which takes each \( E_i \in U_Q^+ \otimes Q B \) to \( E_i^{(l)} \in U_B^+ \) and takes each \( y \in u^+ \) to \( y \).

**Lemma 8.8.** \( \gamma \) is an isomorphism of algebras.
The image of \( \gamma \) contains \( E_i, E_i^0 \) for all \( i \). These elements generate \( U_B \) as an algebra. Hence, \( \gamma \) is surjective. For any \( j \in \mathbb{N}^n \), let \( U_j^+ \) be the intersection of \( U^+ \) with \( U_j^+ \) (see 1.6). We have a direct sum decomposition \( U^+ = \bigoplus U_j^+ \). Tensoring with \( B \) or with \( Q \) we get direct sum decompositions \( U_B^+ = \bigoplus_j (U_B^+)_j \) and \( U_Q^+ \otimes Q B = \bigoplus_j (U_Q^+ \otimes Q B)_j \).

Let \( u_i^+ \) be the intersection of \( u^+ \) with \( (U_B^+)_i \) and let

\[
\gamma_j^+ = \bigoplus_{i,j'} (U_Q^+ \otimes Q B)_{i,j'} \otimes u_j^+.
\]

Then the four algebras \( U_B^+, U_Q^+ \otimes Q B, u^+, \gamma^+ \) are decomposed in direct sum of subspaces defined by the subscript \( j \) for the various \( j \in \mathbb{N}^n \). The dimensions of these subspaces are computable from 6.7(i) and 8.3(i) and we see that the subspaces of \( U_B^+ \), \( \gamma^+ \) with the same subscript \( j \) have the same (finite) dimension. On the other hand, it is clear from the definitions that \( \gamma \) maps \( \gamma_j^+ \) into \( (U_B^+)_j \); being surjective, it is necessarily an isomorphism.

**Lemma 8.9.** There is a unique \( B \)-algebra homomorphism \( U_B^+ \to U_Q^+ \otimes Q B \) which takes each \( E_i^{(N)} \) to \( E_i^{(N)}(m) \) if \( l \) divides \( N \) and to zero otherwise.

The uniqueness is clear. We now prove the existence. Let \( \pi : u^+ \to B \) be the unique homomorphism of algebras with 1 which takes each \( E_i \) to 0, and let \( J^+ \) be its kernel. It is clear that all derivations \( \delta_i \) of \( u^+ \) (see 8.5) map \( u^+ \) into \( J^+ \). It follows that the \( B \)-linear map \( \gamma^+ \to U_Q^+ \otimes Q B \) defined by \( x \otimes y \to \pi(y) x \) is an algebra homomorphism. Composing it with the inverse of \( \gamma \) (see 8.8) we obtain an algebra homomorphism \( U_B^+ \to U_Q^+ \otimes Q B \) which has the required property. (If \( R \) has no components \( G_2 \), one can give a more direct proof, using the defining relations of \( U_B^+ \).)

**Theorem 8.10.** There is a unique \( B \)-algebra homomorphism \( \chi : U_B \to U_B^+ \otimes Q B \) such that \( \chi(E_i^{(N)}) \) is \( E_i^{(N)} \) if \( l \) divides \( N \) and is zero otherwise; \( \chi(F_i^{(N)}) \) is \( F_i^{(N)} \) if \( l \) divides \( N \) and is zero otherwise; \( \chi(K_i^{\pm 1}) = K_i^{\pm 1} \) (1 \( \leq i \leq n \)).

Our requirements define \( \chi \) on \( U_B^+ \), by 8.9 and, by symmetry, also on \( U_B^- \).

