

GEORGE LUSZTIG

QUANTUM GROUPS AT ROOTS OF 1*

Dedicated to Jacques Tits on his sixtieth birthday

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, \dots, 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 $(d_i a_{ij})$ 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 $\mathcal{A} = \mathbf{Z}[v, v^{-1}]$, with quotient field $\mathbf{Q}(v)$. For $h \in \mathbf{N}$, let $[h] = (v^h - v^{-h})/(v - v^{-1})$.

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

$$[N]_d^! = \prod_{h=1}^N \frac{v^{dh} - v^{-dh}}{v^d - v^{-d}} \in \mathcal{A}, \quad \begin{bmatrix} M+N \\ N \end{bmatrix}_d = \frac{[M+N]_d^!}{[M]_d^! [N]_d^!} \in \mathcal{A}.$$

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

$$(a1) \quad K_i K_j = K_j K_i, \quad K_i K_i^{-1} = K_i^{-1} K_i = 1,$$

$$(a2) \quad K_i E_j = v^{d_i a_{ij}} E_j K_i, \quad K_i F_j = v^{-d_i a_{ij}} F_j K_i,$$

$$(a3) \quad E_i F_j - F_j E_i = \delta_{ij} \frac{K_i - K_i^{-1}}{v^{d_i} - v^{-d_i}},$$

$$(a4) \quad \sum_{r+s=1-a_{ij}} (-1)^s \begin{bmatrix} 1-a_{ij} \\ s \end{bmatrix}_{d_i} E_i^r E_j E_i^s = 0 \quad \text{if } i \neq j,$$

$$(a5) \quad \sum_{r+s=1-a_{ij}} (-1)^s \begin{bmatrix} 1-a_{ij} \\ s \end{bmatrix}_{d_i} F_i^r F_j F_i^s = 0 \quad \text{if } i \neq j.$$

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

$$\sum_{r+s=1-a_{ij}} (-1)^s E_i^{(r)} E_j E_i^{(s)} = 0 \quad \text{if } i \neq j,$$

$$\sum_{r+s=1-a_{ij}} (-1)^s F_i^{(r)} F_j F_i^{(s)} = 0 \quad \text{if } i \neq j.$$

\mathbf{U} is a Hopf algebra with comultiplication Δ , antipode S and counit ε defined by

$$(b) \quad \Delta E_i = E_i \otimes 1 + K_i \otimes E_i, \quad \Delta F_i = F_i \otimes K_i^{-1} + 1 \otimes F_i, \\ \Delta K_i = K_i \otimes K_i,$$

$$(c1) \quad S E_i = -K_i^{-1} E_i, \quad S F_i = -F_i K_i, \quad S K_i = K_i^{-1},$$

$$(c2) \quad \varepsilon E_i = \varepsilon F_i = 0, \quad \varepsilon K_i = 1.$$

By iterating Δ we obtain as usual an algebra homomorphism $\Delta^{(N)}: \mathbf{U} \rightarrow \mathbf{U}^{\otimes N}$.

Let $\Omega, \Psi: \mathbf{U} \rightarrow \mathbf{U}^{\text{opp}}$ be the \mathbf{Q} -algebra homomorphisms defined by

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

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

1.2. Let X (resp. Y) be the free abelian group with basis ϖ_i (resp. $\check{\alpha}_i$), $1 \leq i \leq n$. Let $\langle \cdot, \cdot \rangle: Y \times X \rightarrow \mathbf{Z}$ be the bilinear pairing such that $\langle \check{\alpha}_i, \varpi_j \rangle = \delta_{ij}$ and let $\alpha_j \in X$ be defined by $\langle \check{\alpha}_i, \alpha_j \rangle = a_{ij}$. Define $s_i: X \rightarrow X$, $s_i: Y \rightarrow Y$ by $s_i(x) = x - \langle \check{\alpha}_i, x \rangle \alpha_i$, $s_i(y) = y - \langle y, \alpha_i \rangle \check{\alpha}_i$. We identify $\text{GL}(X) = \text{GL}(Y)$ using the pairing above and we let W be its (finite) subgroup generated by s_1, \dots, s_n . Let Π be the set consisting of $\alpha_1, \dots, \alpha_n$, let $R = W\Pi \subset X$ and let $R^+ = R \cap (\mathbf{N}\alpha_1 + \dots + \mathbf{N}\alpha_n)$.

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

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

We have

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

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

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

Let U^+ (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 \mathbf{Q} as a $\mathbf{Q}(v)$ -algebra, with v acting as 1. Tensoring $\mathbf{U}, \mathbf{U}^+, \mathbf{U}^-, \mathbf{U}^0$ with \mathbf{Q} over $\mathbf{Q}(v)$ we obtain the \mathbf{Q} -algebras $U_{\mathbf{Q}}, U_{\mathbf{Q}}^+, U_{\mathbf{Q}}^-, U_{\mathbf{Q}}^0$.

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

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

We shall denote the subalgebra $\mathbf{U}^0 \mathbf{U}^+$ of \mathbf{U} by $\mathbf{U}^{\geq 0}$. We have a direct sum decomposition $\mathbf{U}^{\geq 0} = \bigoplus_{\mathbf{j}} \mathbf{U}_{\mathbf{j}}^{\geq 0}$ where, by definition, $\mathbf{U}_{\mathbf{j}}^{\geq 0} = \mathbf{U}^0 \cdot \mathbf{U}_{\mathbf{j}}^+$.

2. THE U-MODULE M

2.1. Let \mathbf{M} be the $\mathbf{Q}(v)$ -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 \mathbf{M} by

$$\begin{aligned} E_i X_\alpha &= [h] X_{\alpha + \alpha_i} \\ \text{if } \alpha + \alpha_i \in R, \alpha \in R, \dots, \alpha - (h-1)\alpha_i \in R, \alpha - h\alpha_i \notin R \quad (h \geq 1), \\ E_i X_{-\alpha_i} &= t_i, \quad E_i X_\alpha = 0 \quad \text{for all other } \alpha \in R, \\ E_i t_i &= (v^{d_i} + v^{-d_i}) X_{\alpha_i}, \quad E_i t_j = [-a_{ji}] X_{\alpha_i} \quad \text{if } i \neq j. \\ F_i X_\alpha &= [h] X_{\alpha - \alpha_i} \\ \text{if } \alpha - \alpha_i \in R, \alpha \in R, \dots, \alpha + (h-1)\alpha_i \in R, \alpha + h\alpha_i \notin R \\ (h \geq 1), \\ F_i X_{\alpha_i} &= t_i, \quad F_i X_\alpha = 0 \quad \text{for all other } \alpha \in R, \\ F_i t_i &= (v^{d_i} + v^{-d_i}) X_{-\alpha_i}, \quad F_i t_j = [-a_{ji}] X_{-\alpha_i} \quad \text{if } i \neq j, \\ K_i X_\alpha &= v^{d_i \langle \check{\alpha}_i, \alpha \rangle} X_\alpha, \quad K_i t_k = t_k. \end{aligned}$$

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

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

3. BRAID GROUP ACTION ON U

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

$$\begin{aligned} T_i E_i &= -F_i K_i, \\ T_i E_j &= \sum_{r+s=-a_{ij}} (-1)^r v^{-d_{is}} E_i^{(r)} E_j E_i^{(s)} \quad \text{if } i \neq j, \\ T_i F_i &= -K_i^{-1} E_i, \\ T_i F_j &= \sum_{r+s=-a_{ij}} (-1)^r v^{d_{is}} F_i^{(s)} F_j F_i^{(r)} \quad \text{if } i \neq j, \\ T_i K_j &= K_j K_i^{-a_{ij}}. \end{aligned}$$

It commutes with Ω 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 \mathbf{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 \mathbf{U} .*

These results are proved by computations which will be omitted.

