JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 3, Number 1, January 1990

FINITE DIMENSIONAL HOPF ALGEBRAS ARISING FROM QUANTIZED UNIVERSAL ENVELOPING ALGEBRAS

GEORGE LUSZTIG

INTRODUCTION

0.1. An important role in the theory of modular representations is played by certain finite dimensional Hopf algebras $\bar{\mathfrak{u}}$ over F_p (the field with p elements, $p =$ prime). Originally, $\bar{\mathfrak{u}}$ was defined (Curtis [3]) as the restricted enveloping algebra of a "simple" Lie algebra over F_p.

For our purposes, it will be more convenient to define $\bar{\mathfrak{u}}$ as follows.

Let us fix an indecomposable positive definite symmetric Cartan matrix

$$\text{(a)} \qquad (a_{ij})_{1\le i,j\le n}.$$

In particular $a_{ii} = 2$ and $a_{ij} = a_{ji} \in \{0, -1\}$, for $i \neq j$. Let $\overline{U}_Q$ be the Q-algebra defined by the generators $\overline{E}_i$, $\overline{F}_i$, H_i $(1 \le i \le n)$, and the relations

$$\text{(b1)} \qquad H_iH_j = H_jH_i,$$

$$\text{(b2)} \qquad H_i\overline{E}_j - \overline{E}_jH_i = a_{ij}\overline{E}_j, \qquad H_i\overline{F}_j - \overline{F}_jH_i = -a_{ij}\overline{F}_j,$$

$$\text{(b3)} \qquad \overline{E}_i\overline{F}_j - \overline{F}_j\overline{E}_i = \delta_{ij}H_i,$$

$$\text{(b4)} \qquad \overline{E}_i\overline{E}_j = \overline{E}_j\overline{E}_i, \quad \overline{F}_i\overline{F}_j = \overline{F}_j\overline{F}_i, \quad \text{if } a_{ij} = 0,$$

(b5)

$$\overline{E}_i^2\overline{E}_j - 2\overline{E}_i\overline{E}_j\overline{E}_i + \overline{E}_j\overline{E}_i^2 = 0, \quad \overline{F}_i^2\overline{F}_j - 2\overline{F}_i\overline{F}_j\overline{F}_i + \overline{F}_j\overline{F}_i^2 = 0, \quad \text{if } a_{ij} = -1.$$

Then $\overline{U}_Q$ is known to be the enveloping algebra of the simple Lie algebra $\mathfrak{g}$ over Q corresponding to (a).

Chevalley [2] has proved that any $\overline{U}_Q$-module of finite dimension over Q admits a lattice which is stable under the subring $\overline{U}$ of $\overline{U}_Q$ generated by the $\overline{E}_i^{(N)} = \overline{E}_i^N/N!$ and $\overline{F}_i^{(N)} = \overline{F}_i^N/N!$ $(1 \le i \le n, N \ge 0)$, and Kostant [7] constructed a nice $\mathbb{Z}$-basis for $\overline{U}$.

Then $\bar{\mathfrak{u}}$ can be defined as the subring of $\overline{U} \otimes F_p = \overline{U}_{F_p}$ generated by the elements $\overline{E}_i^{(1)}$ and $\overline{F}_i^{(1)}$ $(1 \le i \le n)$. The pth powers of these generators are zero and in fact $\bar{\mathfrak{u}}$ is of finite dimension $(= p^{\dim \mathfrak{g}})$ over F_p.

Received by the editors May 3, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20G99.
Supported in part by National Science Foundation grant DMS 8702842.

0.2. From [3] it is known that the simple $\bar{\mathrm{u}}$-modules can be naturally parametrized by elements of $(\mathbb{Z}/p)^n$; but the structure of simple $\bar{\mathrm{u}}$-modules (e.g. their dimensions) is not known. From [3, 12] it is known that from the representation theory of $\bar{\mathrm{u}}$ one can recover essentially the whole rational representation theory of the simple algebraic group over $\overline{F}_p$ corresponding to (a_{ij}).

0.3. Let $\mathscr{B}$ be the ring $\mathbb{Z}/[\zeta]$, where ζ is a pth root of 1, $\zeta \neq 1$, p an odd prime; thus $\mathscr{B}$ is the ring of integers in a cyclotomic filed $\mathscr{B}'$. One of the main results of this paper is that $\bar{\mathrm{u}}$ can be regarded naturally as reduction modulo a maximal ideal of a Hopf algebra over $\mathscr{B}$. More precisely, we shall define a Hopf algebra $\tilde{\mathrm{u}}$ over $\mathscr{B}$ with the following properties.