We define \( \chi : U_B^0 \to U_B^0 \otimes Q B \) by \( \chi(K_i^{\pm 1}) = K_i^{\pm 1} \), \( \chi \left( \begin{bmatrix} K_i; 0 \\ 0 \\ 0 \\ N \\ l \end{bmatrix} \right) = \begin{bmatrix} K_i; 0 \\ N/l \end{bmatrix} \) if \( l \) divides \( N \) and \( \chi \left( \begin{bmatrix} K_i; 0 \\ N \end{bmatrix} \right) = 0 \), otherwise. It is easy to check that these maps extend to the whole of \( U_B \) as an algebra homomorphism. (We use the presentation of \( U_B \) provided by 6.6(i). We only have to verify the relatively simple relations 6.5(a1)–(a6); the other relations are automatically satisfied.)
8.11. The Hopf algebra structure on $U$ (see 1.1) induces a Hopf algebra structure on $U$ (by 6.7(ii) and 1.3(a), (b)). This, in turn, induces Hopf algebra structures on $U_B$, $U_Q \otimes Q B$, $u$. It is easy to check that $\chi$ in 8.10 is compatible with the Hopf algebra structures.

8.12. The braid group action on $U$ (see 6.6(ii)) induces braid group actions on $U_B$, $U_Q \otimes Q B$, $u$, and one verifies that $\chi$ in 8.10 is compatible with these braid group actions. It follows that, for any $\alpha \in R^+$, $\chi$ takes $E^{(N)}_\alpha$ to $E^{(N_l)}_\alpha$ if $l$ divides $N$ and to zero, otherwise; it takes $F^{(N)}_\alpha$ to $F^{(N_l)}_\alpha$ if $l$ divides $N$ and to zero, otherwise. It follows that the kernel of $\chi$ is precisely the subspace $\mathcal{F}$ of $U_B$ spanned by the basis elements $F K E$ with $F$, $K$, $E$ as in 6.7(b), (c), (a), such that at least one of the exponents $N_F$, $N_K$, $h$ is not divisible by $l$.

8.13. Let $\mathcal{B}$ be the quotient ring of $\mathcal{A}$ by the ideal generated by the $l$th cyclotomic polynomial. We regard $\mathcal{B}$ as an $\mathcal{A}$-algebra via the natural homomorphism $\mathcal{A} \to \mathcal{B}$, taking $v$ to $v$, and we form the $\mathcal{B}$-algebra $U_{\mathcal{B}} = U \otimes_{\mathcal{A}} \mathcal{B}$.

**COROLLARY 8.14.** There is a unique $\mathcal{B}$-algebra homomorphism $\chi_{\mathcal{B}} : U_{\mathcal{B}} \to U_{\mathcal{Z}} \otimes \mathcal{B}$ which is given by the same formulas as $\chi$ in 8.10.

The uniqueness is clear. For the existence, define $\chi_{\mathcal{B}}$ as the restriction of $\chi$ to $U_{\mathcal{B}}$.

8.15. Assume in this paragraph that our $l$ (in 8.4) is a prime number $p$. We can regard the finite field $F_p$ as a $\mathcal{B}$-algebra with $v$ acting as 1. Applying the functor $\otimes_{\mathcal{B}} F_p$, $U_{\mathcal{Z}} \otimes \mathcal{B}$ becomes $U_{F_p}$ (by the definition 1.5), $U_{\mathcal{B}}$ becomes $U_{F_p}$ (exactly as in [8, §6]) and $\chi_{\mathcal{B}}$ becomes the $F_p$-algebra homomorphism $\chi_p : U_{F_p} \to U_{F_p}$ defined by the same formulas as $\chi$ in 8.10.

Let $\bar{U}_{F_p}$ be the quotient of the $F_p$-algebra $U_{F_p}$ by the ideal generated by the central elements $K_1 - 1, \ldots, K_n - 1$. Then $\bar{U}_{F_p}$ is the ‘hyperalgebra’ of a semisimple algebraic group $G$ defined over $F_p$ and $\chi_p$ induces on $U_{F_p}$ an endomorphism which coincides with that induced by the Frobenius morphism $G \to G$.

In this sense, we may regard $\chi$ or $\chi_{\mathcal{B}}$ as a lifting of the Frobenius morphism to characteristic zero.