4. A BASIS OF \mathbf{U}

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

$$\mathbf{U}^- \otimes \mathbf{U}^0 \otimes \mathbf{U}^+ \cong \mathbf{U};$$

moreover, the monomials $K^\varphi = \prod_i K_i^{\varphi(i)}$ (with φ running over all functions $[1, n] \rightarrow \mathbf{Z}$) form a basis for \mathbf{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 \mathbf{N}^{R^+} be the set of all functions $R^+ \rightarrow \mathbf{N}$. We fix a total order on R^+ and define for any $\psi, \psi' \in \mathbf{N}^{R^+}$:

$$E^\psi = \prod_{\beta \in R^+} T_{w_\beta}(E_{i_\beta}^{(\psi(\beta))}), \quad F^{\psi'} = \Omega(E^{\psi'}),$$

where the factors in E^ψ are written in the given order of R^+ .

PROPOSITION 4.2. *The elements E^ψ (resp. $F^{\psi'}$) form a basis of the $\mathbf{Q}(v)$ -vector space \mathbf{U}^+ (resp. \mathbf{U}^-). Hence the elements $F^{\psi'} K^\varphi E^\psi$ for various ψ, ψ', φ as above, form a basis of the $\mathbf{Q}(v)$ -vector space \mathbf{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 α appears in any $\beta \in R^+$ (expressed as \mathbf{N} -linear combination of simple roots) is ≤ 1 . A simple root $\alpha \in \Pi$ is said to be *semispecial* if the coefficient with which α appears in any $\beta \in R^+$ is ≤ 1 , except for a single root β , 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 Π) has been, so far, arbitrary. We say that this numbering is *good* if for any $i \in [1, n]$, α_i is special or semispecial when considered as a simple root of the root system $R \cap (\mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_i)$. 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 $\beta = \sum_{j=1}^i c_{ij} \alpha_j$ with $c_{ij} \geq 0$, $c_{ii} > 0$. We then set $g(\beta) = i$, $c_\beta = c_{ii}$. Let $R_i^+ = \{\beta \in R^+ \mid g(\beta) = i\}$.

We define $h' : R_i^+ \rightarrow \mathbf{Q}$ by $h'(\beta) = c_\beta^{-1}$ height (β) (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 $R^+ \rightarrow [1, n]$, $(\beta \rightarrow i_\beta)$ such that the following three properties hold. First, $s_{i_\alpha}, s_{i_\beta}$ commute in W whenever α, β are in the same box; hence, for any box B , the product of all s_α with $\alpha \in B$ is a well defined element $s(B) \in W$, independent of the order of factors. Second, we have $i_{\alpha_j} = j$. Finally, if $\beta \in R_i^+$ and B_1, \dots, B_k are the boxes in R_i^+ preceding strictly β , in increasing order (for \leq), then $s(B_1) \cdots s(B_k)(\alpha_{i_\beta}) = \beta$; 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_β, w_β just defined and we obtain a basis of \mathbf{U} which is independent of the choice of order; it depends only on the choice of good numbering. Note also that the function $\beta \rightarrow w_\beta$ considered above does not coincide with that in [8, 3.5]; however, it leads to the same basis of \mathbf{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 \mathbf{U} :

$$\begin{aligned} E_2, T_2(E_1), T_2 T_1(E_2) & \text{ if } \mu = 1, \\ E_2, T_2(E_1), T_2 T_1(E_2), T_2 T_1 T_2(E_1) & \text{ if } \mu = 2, \\ E_2, T_2(E_1), T_2 T_1(E_2), T_2 T_1 T_2(E_1), \\ T_2 T_1 T_2 T_1(E_2), T_2 T_1 T_2 T_1 T_2(E_1) & \text{ if } \mu = 3. \end{aligned}$$

(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_μ) :

$$\begin{aligned} (a1) \quad & E_2, E_{12}, E_1 \\ (a2) \quad & E_2, E_{12}, E_{112}, E_1, \\ (a3) \quad & E_2, E_{12}, E_{11122}, E_{112}, E_{1112}, E_1. \end{aligned}$$

(The subscripts correspond to the various positive roots; for example, 11122 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 $(a\mu)$ for $N \in \mathbb{N}$; they are defined as $E^N/[N]_d!$ 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 $\mu = 1$, we have

$$\begin{aligned} E_{12}E_2 &= v^{-d}E_2E_{12}, & E_1E_{12} &= v^{-d}E_{12}E_1, \\ E_1E_2 &= v^dE_2E_1 + v^dE_{12} \end{aligned}$$

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

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

If $\mu = 3$, we have

$$\begin{aligned} E_{12}E_2 &= v^{-3}E_2E_{12}, & E_{11122}E_{12} &= v^{-3}E_{12}E_{11122}, \\ E_{112}E_{11122} &= v^{-3}E_{11122}E_{112}, \\ E_{1112}E_{112} &= v^{-3}E_{112}E_{1112}, & E_1E_{1112} &= v^{-3}E_{1112}E_1, \\ E_{11122}E_2 &= v^{-3}E_2E_{11122} + (v^{-1} - v)(v^{-2} - v^2)E_{12}^{(3)}, \\ E_{112}E_{12} &= v^{-1}E_{12}E_{112} + v^{-1}[3]E_{11122}, \\ E_{1112}E_{11122} &= v^{-3}E_{11122}E_{1112} + (v^{-1} - v)(v^{-2} - v^2)E_{12}^{(3)}, \\ E_1E_{112} &= v^{-1}E_{112}E_1 + v^{-1}[3]E_{1112}, \\ E_{112}E_2 &= E_2E_{112} + v(v^{-2} - v^2)E_{12}^{(2)}, \\ E_{1112}E_{12} &= E_{12}E_{1112} + v(v^{-2} - v^2)E_{112}^{(2)}, \\ E_1E_{11122} &= E_{11122}E_1 + v(v^{-2} - v^2)E_{112}^{(2)}, \\ E_{1112}E_2 &= v^3E_2E_{1112} + (-v^4 - v^2 + 1)E_{11122} \\ &\quad + (v^2 - v^4)E_{12}E_{112}, \\ E_1E_{12} &= vE_{12}E_1 + v[2]E_{112}, & E_1E_2 &= v^3E_2E_1 + v^3E_{12}. \end{aligned}$$

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:

$$\begin{aligned} \text{(a)} \quad & E_{12}^{(r)} E_2^{(s)} = v^{-drs} E_2^{(s)} E_{12}^{(r)}, \\ \text{(b)} \quad & E_1^{(r)} E_{12}^{(s)} = v^{-drs} E_{12}^{(s)} E_1^{(r)}, \\ \text{(c)} \quad & E_1^{(k)} E_2^{(k')} = \sum_{\substack{r \geq 0, s \geq 0 \\ r+s=k' \\ s+t=k}} v^{d(tr+s)} E_2^{(r)} E_{12}^{(s)} E_1^{(t)}. \end{aligned}$$