(a) $\tilde{\mathrm{u}}$ is free of rank $p^{\dim \mathfrak{g}}$ as a $\mathscr{B}$-module.
(b) If $\mathbf{m}$ is the maximal ideal of $\mathscr{B}$ defined as the kernel of the ring homomorphism $\mathscr{B} \to F_p$ ($\zeta \to 1$, $z \to z \bmod p$, $z \in \mathbb{Z}$), then $\tilde{\mathrm{u}}/\mathbf{m}\tilde{\mathrm{u}} = \bar{\mathrm{u}} \otimes_{\mathscr{B}} F_p$ is isomorphic to $\bar{\mathrm{u}}$ as a Hopf algebra over F_p.
(c) The simple modules of the $\mathscr{B}'$-algebra $'\tilde{\mathrm{u}} = \tilde{\mathrm{u}}_{\mathscr{B}} \otimes \mathscr{B}'$ are naturally parametrized by elements of $(\mathbb{Z}/p)^n$; if M is such a simple module, then M contains some $\mathscr{B}$-lattice M_0 which is a $\tilde{\mathrm{u}}$-submodule and the corresponding $\tilde{\mathrm{u}}$-module $M_0/\mathbf{m}M_0$ has as a quotient the simple $\bar{\mathrm{u}}$-module with the same parameter (in $(\mathbb{Z}/p)^n$) as M.

In particular, the simple $'\tilde{\mathrm{u}}$-modules are in natural bijection with the simple $\bar{\mathrm{u}}$-modules so that the simple $\bar{\mathrm{u}}$-module corresponding to a simple $\tilde{\mathbf{u}}$-module M has dimension $\leq \dim M$.

We conjecture that the last inequality is an equality (at least for p not too small) and that in fact $\bar{\mathrm{u}}$ and $'\tilde{\mathrm{u}}$ have identical representation theories.

0.4. The definition of $\tilde{\mathrm{u}}$ is in the framework of the theory of quantum groups. Let v be an indeterminate and let $\mathscr{A} = \mathbb{Z}[v, v^{-1}]$, $\mathscr{A}' = Q(v)$ its quotient filed. Following Drinfel′d [4] and Jimbo [6] we define $U_{\mathscr{A}'}$ to be the $\mathscr{A}'$-algebra defined by the generators E_i, F_i, K_i, K_i^{-1} $(1 \leq i \leq n)$, and the relations

$$K_iK_j = K_jK_i, \qquad K_iK_i^{-1} = K_i^{-1}K_i = 1, \tag{a1}$$

$$K_iE_j = v^{a_{ij}}E_jK_i, \qquad K_iF_j = v^{-a_{ij}}F_jK_i, \tag{a2}$$

$$E_iF_j - F_jE_i = \delta_{ij}\frac{K_i - K_i^{-1}}{v - v^{-1}}, \tag{a3}$$

$$E_iE_j = E_jE_i, \qquad F_iF_j = F_jF_i, \qquad \text{if } a_{ij} = 0, \tag{a4}$$

$$\begin{gathered} E_i^2E_j - (v + v^{-1})E_iE_jE_i + E_jE_i^2 = 0, \\ F_i^2F_j - (v + v^{-1})F_iF_jF_i + F_jF_i^2 = 0, \\ \text{if } a_{ij} = -1. \end{gathered} \tag{a5}$$

(We adopt the notation in [9] which is slightly different from the original one.) Then $U_{\mathscr{A}'}$ is a Hopf algebra over $\mathscr{A}'$ with comultiplication $\Delta : U_{\mathscr{A}'} \to U_{\mathscr{A}'} \otimes U_{\mathscr{A}'}$ defined by

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

Following [8] we define U to be the $\mathscr{A}$-subalgebra of $U_{\mathscr{A}'}$ generated by the elements $E_i^{(N)} = E_i^N/[N]!$, $F_i^{(N)}/[N]!$, K_i, and K_i^{-1} $(1 \leq i \leq n,\ N \geq 0)$, where

$$\text{(c)} \qquad [N]! = \prod_{s=1}^{N} \frac{v^s - v^{-s}}{v - v^{-1}} \in \mathscr{A}.$$

We shall prove that U is a free $\mathscr{A}$-module and that U is itself a Hopf algebra over $\mathscr{A}$ in a natural way. We regard $\mathscr{B}$ as an $\mathscr{A}$-algebra with v acting as multiplication by ζ and we form $U_{\mathscr{B}} = U \otimes_{\mathscr{A}} \mathscr{B}$; this is a Hopf algebra over $\mathscr{B}$.

Now $\tilde{\mathrm{u}}$ is defined as the $\mathscr{B}$-subalgebra of $U_{\mathscr{B}}$ generated by the elements $E_i^{(1)}$, $F_i^{(1)}$, K_i, and K_i^{-1} $(1 \leq i \leq n)$ modulo the left (or two-sided) ideal generated by the central elements $K_1^p - 1, \dots, K_n^p - 1$. It has a natural Hopf algebra structure over $\mathscr{B}$ and it satisfies assertions (a)–(c) in §0.3.

The algebra $\tilde{\mathrm{u}} \otimes \mathbb{C}$ appears in the simplest case (type A_1) in the physics literature; see [14, 15].

0.5. We shall try to motivate the definition of U as follows. Consider the symmetric bilinear form $(\ ,\ )$ on $\mathbb{Z}^n$ (with canonical basis $\Pi = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$) given by $(\alpha_i, \alpha_j) = a_{ij}$.