8.16. We no longer assume that $l$ is prime. The quotient of $U_Q$ by the ideal generated by the central elements $K_1 - 1, \ldots, K_n - 1$ is denoted $\bar{U}_Q$. This is the classical enveloping algebra corresponding to the semisimple Lie algebra over $Q$ with the given Cartan matrix. Composing the obvious homomorphism $U_Q \otimes_Q B \to \bar{U}_Q \otimes_Q B$ with $\chi$, we obtain a surjective homomorphism $\chi' : U_B \to \bar{U}_Q \otimes_Q B$. (This homomorphism has been introduced, in the simply
112 GEORGE LUSZTIG

laced case, in [6, 7.5].) From what it has been said in 8.12, we see that the kernel of \( \chi' \) is precisely

\[ \mathcal{J}' = \sum_{i=1}^{n} (K_i - 1) \mathcal{J} \]

where \( \mathcal{J} \) is as in 8.12. It is easy to see that \( \mathcal{J}' \) coincides with the two-sided ideal of \( U_B \) generated by the augmentation ideal of \( u \).

Hence the classical enveloping algebra \( \bar{U}_Q \otimes_Q B \) may be regarded as the 'Hopf algebra quotient' of the Hopf algebra \( U_B \) by the finite dimensional Hopf subalgebra \( u \).

8.17. Let

\[ O_B = O \otimes_{\mathcal{A}_0} B, \quad O_Q = O \otimes_{\mathcal{A}_0} Q. \]

Then \( O_Q \) may be regarded as the coordinate algebra of the simply connected semisimple group over \( Q \) with the given Cartan matrix. The homomorphism \( \chi \) induces by passage to dual, an imbedding of Hopf algebras over \( B \):

\[ O_Q \otimes B \subseteq O_B. \]

Thus, the classical coordinate algebra appears as a sub-Hopf algebra of the quantum coordinate algebra.

APPENDIX (by Matthew Dyer and George Lusztig)

Theorem 6.7 admits the following generalization. Let \( s_i s_i^2 \cdots s_i \) be a reduced expression of the longest element \( w_0 \) of \( W \); thus, \( v = \# R^+ \). We have a bijection \([1, v] \to R^+\) defined by

\[ j \mapsto s_i s_i^2 \cdots s_i (\alpha_{i_j}). \]

We use this to totally order \( R^+ \). If \( \beta \in R^+ \) corresponds to \( j \), we set \( w_\beta = s_i s_i^2 \cdots s_{i_{j-1}} \) and \( i_\beta = i_j \). We define

\[ E^{(N)}_\beta = T_{w_\beta}(E^{(N)}_{i_\beta}) \in U^+, \quad F^{(N)}_\beta = T_{w_\beta}(F^{(N)}_{i_\beta}) \in U^-. \]

These elements generalize those in 6.7 (which are obtained for a particular reduced expression of \( w_0 \)). Moreover, the statement of 6.7 remains true in this more general case. We sketch a proof.

Let \( U_1^+ \) be the \( \mathcal{A} \)-submodule of \( U^+ \) generated by the elements 6.7(a) (in the present, more general setting). Using 4.2 and 6.7(d) we see that we only have to check that \( U_1^+ = U^+ \). When \( n = 2 \), this follows easily from the results in Section 5. The general case can be reduced to the rank 2 case as follows. Consider another reduced expression \( s_i s_i^2 \cdots s_i \) for \( w_0 \) and let \( U_2^+ \) be the
corresponding \mathcal{A}\text{-submodule of } U^+. We first want to show that \( U^+_1 = U^+_2 \). Now any two reduced expressions of \( w_0 \) can be obtained one from another by a successive application of the braid group relations; hence, we may assume that our two reduced expressions are related to each other by an application of a single braid group relation. In this case, the equality \( U^+_1 = U^+_2 \) follows immediately from the analogous equality in the rank 2 case corresponding to that braid group relation and from 6.6(ii). It is clear that \( U^+_1 \) is stable by left multiplication by the elements \( E_i^{(N)} \ (N \geq 0) \). Now any simple reflection appears as the first factor in some reduced expression of \( w_0 \). Since \( U^+_1 \) is independent of the reduced expression, it must be stable by left multiplication by any element \( E_i^{(N)} \ (N \geq 0, 1 \leq i \leq n) \). Since it contains 1, it must coincide with \( U^+ \), as desired.

REFERENCES


Author's address:

George Lusztig,
Department of Mathematics,
Massachusetts Institute of Technology,
Cambridge, MA 02139,
U.S.A.

(Received, August 1, 1989)