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

$$\begin{aligned} \text{(d)} \quad & E_{12}^{(r)} E_2^{(s)} = v^{-2rs} E_1^{(s)} E_{12}^{(r)}, \\ \text{(e)} \quad & E_{112}^{(r)} E_{12}^{(s)} = v^{-2rs} E_{12}^{(s)} E_{112}^{(r)}, \\ \text{(f)} \quad & E_1^{(r)} E_{112}^{(s)} = v^{-2rs} E_{112}^{(s)} E_1^{(r)}, \\ \text{(g)} \quad & E_{112}^{(k)} E_2^{(k')} \\ &= \sum_{\substack{r \geq 0, s \geq 0, t \geq 0 \\ r+s=k' \\ s+t=k}} v^{-2sr-2st+2s} \left(\prod_{i=1}^s (v^{2-4i} - 1) \right) E_2^{(r)} E_{12}^{(2s)} E_{112}^{(t)}, \\ \text{(h)} \quad & E_1^{(k)} E_{12}^{(k')} = \sum_{\substack{r \geq 0, s \geq 0, t \geq 0 \\ r+s=k' \\ s+t=k}} v^{-sr-st+s} \left(\prod_{i=1}^s (v^{2i} + 1) \right) E_{12}^{(r)} E_{112}^{(s)} E_1^{(t)}, \\ \text{(i)} \quad & E_1^{(k)} E_2^{(k')} = \sum_{\substack{r \geq 0, s \geq 0, t \geq 0, u \geq 0 \\ r+s+t=k' \\ s+2t+u=k}} v^{2ru+2rt+us+2s+2t} E_2^{(r)} E_{12}^{(s)} E_{112}^{(t)} E_1^{(u)}. \end{aligned}$$

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

$$\text{(a1)} \quad E_1^{(k)} E_2^{(k')} = \sum v^{f(p,q,r,s,t,u)} E_2^{(p)} E_{12}^{(q)} E_{112}^{(r)} E_{1112}^{(s)} E_{1112}^{(t)} E_1^{(u)},$$

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

$$\begin{aligned} f(p, q, r, s, t, u) \\ &= 3up + 2uq + 3ur + us + 6tp + 3tq + 3tr \\ &\quad + 3sp + sq + 3rp + 3q + 6r + 4s + 3t. \end{aligned}$$

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

$$\begin{aligned} \text{(a2)} \quad & E_1 E_2^{(k')} = v^{3k'} E_2^{(k')} E_1 + v^3 E_2^{(k'-1)} E_{12}, \\ \text{(a3)} \quad & E_1 E_{12}^{(k')} = v^{k'} E_{12}^{(k')} E_1 + v(v + v^{-1}) E_{12}^{(k'-1)} E_{112} \\ &\quad + v^{2-k'} (v^2 + 1 + v^{-2}) E_{12}^{(k'-2)} E_{1112} \end{aligned}$$

$$\begin{aligned}
 \text{(a4)} \quad E_1 E_{112}^{(k')} &= v^{-k'} E_{112}^{(k')} E_1 + v^{-2k'+1} (v^2 + 1 + v^{-2}) E_{112}^{(k'-1)} E_{1112}, \\
 \text{(a5)} \quad E_1 E_{11122}^{(k')} &= E_{11122}^{(k')} E_1 + v^{-3k'+2} (1 - v^4) E_{11122}^{(k'-1)} E_{112}^{(2)}, \\
 \text{(a6)} \quad E_1^{(k)} E_2 &= v^{3k} E_2 E_1^{(k)} + v^{2k+1} E_{12} E_1^{(k-1)} \\
 &\quad + v^{k+2} E_{112} E_1^{(k-2)} + v^3 E_{1112} E_1^{(k-3)}, \\
 \text{(a7)} \quad E_{11122}^{(k)} E_2 &= v^{-3k} E_2 E_{11122}^{(k)} + v^{-6k+3} (v^2 - 1) (v^4 - 1) E_{12}^{(3)} E_{11122}^{(k-1)}, \\
 \text{(a8)} \quad E_{112}^{(k)} E_2 &= E_2 E_{112}^{(k)} + v^{-2k+2} (v^{-3} - v^3) E_{12} E_{11122} E_{112}^{(k-2)} \\
 &\quad + v^{-3k+6} (v^{-6} - v^6) E_{11122}^{(2)} E_{112}^{(3)} \\
 &\quad + v^{-k+2} (v^{-2} - v^2) E_{12}^{(2)} E_{112}^{(k-1)}, \\
 \text{(a9)} \quad E_{1112}^{(k)} E_2 &= v^{3k} E_2 E_{1112}^{(k)} + (-v^4 - v^2 + 1) E_{11122} E_{1112}^{(k-1)} \\
 &\quad + (v^2 - v^4) E_{12} E_{112} E_{1112}^{(k-1)} \\
 &\quad + v^{-3k+6} (v^2 - 1) (v^4 - 1) E_{112}^{(3)} E_{1112}^{(k-2)}, \\
 \text{(a10)} \quad E_{112}^{(k)} E_{12} &= v^{-k} E_{12} E_{112}^{(k)} + v^{-2k-1} (1 + v^2 + v^4) E_{11122} E_{112}^{(k-1)}, \\
 \text{(a11)} \quad E_{1112}^{(k)} E_{12} &= E_{12} E_{1112}^{(k)} + v^{-3k+4} (v^{-2} - v^2) E_{112}^{(2)} E_{1112}^{(k-1)}.
 \end{aligned}$$

5.5. We have:

$$E_{12}^{(k)} = \sum_{t=0}^k (-1)^{k-t} v^{-d_{2t}} E_2^{(k-t)} E_1^{(t)} E_2^{(t)}.$$

Furthermore, $E_{12}^{(k)}$ (when $\mu = 1$), $E_{112}^{(k)}$ (when $\mu = 2$) and $E_{1112}^{(k)}$ (when $\mu = 3$) are given by:

$$\sum_{k=0}^{d_{2k'}} (-1)^{d_{2k'}-k} v^{-k} E_1^{(k)} E_2^{(k')} E_1^{(d_{2k'}-k)}.$$

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 μ) belong to U^+ . This follows from 5.5 for all elements except for E_{112} , E_{11122} 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 $v^{4q} E_{112}^{(q)} - E_{112}^{(2q)} E_2^{(q)}$ is a sum of terms of form $u_1 E_{11122}^{(b)} E_{112}^{(c)} u_2$ with $b \leq q/2$, $c < q$, while $v^{6p} E_{11122}^{(p)} - E_{11122}^{(3p)} E_2^{(2p)}$ is a sum of terms of form $u_3 E_{11122}^{(b_1)} E_{112}^{(c_1)} u_4$ with $b_1 < p$, $c_1 \leq 3p/2$; 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^ψ 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 $\mathbf{Q}(v)$ -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, section 2, Lemma 8]).

We define a lexicographic order on \mathbf{N}^6 as follows. If $\mathbf{n} = (n_1, \dots, n_6)$, $\mathbf{n}' = (n'_1, \dots, n'_6)$ belong to \mathbf{N}^6 , we say that $\mathbf{n} < \mathbf{n}'$ 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 $\mathbf{n} \leq \mathbf{n}'$ if $\mathbf{n} < \mathbf{n}'$ or $\mathbf{n} = \mathbf{n}'$.

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

$$\begin{pmatrix} 1 & \cdots & 1 & 3 & \cdots & 3 & 2 & \cdots & 2 & 3 & \cdots & 3 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & \cdots & 1 & 1 & \cdots & 1 & 2 & \cdots & 2 & 1 & \cdots & 1 & 1 & \cdots & 1 \end{pmatrix}$$

which contains n_1 columns $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, n_2 columns $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$, n_3 columns $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$, n_4 columns $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$, n_5 columns $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and n_6 columns $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. (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:

$$\begin{aligned} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &\Rightarrow \emptyset; & \begin{pmatrix} 3 \\ 1 \end{pmatrix} &\Rightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix} \right\}; \\ \begin{pmatrix} 2 \\ 1 \end{pmatrix} &\Rightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\}; & \begin{pmatrix} 3 \\ 2 \end{pmatrix} &\Rightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix} \right\}; \\ \begin{pmatrix} 1 \\ 1 \end{pmatrix} &\Rightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}; & \begin{pmatrix} 0 \\ 1 \end{pmatrix} &\Rightarrow \emptyset. \end{aligned}$$

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

(We leave the easy verification to the reader.) Recall from 1.6 that $\mathbf{U}^{\geq 0}$ has been decomposed in a direct sum of subspaces $\mathbf{U}_{\mathbf{j}}^{\geq 0}$ indexed by pairs \mathbf{j} of natural numbers. It will be convenient to write such a pair as a column $\mathbf{j} = \begin{pmatrix} j_1 \\ j_2 \end{pmatrix}$. A vector in the subspace $\mathbf{U}_{\mathbf{j}}^{\geq 0}$ is said to have degree \mathbf{j} . If $\alpha \in R^+$, then

the degree \mathbf{j} of E_α is well defined; it is one of $\binom{1}{0}, \binom{3}{1}, \binom{2}{1}, \binom{3}{2}, \binom{1}{1}, \binom{0}{1}$ and we have:

ASSERTION B. (i) $\Delta(E_\alpha) = E_\alpha \otimes 1 + \kappa_\alpha \otimes E_\alpha$ plus a sum of terms of form $u_1 \otimes u_2$ where $u_1, u_2 \in \mathbf{U}^{\geq 0}$ have well-defined degrees and the degree of u_2 is subordinate to \mathbf{j} . (κ_α is a monomial in K_1, K_2 .) (ii) $\Delta^{[N]}(E_\alpha) \in (\mathbf{U}^{\geq 0})^{\otimes N}$ is equal to the sum over $k \in [1, N]$ of the terms (said to be principal) $K \otimes \cdots \otimes K \otimes E_\alpha \otimes 1 \cdots \otimes 1$ with K a fixed monomial in K_1, K_2 , and E_α in the k th position, plus a sum of terms (said to be subordinate) of form $u_1 \otimes \cdots \otimes u_{h-1} \otimes u_h \otimes 1 \otimes \cdots \otimes 1$, where u_1, \dots, u_h are elements of $\mathbf{U}^{\geq 0}$ with well-defined degrees and the degree of u_h is subordinate to \mathbf{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 \mathbf{N} . Then L defines a subspace $\mathbf{U}_{\mathbf{j}^1}^{\geq 0} \otimes \cdots \otimes \mathbf{U}_{\mathbf{j}^N}^{\geq 0}$ of $(\mathbf{U}^{\geq 0})^{\otimes N}$, where $\mathbf{j}^1, \dots, \mathbf{j}^N$ are the first, \dots , N th 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 $(\mathbf{U}^{\geq 0})^{\otimes N}$. Let $\mathbf{n}, \mathbf{n}' \in \mathbf{N}^6$ be such that $\sum_j n_j = \sum_j n'_j = N$. Let $E(\mathbf{n}) = E_1^{n_1} E_{1112}^{n_2} E_{112}^{n_3} E_{11122}^{n_4} \times E_{12}^{n_5} E_2^{n_6} \in \mathbf{U}^{\geq 0}$. Let $\tau_{\mathbf{n}, \mathbf{n}'}$ be the projection of $\Delta^{[N]}(E(\mathbf{n}))$ onto the subspace of vectors of multidegree $L(\mathbf{n}')$ (in the direct sum decomposition above).

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

Let $E((\mathbf{n})) \in (\mathbf{U}^{\geq 0})^{\otimes N}$ be defined as $x_1 \otimes \cdots \otimes x_N$, where $x_k = E_1$ for $k \in S_1(\mathbf{n})$, $x_k = E_{1112}$ for $k \in S_2(\mathbf{n})$, $x_k = E_{112}$ for $k \in S_3(\mathbf{n})$, $x_k = E_{11122}$ for $k \in S_4(\mathbf{n})$, $x_k = E_{12}$ for $k \in S_5(\mathbf{n})$, $x_k = E_2$ for $k \in S_6(\mathbf{n})$. Let $c(\mathbf{n}) = [n_1]_3! [n_2]_3! [n_3]_3! [n_4]_3! [n_5]_3! [n_6]_3! \in \mathcal{A}$.

ASSERTION C. (i) If $\tau_{\mathbf{n}, \mathbf{n}'} \neq 0$, then $\mathbf{n} \leq \mathbf{n}'$.

(ii) For $\mathbf{n} = \mathbf{n}'$ we have

$$\tau_{\mathbf{n}, \mathbf{n}} = c(\mathbf{n}) v^f \kappa E((\mathbf{n}));$$

here f is some integer, $\kappa = \kappa_1 \otimes \cdots \otimes \kappa_N$ and κ_j are certain monomials in K_1, K_2 .

Since $\Delta^{[N]}$ is an algebra homomorphism, we can express $\Delta^{[N]}(E(\mathbf{n}))$ as a product of factors $\Delta^{[N]}(E_\alpha)$; each of these factors can be written as a sum of terms as in Assertion A(ii). Let us select one such term ξ_k in the k th factor such

that the product $\xi_1 \cdots \xi_N$ is non-zero, of multidegree $L(\mathbf{n}')$. (Then $\tau_{\mathbf{n}, \mathbf{n}'}$ is the sum of all such products). Let Λ_k be the multidegree of ξ_k . We have $\sum_k \Lambda_k = L(\mathbf{n}')$. We can apply Assertion A (its assumptions are satisfied by Assertion B(ii)). Assertion C(i) follows; moreover, in the case where $\mathbf{n} = \mathbf{n}'$, it follows that the terms ξ_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 $t(\alpha) = E_\alpha X_{-\alpha}$, ($\alpha \in R^+$). Then $t(\alpha)$ is an indivisible element of the \mathcal{A} -lattice M .*

Indeed, we have $t(\alpha_1) = t_1$, $t(3\alpha_1 + \alpha_2) = v^{-1}t_1 - t_2$, $t(2\alpha_1 + \alpha_2) = -v^{-2}[2]t_1 + [3]t_2$, $t(3\alpha_1 + 2\alpha_2) = -v^{-5}t_1 + v^{-3}[2]t_2$, $t(\alpha_1 + \alpha_2) = v^{-3}t_1 - [3]t_2$, $t(\alpha_2) = t_2$.

Assume that there exists an element $u \in U^+$ which is a $\mathbf{Q}(v)$ linear combination of basis elements E^ψ 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 $u' = \sum_{\mathbf{n}} b(\mathbf{n}, u')E(\mathbf{n})$ with $b(\mathbf{n}, u') \in \mathbf{Q}(v)$. Using our assumption and the fact that $\Psi(U^+) = U^+$ we see that $b(\mathbf{n}, u') \notin c(\mathbf{n})^{-1}\mathcal{A}$ for some \mathbf{n} , where $u' = \Psi(u)$. Moreover, we can choose \mathbf{n} so that we also have $b(\mathbf{n}', u') \in c(\mathbf{n}')^{-1}\mathcal{A}$ for all $\mathbf{n}' < \mathbf{n}$. Let $u'' = u' - \sum_{\mathbf{n}' < \mathbf{n}} b(\mathbf{n}', u')E(\mathbf{n}')$. Then $u'' \in U^+$, $b(\mathbf{n}, u'') \notin c(\mathbf{n})^{-1}\mathcal{A}$, $b(\mathbf{n}', u'') = 0$ for all $\mathbf{n}' < \mathbf{n}$. Let $N = n_1 + \cdots + n_6$. In the U -module $M^{\otimes N}$ (see 2.3) we consider the elements $X(\mathbf{n}) = x_1 \otimes \cdots \otimes x_N$, $t(\mathbf{n}) = y_1 \otimes \cdots \otimes y_N$, where $x_k = X_{-\alpha_1}$, $y_k = t(\alpha_1)$ for $k \in S_1(\mathbf{n})$; $x_k = X_{-3\alpha_1 - \alpha_2}$, $y_k = t(3\alpha_1 + \alpha_2)$ for $k \in S_2(\mathbf{n})$; $x_k = X_{-2\alpha_1 - \alpha_2}$, $y_k = t(2\alpha_1 + \alpha_2)$ for $k \in S_3(\mathbf{n})$; $x_k = X_{-3\alpha_1 - 2\alpha_2}$, $y_k = t(3\alpha_1 + 2\alpha_2)$ for $k \in S_4(\mathbf{n})$; $x_k = X_{-\alpha_1 - \alpha_2}$, $y_k = t(\alpha_1 + \alpha_2)$ for $k \in S_5(\mathbf{n})$; $x_k = X_{-\alpha_1}$, $y_k = t(\alpha_1)$ for $k \in S_6(\mathbf{n})$. Let \mathbf{M}_0 (resp. M_0) be the $\mathbf{Q}(v)$ - (resp. \mathcal{A} -) submodule of \mathbf{M} (resp. M) generated by t_1, t_2 . Consider the projection $\mathbf{M} \rightarrow \mathbf{M}_0$ which takes t_i to t_i ($i = 1, 2$) and all other basis elements to zero. Taking a tensor power, we get a $\mathbf{Q}(v)$ -linear projection $\mathbf{M}^{\otimes N} \rightarrow \mathbf{M}_0^{\otimes N}$ which is denoted by π . We have clearly $\pi(M^{\otimes N}) \subset M_0^{\otimes N}$. In particular,

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

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

$$\pi(E(\mathbf{n}'')X(\mathbf{n})) = \pi(\tau_{\mathbf{n}'', \mathbf{n}}X(\mathbf{n})).$$

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

$$\begin{aligned} \pi(u''X(\mathbf{n})) &= b(\mathbf{n}, u'')\pi(E(\mathbf{n})X(\mathbf{n})) = b(\mathbf{n}, u'')\pi(\tau_{\mathbf{n}, \mathbf{n}}X(\mathbf{n})) \\ &= b(\mathbf{n}, u'')c(\mathbf{n})v^f E((\mathbf{n}))X(\mathbf{n}) = b(\mathbf{n}, u'')c(\mathbf{n})v^f t(\mathbf{n}), \end{aligned}$$

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

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

$$(a) \quad e_1, e_2, e_3, \dots, e_v$$

(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 $k, k' \in \mathbf{N}$ we have

$$(b) \quad e_j^{(k)} e_i^{(k')} = \sum_{\xi} c_{\xi, i, j, k, k'} e_i^{(\xi(i))} e_{i+1}^{(\xi(i+1))} \dots e_j^{(\xi(j))}$$

where ξ runs over all maps of the interval $\{z \in \mathbf{N} : i \leq z \leq j\}$ to \mathbf{N} , and all but finitely many of the coefficients $c_{\xi, i, j, k, k'} \in \mathbf{Q}(v)$ 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) $V_v^+(d_1, d_2)$ with generators $e_i^{(N)} (1 \leq i \leq v, N \in \mathbf{N})$ with $e_i^{(0)} = 1$ for all i and relations given by (b) above and

$$(c) \quad e_i^{(N)} e_i^{(M)} = \begin{bmatrix} M + N \\ N \end{bmatrix}_d e_i^{(M+N)}$$

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 $v \rightarrow v^{-1}$ 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

$$\begin{aligned} V_v^+(d_1, d_2) &\rightarrow U^+, & V_v^{+*}(d_1, d_2) &\rightarrow U^+, \\ V_v^-(d_1, d_2) &\rightarrow U^-, & V_v^{-*}(d_1, d_2) &\rightarrow U^-; \end{aligned}$$

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 $X \otimes \mathbf{Q}$ such that $R_p = R \cap P$ generates P over \mathbf{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.

$$(a) \quad R_P^+ = \{\alpha, \alpha_i\} \quad \text{with } i < g(\alpha),$$

$$(b) \quad R_P^+ = \{\alpha, \alpha + \alpha_i, \alpha_i\} \quad \text{with } i < g(\alpha),$$

$$(c) \quad R_P^+ = \{\alpha', \alpha' + \alpha, \alpha\} \quad \text{with } h'(\alpha) = l, h'(\alpha') = l + 1,$$

$$h'(\alpha' + \alpha) = \frac{2l + 1}{2}, \quad g(\alpha) = g(\alpha'),$$

$$(d) \quad R_P^+ = \{\alpha, \alpha + \alpha_i, \alpha + 2\alpha_i, \alpha_i\} \quad \text{with } i < g(\alpha)$$

$$(e) \quad R_P^+ = \{\alpha_j, \alpha_j + \alpha, \alpha_j + 2\alpha, \alpha\}$$

$$\text{with } h'(\alpha) = l, h'(\alpha_j + 2\alpha) = \frac{2l + 1}{2}, j < g(\alpha)$$

$$(f) \quad R_P^+ = \{\alpha_j, \alpha_i + \alpha_j, 3\alpha_i + 2\alpha_j, 2\alpha_i + \alpha_j, 3\alpha_i + \alpha_j, \alpha_i\}.$$

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 α is in the W -orbit of α_k .

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

$$(a) \quad E_\alpha^{(N)} \quad (\alpha \in R^+, N \in \mathbf{N})$$

with $E_\alpha^{(0)} = 1$. For each admissible plane P (see 6.1) we impose a set of relations among the generators $E_{\alpha[1]}^{(N_1)}, E_{\alpha[2]}^{(N_2)}, \dots, E_{\alpha[v]}^{(N_v)}$ (where the subscripts are the elements of R_P^+ 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 $V_v^+(d', d'')$. If P is as in 6.1(c), (e), these generators are required to satisfy the relations of the algebra $V_v^{+*}(d', d'')$. (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

$$(a) \quad F_\alpha^{(N)} \quad (\alpha \in R^+, N \in \mathbf{N})$$

with $F_\alpha^{(0)} = 1$. For each admissible plane P we impose a set of relations among the generators $F_{\alpha[1]}^{(N_1)}, F_{\alpha[2]}^{(N_2)}, \dots, F_{\alpha[v]}^{(N_v)}$ (where the subscripts are the elements of R_P^+ 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 $V_v^-(d', d'')$. If P is as in 6.1(c), (e), these generators are required to satisfy the relations of the algebra $V_v^{-*}(d', d'')$. (Here, (d', d'') is as in 6.1.)

6.4. We define an \mathcal{A} -algebra V^0 (with 1) by generators and relations as follows. The generators are:

$$(a) \quad K_i, K_i^{-1}, \begin{bmatrix} K_i; c \\ t \end{bmatrix} \quad (i \in [1, n], c \in \mathbf{Z}, t \in \mathbf{N}).$$

The relations are:

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

$$(b2) \quad K_i K_i^{-1} = 1, \quad \begin{bmatrix} K_i; c \\ 0 \end{bmatrix} = 1,$$

$$(b3) \quad \begin{bmatrix} K_i; 0 \\ t \end{bmatrix} \begin{bmatrix} K_i; -t \\ t' \end{bmatrix} = \begin{bmatrix} t+t' \\ t \end{bmatrix}_{d_i} \begin{bmatrix} K_i; 0 \\ t+t' \end{bmatrix}, \quad (t, t' \geq 0),$$

$$(b4) \quad \begin{bmatrix} K_i; c \\ t \end{bmatrix} - v^{-d_i t} \begin{bmatrix} K_i; c+1 \\ t \end{bmatrix} = -v^{-d_i(c+1)} K_i^{-1} \begin{bmatrix} K_i; c \\ t-1 \end{bmatrix}, \quad (t \geq 1),$$

$$(b5) \quad (v^{d_i} - v^{-d_i}) \begin{bmatrix} K_i; 0 \\ 1 \end{bmatrix} = K_i - K_i^{-1}.$$

6.5. Let V be the \mathcal{A} -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:

$$(a1) \quad E_{\alpha_i}^{(N)} F_{\alpha_j}^{(M)} = F_{\alpha_j}^{(M)} E_{\alpha_i}^{(N)} \quad \text{if } i \neq j$$

$$(a2) \quad E_{\alpha_i}^{(N)} F_{\alpha_i}^{(M)} = \sum_{t \geq 0, t \leq N, t \leq M} F_{\alpha_i}^{(M-t)} \begin{bmatrix} K_i; 2t - N - M \\ t \end{bmatrix} E_{\alpha_i}^{(N-t)},$$

$$(a3) \quad K_i^{\pm 1} E_{\alpha_j}^{(N)} = v^{\pm d_i a_{ij} N} E_{\alpha_j}^{(N)} K_i^{\pm 1},$$

$$(a4) \quad K_i^{\pm 1} F_{\alpha_j}^{(N)} = v^{\mp d_i a_{ij} N} F_{\alpha_j}^{(N)} K_i^{\pm 1},$$

$$(a5) \quad \begin{bmatrix} K_i; c \\ t \end{bmatrix} E_{\alpha_j}^{(N)} = E_{\alpha_j}^{(N)} \begin{bmatrix} K_i; c + N a_{ij} \\ t \end{bmatrix},$$

$$(a6) \quad \begin{bmatrix} K_i; c \\ t \end{bmatrix} F_{\alpha_j}^{(N)} = F_{\alpha_j}^{(N)} \begin{bmatrix} K_i; c - N a_{ij} \\ t \end{bmatrix}.$$

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

THEOREM 6.6. (i) *There are unique homomorphisms of \mathcal{A} -algebras with the indicated properties:*

$$(a) \quad V^+ \rightarrow U^+(E_{\alpha_i}^{(N)} \rightarrow E_i^{(N)} \quad \forall i, N)$$

- (b) $V^- \rightarrow U^-(F_{\alpha_i}^{(N)} \rightarrow F_i^{(N)} \quad \forall i, N)$
- (c) $V \rightarrow U (E_{\alpha_i}^{(N)} \rightarrow E_{\alpha_i}^{(N)}, F_{\alpha_i}^{(N)} \rightarrow F_i^{(N)}, K_i^{\pm 1} \rightarrow K_i^{\pm 1} \quad \forall i, N)$

These are actually algebra isomorphisms.

- (ii) The braid group action on U restricts to a braid group action on U .
- (iii) Under (a) and (c), $E_{\beta}^{(N)}$ is carried to $T_{w_{\beta}}(E_{\beta}^{(N)})$ for all $\beta \in R^+$, (notations of 4.3). Similarly, under (b) and (c), $F_{\beta}^{(N)}$ is carried to $T_{w_{\beta}}(F_{\beta}^{(N)})$ for all $\beta \in R^+$.
- (iv) The obvious homomorphism $V^0 \rightarrow V$ composed with (c) is an injective algebra homomorphism

(d) $V^0 \rightarrow U$.

(Compare [8, 4.3, 4.5, 4.7].) We shall identify $V^+ = U^+$, $V^- = U^-$, $V = U$ using (a), (b), (c) above. We also identify V^0 with a subalgebra of U , denoted U^0 , using (d). In particular, we have well defined elements

$$E_{\beta}^{(N)} \in U^+, \quad F_{\beta}^{(N)} \in U^-(\beta \in R^+), \quad \begin{bmatrix} K_i; c \\ t \end{bmatrix} \in U^0.$$

We have

$$\begin{bmatrix} K_i; c \\ t \end{bmatrix} = \prod_{s=1}^t \frac{K_i v^{d_i(c-s+1)} - K_i^{-1} v^{d_i(-c+s-1)}}{v^{d_i s} - v^{-d_i s}}.$$

THEOREM 6.7. (i) *The elements*

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

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

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

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 $\mathbf{Q}(v)$ -basis of U . Hence the natural homomorphism

$$U \otimes \mathbf{Q}(v) \rightarrow U$$

is an isomorphism of $\mathbf{Q}(v)$ -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 \mathbf{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 $r \in \mathbf{N}$ such that for any $i \in [1, n]$ we have $\prod_{h=-r}^r (K_i - v^{di^h}) \in I$.

Let $\mathcal{A}_0 = \mathbf{Q}[v, v^{-1}]$ 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 $\mathbf{Q}(v)$ -linear maps $U \rightarrow \mathbf{Q}(v)$ and let \mathbf{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 $U_{\mathcal{A}_0} \rightarrow \mathcal{A}_0$ and let $O = \mathbf{O} \cap U_{\mathcal{A}_0}^*$. (We identify $U_{\mathcal{A}_0}^*$ with a subset of U^* , using 6.7.) We can regard \mathbf{O} (resp. O) as a Hopf algebra over $\mathbf{Q}(v)$ (resp. \mathcal{A}_0): as in *loc. cit.* we define product and coproduct in \mathbf{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 $U_{\mathcal{A}_0}/I_0 \rightarrow \text{End}_{\mathcal{A}_0}(\mathcal{L})$. 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 \mathbf{U} -module L generated by a highest weight vector is simple. Let L_0 be the $U_{\mathcal{A}_0}$ -submodule of L generated by x . This coincides with the $U_{\mathcal{A}_0} \cap \mathbf{U}^-$ -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 \mathcal{A}_0 -modules of finite rank and that the natural homomorphism $Q(v) \otimes_{\mathcal{A}_0} L_0 \rightarrow L$ 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 $O \subset \mathbf{O}$ induces an isomorphism of Hopf algebras over $\mathbf{Q}(v)$

$$O \otimes_{\mathcal{A}_0} \mathbf{Q}(v) \cong \mathbf{O}.$$

We call \mathbf{O} the quantum coordinate algebra and O its \mathcal{A}_0 -form.

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

7.5. The definition of \mathbf{O} in terms of matrix coefficients of finite dimensional \mathbf{U} -modules is suggested by Drinfeld in [2], where he describes \mathbf{O} in type A_n ; for further results on \mathbf{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 \mathbf{B} be the quotient ring of $\mathbf{Q}[v, v^{-1}]$ by the ideal generated by the l th cyclotomic polynomial. We denote the image of v in \mathbf{B} again by v . Then v has order l in \mathbf{B} .

Let l_i be the order of v^{2d_i} in \mathbf{B} (a divisor of l). For any $\alpha \in R^+$ we set $l_\alpha = l_i$

where α_i is in the W -orbit of α . We regard \mathbf{B} as an \mathcal{A} -algebra via the natural homomorphism $\mathcal{A} \rightarrow \mathbf{B}$, taking v to v , and we form the \mathbf{B} -algebras $U_{\mathbf{B}} = U \hat{\otimes}_{\mathcal{A}} \mathbf{B}$, $U_{\mathbf{B}}^+ = U^+ \otimes_{\mathcal{A}} \mathbf{B}$, $U_{\mathbf{B}}^- = U^- \otimes_{\mathcal{A}} \mathbf{B}$, $U_{\mathbf{B}}^0 = U^0 \otimes_{\mathcal{A}} \mathbf{B}$. The generators of U are mapped by the canonical homomorphism $U \rightarrow U_{\mathbf{B}}$ to generators of $U_{\mathbf{B}}$ denoted by the same letters. Similar conventions apply to the other algebras.

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

THEOREM 8.3. (i) *The elements F (resp. E) with $F \in U_{\mathbf{B}}^-$, $E \in U_{\mathbf{B}}^+$ as in 6.7(b), (a), satisfying respectively $N_{\alpha} < l_{\alpha}$, $N'_{\alpha} < l_{\alpha}$, $\forall \alpha \in R^+$, form a \mathbf{B} -basis of \mathbf{u}^+ (resp. \mathbf{u}^-).*

- (ii) *The elements $K = \prod_{i=1}^n K_i^{N_i}$ ($0 \leq N_i \leq 2l_i - 1$) form a \mathbf{B} -basis of \mathbf{u}^0 .*
- (iii) *The elements $FK E$ with F, E as in (i), K as in (ii), form a \mathbf{B} -basis of \mathbf{u} .*
- (iv) *In particular,*

$$\dim_{\mathbf{B}} \mathbf{u} = 2^n \prod_{i=1}^n l_i \prod_{\alpha \in R^+} l_{\alpha}^2.$$

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 \mathcal{A} -algebra U^+). Assume that the exponents k, k' in the left-hand side of that relation satisfy: $k < l_1$ if j is even, $k < l_2$ if j is odd, $k' < l_1$ if i is even, $k' < l_2$ if i is odd. Then the exponents $\zeta(h)$, ($i \leq h \leq j$) in the right-hand side satisfy the analogous inequality $\zeta(h) < l_1$ if h is even, $\zeta(h) < l_2$ if h is odd, at least when the coefficient $c(\zeta, i, j, k, k')$ is non-zero as an element of \mathbf{B} . (In other words, if we regard the relation 5.8(b) over \mathbf{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 \mathcal{A} but zero in \mathbf{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 \mathbf{u}_1 be the \mathbf{B} -subspace of $U_{\mathbf{B}}^+$ spanned by the elements E in (i). It is sufficient to show that \mathbf{u}_1 is stable under left and right multiplication by a set of algebra generators of \mathbf{u}^+ .

This can be easily checked using the commutation formulas in 5.4. (Note that we can take as algebra generators for \mathfrak{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 $l_\alpha = l$ for all $\alpha \in R^+$. Let δ_i (resp. δ'_i) be the derivation of the algebra $U_{\mathbf{B}}$ defined by $\delta_i(x) = E_i^{(l)}x - xE_i^{(l)}$ (resp. $\delta'_i(x) = F_i^{(l)}x - xF_i^{(l)}$).

LEMMA 8.5. (i) δ_i leaves \mathfrak{u} and \mathfrak{u}^+ stable.

(ii) δ'_i leaves \mathfrak{u} and \mathfrak{u}^- stable.

This is trivial for $l = 1$. Assume now that $l > 1$. Then the algebra \mathfrak{u}^+ (resp. \mathfrak{u}^-) is generated by the elements E_i (resp. F_i) for $1 \leq i \leq n$; moreover, the algebra \mathfrak{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:

$$\begin{aligned}\delta_i(E_j) &= \sum_{\substack{h > 0 \\ h \leq -a_{ij}}} \begin{bmatrix} -a_{ij} \\ h \end{bmatrix} E_i^{(h)} E_j E_i^{(l-h)} \quad \text{if } a_{ji} = -1, \\ \delta_i(E_j) &= -E_i^{(l-1)} E_j E_i \quad \text{if } a_{ij} = -1, \\ \delta_i(F_i) &= \begin{bmatrix} K_i & 1 \\ & 1 \end{bmatrix} E_i^{(l-1)}\end{aligned}$$

and δ_i maps the generators F_j ($j \neq i$), E_i and $K_i^{\pm 1}$ to 0. Similarly,

$$\begin{aligned}\delta'_i(F_j) &= - \sum_{\substack{h > 0 \\ h \leq -a_{ij}}} \begin{bmatrix} -a_{ij} \\ h \end{bmatrix} F_i^{(l-h)} F_j F_i^{(h)} \quad \text{if } a_{ji} = -1, \\ \delta'_i(F_j) &= F_i F_j F_i^{(l-1)} \quad \text{if } a_{ij} = -1, \\ \delta'_i(E_i) &= -F_i^{(l-1)} \begin{bmatrix} K_i & 1 \\ & 1 \end{bmatrix}\end{aligned}$$

and δ'_i maps the generators E_j ($j \neq i$), F_i and $K_i^{\pm 1}$ to 0. (These formulas follow from the results for rank 2 in Section 5.)

LEMMA 8.6. *There is a unique \mathbf{B} -algebra homomorphism $\psi: U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B} \rightarrow U_{\mathbf{B}}^+$ which takes E_i to $E_i^{(l)}$ 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 $U_{\mathbf{B}}^+$:

$$\begin{aligned} E_1^{(3l-h)} E_2^{(l)} E_1^{(hl)} &= \sum_{\substack{r+s+t=l \\ s+2t+u'=3l-hl}} E_2^{(r)} E_{12}^{(s)} E_{112}^{(t)} E_1^{(u')} E_1^{(hl)} \\ &= \sum_{\substack{r+s+t=l \\ s+2t+u=3l}} \begin{bmatrix} u \\ hl \end{bmatrix} E_2^{(r)} E_{12}^{(s)} E_{112}^{(t)} E_2^{(u)} \end{aligned}$$

($0 \leq h \leq 3$); we use the convention that $\begin{bmatrix} m \\ m' \end{bmatrix} = 0$ if $0 \leq m < m'$. Let

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

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

$$\sum_{h=0}^3 (-1)^h \begin{bmatrix} u \\ hl \end{bmatrix} = 0$$

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

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

An entirely similar argument shows that

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

This proves the lemma in the case where $u = 2$. The proof in the case where $u = 1$ or 3 is entirely similar.

8.7. Consider the **B**-vector space $\mathcal{V}^+ = (U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B}) \otimes_{\mathbf{B}} \mathbf{u}^+$. We identify $U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B}$ (resp. \mathbf{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 $U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B}$ (an enveloping algebra of a nilpotent Lie algebra) and on \mathbf{u}^+ , and is such that

$$E_i \cdot y = y \cdot E_i + \delta_i(y)$$

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

LEMMA 8.8. γ is an isomorphism of algebras.

The image of γ contains $E_i, E_i^{(l)}$ for all i . These elements generate $U_{\mathbf{B}}^+$ as an algebra. Hence, γ is surjective. For any $\mathbf{j} \in \mathbf{N}^n$, let $U_{\mathbf{j}}^+$ be the intersection of U^+ with $U_{\mathbf{j}}^+$ (see 1.6). We have a direct sum decomposition $U^+ = \bigoplus_{\mathbf{j}} U_{\mathbf{j}}^+$. Tensoring with \mathbf{B} or with \mathbf{Q} we get direct sum decompositions $U_{\mathbf{B}}^+ = \bigoplus_{\mathbf{j}} (U_{\mathbf{B}}^+)_{\mathbf{j}}$ and $U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B} = \bigoplus_{\mathbf{j}} (U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B})_{\mathbf{j}}$.

Let $\mathbf{u}_{\mathbf{j}}^+$ be the intersection of \mathbf{u}^+ with $(U_{\mathbf{B}}^+)_{\mathbf{j}}$ and let

$$\mathcal{V}_{\mathbf{j}}^+ = \bigoplus_{\substack{\mathbf{j}, \mathbf{j}' \\ \mathbf{j} + \mathbf{j}' = \mathbf{j}}} (U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B})_{\mathbf{j}'} \otimes \mathbf{u}_{\mathbf{j}}^+.$$

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

LEMMA 8.9. *There is a unique \mathbf{B} -algebra homomorphism $U_{\mathbf{B}}^+ \rightarrow U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B}$ which takes each $E_i^{(N)}$ to $E_i^{(N/l)}$ if l divides N and to zero otherwise.*

The uniqueness is clear. We now prove the existence. Let $\pi: \mathbf{u}^+ \rightarrow \mathbf{B}$ 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 δ_i of \mathbf{u}^+ (see 8.5) map \mathbf{u}^+ into J^+ . It follows that the \mathbf{B} -linear map $\mathcal{V}^+ \rightarrow U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B}$ defined by $x \otimes y \rightarrow \pi(y)x$ is an algebra homomorphism. Composing it with the inverse of γ (see 8.8) we obtain an algebra homomorphism $U_{\mathbf{B}}^+ \rightarrow U_{\mathbf{Q}}^+ \otimes_{\mathbf{Q}} \mathbf{B}$ which has the required property. (If R has no components G_2 , one can give a more direct proof, using the defining relations of $U_{\mathbf{B}}^+$.)

THEOREM 8.10. *There is a unique \mathbf{B} -algebra homomorphism $\chi: U_{\mathbf{B}} \rightarrow U_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}$ such that $\chi(E_i^{(N)})$ is $E_i^{(N/l)}$ if l divides N and is zero otherwise; $\chi(F_i^{(N)})$ is $F_i^{(N/l)}$ 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 χ on $U_{\mathbf{B}}^+$, by 8.9 and, by symmetry, also on $U_{\mathbf{B}}^-$. We define $\chi: U_{\mathbf{B}}^0 \rightarrow U_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}$ by $\chi(K_i^{\pm 1}) = K_i^{\pm 1}$, $\chi \begin{bmatrix} K_i; 0 \\ N \end{bmatrix} = \begin{bmatrix} K_i; 0 \\ N/l \end{bmatrix}$ if l divides N and $\chi \begin{bmatrix} K_i; 0 \\ N \end{bmatrix} = 0$, otherwise. It is easy to check that these maps extend to the whole of $U_{\mathbf{B}}$ as an algebra homomorphism. (We use the presentation of $U_{\mathbf{B}}$ 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 $U_{\mathbf{B}}, U_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}, \mathbf{u}$. It is easy to check that χ 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 $U_{\mathbf{B}}, U_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}, \mathbf{u}$, and one verifies that χ in 8.10 is compatible with these braid group actions. It follows that, for any $\alpha \in R^+$, χ takes $E_{\alpha}^{(N)}$ to $E_{\alpha}^{(N/l)}$ if l divides N and to zero, otherwise; it takes $F_{\alpha}^{(N)}$ to $F_{\alpha}^{(N/l)}$ if l divides N and to zero, otherwise. It follows that the kernel of χ is precisely the subspace \mathcal{I} of $U_{\mathbf{B}}$ spanned by the basis elements FKE with F, K, E as in 6.7(b), (c), (a), such that at least one of the exponents $N_{\alpha}, N'_{\alpha}, t_i$ 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 $\mathcal{A} \rightarrow \mathcal{B}$, 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 $\chi_{\mathcal{B}}: U_{\mathcal{B}} \rightarrow U_{\mathbf{Z}} \otimes \mathcal{B}$ which is given by the same formulas as χ in 8.10.*

The uniqueness is clear. For the existence, define $\chi_{\mathcal{B}}$ as the restriction of χ 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 \mathbf{F}_p as a \mathcal{B} -algebra with v acting as 1. Applying the functor $\otimes_{\mathcal{B}} \mathbf{F}_p$, $U_{\mathbf{Z}} \otimes \mathcal{B}$ becomes $U_{\mathbf{F}_p}$ (by the definition 1.5), $U_{\mathcal{B}}$ becomes $U_{\mathbf{F}_p}$ (exactly as in [8, §6]) and $\chi_{\mathcal{B}}$ becomes the \mathbf{F}_p -algebra homomorphism $\chi_p: U_{\mathbf{F}_p} \rightarrow U_{\mathbf{F}_p}$ defined by the same formulas as χ in 8.10.

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

In this sense, we may regard χ 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 $U_{\mathbf{Q}}$ by the ideal generated by the central elements $K_1 - 1, \dots, K_n - 1$ is denoted $\bar{U}_{\mathbf{Q}}$. This is the classical enveloping algebra corresponding to the semisimple Lie algebra over \mathbf{Q} with the given Cartan matrix. Composing the obvious homomorphism $U_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B} \rightarrow \bar{U}_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}$ with χ , we obtain a surjective homomorphism $\chi': U_{\mathbf{B}} \rightarrow \bar{U}_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}$. (This homomorphism has been introduced, in the simply

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

$$\mathcal{I}' = \sum_{i=1}^n (K_i - 1)\mathcal{I}$$

where \mathcal{I} is as in 8.12. It is easy to see that \mathcal{I}' coincides with the two-sided ideal of $U_{\mathbf{B}}$ generated by the augmentation ideal of \mathbf{u} .

Hence the classical enveloping algebra $\bar{U}_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{B}$ may be regarded as the 'Hopf algebra quotient' of the Hopf algebra $U_{\mathbf{B}}$ by the finite dimensional Hopf subalgebra \mathbf{u} .

8.17. Let

$$O_{\mathbf{B}} = O \otimes_{\mathcal{A}_0} \mathbf{B}, \quad O_{\mathbf{Q}} = O \otimes_{\mathcal{A}_0} \mathbf{Q}.$$

Then $O_{\mathbf{Q}}$ may be regarded as the coordinate algebra of the simply connected semisimple group over \mathbf{Q} with the given Cartan matrix. The homomorphism χ induces by passage to dual, an imbedding of Hopf algebras over \mathbf{B} :

$$O_{\mathbf{Q}} \otimes \mathbf{B} \subset O_{\mathbf{B}}.$$

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 $s_{i_1} s_{i_2} \cdots s_{i_v}$ be a reduced expression of the longest element w_0 of W ; thus, $v = \#R^+$. We have a bijection $[1, v] \rightarrow R^+$ defined by

$$j \rightarrow s_{i_1} s_{i_2} \cdots s_{i_{j-1}}(\alpha_{i_j}).$$

We use this to totally order R^+ . If $\beta \in R^+$ corresponds to j , we set $w_{\beta} = s_{i_1} s_{i_2} \cdots s_{i_{j-1}}$ and $i_{\beta} = i_j$. We define

$$E_{\beta}^{(N)} = T_{w_{\beta}}(E_{i_{\beta}}^{(N)}) \in U^+, \quad F_{\beta}^{(N)} = T_{w_{\beta}}(F_{i_{\beta}}^{(N)}) \in U^-.$$

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 $s_{i_1} s_{i_2} \cdots s_{i_v}$ for w_0 and let U_2^+ be the

corresponding \mathcal{A} -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

1. Chevalley, C., 'Certains schémas de groupes semisimples', *Séminaire Bourbaki* (1961/62).
2. Drinfeld, V. G., 'Hopf algebras and the Yang-Baxter equation', *Soviet Math. Dokl.* **32** (1985), 254–258.
3. Jimbo, M., 'A q -difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation', *Lett. Math. Phys.* **10** (1985), 63–69.
4. Kostant, B., 'Groups over \mathbf{Z} ', *Proc. Symp. Pure Math.* **9** (1966), 90–98.
5. Lusztig, G., 'Quantum deformations of certain simple modules over enveloping algebras', *Adv. Math.* **70** (1988), 237–249.
6. Lusztig, G., 'Modular representations and quantum groups', *Contemp. Math.* **82** (1989), 59–77.
7. Lusztig, G., 'On quantum groups', *J. of Algebra* **128** (1990).
8. Lusztig, G., 'Finite dimensional Hopf algebras arising from quantum groups', *J. Amer. Math. Soc.* **3** (1990).
9. Rosso, M., 'Finite dimensional representations of the quantum analog of the enveloping algebra of a complex simple Lie algebra', *Comm. Math. Phys.* **117** (1988), 581–593.
10. Rosso, M., 'Analogues de la forme de Killing et du théorème d'Harish-Chandra pour les groupes quantiques', Preprint.
11. Steinberg, R., *Lectures on Chevalley Groups* (in Russian), Mir, Moscow, 1975.
12. Tanisaki, T., 'Finite dimensional representations of quantum groups', Preprint.

Author's address:

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

(Received, August 1, 1989)