Let $R = \{\alpha \in \mathbb{Z}^n | (\alpha, \alpha) = 2\}$. Then R is a root system in $\mathbb{Z}^n$ with set of simple roots Π.

Consider the free $\mathscr{A}$-module $\mathscr{M}$ with basis $\{X_\alpha\,(\alpha \in R),\ t_i (1 \leq i \leq n)\}$.

Define $\mathscr{A}$-linear maps $E_i, F_i : \mathscr{M} \to \mathscr{M}$ as follows:

$$\text{(a)} \qquad \begin{aligned} E_i X_\alpha &= X_{\alpha+\alpha_i} \quad \text{if } \alpha, \alpha + \alpha_i \in R, \\ F_i X_\alpha &= X_{\alpha-\alpha_i} \quad \text{if } \alpha, \alpha - \alpha_i \in R, \end{aligned}$$

$$\text{(b)} \qquad E_i X_{-\alpha_i} = t_i; \qquad F_i X_{\alpha_i} = t_i,$$

$$\text{(c)} \qquad \begin{aligned} E_i X_\alpha &= 0 \quad \text{if } \alpha \in R,\ \alpha + \alpha_i \notin R \cup 0; \\ F_i X_\alpha &= 0 \quad \text{if } \alpha \in R,\ \alpha - \alpha_i \notin R \cup 0, \end{aligned}$$

$$\text{(d)} \qquad E_i t_j = -a_{ij} X_{\alpha_i}, \quad F_i t_j = -a_{ij} X_{-\alpha_i} \quad \text{if } i \neq j,$$

$$\text{(e)} \qquad E_i t_i = (v + v^{-1}) X_{\alpha_i}, \qquad F_i t_i = (v + v^{-1}) X_{-\alpha_i}.$$

Consider $\overline{\mathscr{M}} = \mathscr{M} \otimes_{\mathscr{A}} \mathbb{Z}$, where $\mathbb{Z}$ is regarded as an $\mathscr{A}$-module with v acting as 1. Then $\overline{\mathscr{M}}$ inherits a basis $\{X_\alpha, t_i\}$ and E_i, F_i define endomorphisms

$\overline{E}_i, \overline{F}_i$ of $\overline{\mathscr{M}}$; these are defined by the same formulas as E_i, F_i except that (e) is replaced by

$$\overline{E}_i t_i = 2X_{\alpha_i}, \qquad \overline{F}_i t_i = 2X_{-\alpha_i}.$$

If we set $H_i = \overline{E}_i\overline{F}_i - \overline{F}_i\overline{E}_i$ we see that the endomorphisms $\overline{E}_i, \overline{F}_i$, and H_i of $\overline{\mathscr{M}}$ satisfy relations 0.1(b1)–(b5) of $\overline{U}_Q$. Hence $\overline{\mathscr{M}} \otimes Q$ is a $\overline{U}_Q$-module (it is the standard representation of $\overline{U}_Q$ on $\mathfrak{g}$). Now $\overline{E}_i$ and $\overline{F}_i$ act on $\overline{V}$ by matrices whose entries are in $\{0, 1, 2\}$. The simplest deformation of such a matrix is obtained by leaving the entries $0, 1$ unchanged and replacing 2 by $v + v^{-1}$; we thus obtain the endomorphisms E_i and F_i. If we define automorphisms $K_i : \mathscr{M} \to \mathscr{M}$ by $K_i X_\alpha = v^{(\alpha, \alpha_i)} X_\alpha$ $(\alpha \in R)$, $K_i t_j = t_j$, we see that, miraculously, the endomorphisms $E_i, F_i, K_i, K_i^{-1} : \mathscr{M} \to \mathscr{M}$ satisfy relations (a1)–(a5) in §0.4, hence they define a $U_{\mathscr{A}'}$-module structure on $\mathscr{M} \otimes_{\mathscr{A}} \mathscr{A}'$. Now E_i^2 maps $\mathscr{M}$ into $(v + v^{-1})\mathscr{M}$ hence $E_i^2/[2]!$ maps $\mathscr{M}$ into $\mathscr{M}$. This leads us to consider the $\mathscr{A}$-subalgebra U of $U_{\mathscr{A}'}$; it leaves $\mathscr{M}$ stable.

0.6. Consider the following three (unsolved) problems.

(a) Finding the characters of the finite dimensional simple modules of the algebraic group of $\overline{F}_p$ corresponding to (a_{ij}).

(b) Finding the characters of the finite dimensional simple modules over the quantum group corresponding to (a_{ij}) at $\sqrt[p]{1}$.

(c) Finding the characters of the simple highest weight modules of level $-p - h$ ($h =$ Coxeter number) over the affine Lie algebra corresponding to (a_{ij}).

It is expected that these three problems are very closely related. (See the conjectures in [10] as well as in [9].) The present paper is an attempt to relate problems (a) and (b).

0.7. We now review the contents of this paper in some detail. For several purposes it seems necessary to introduce in $U_{\mathscr{A}'}$ elements E_α and F_α corresponding to any positive root, generalizing E_i and F_i (which correspond to simple roots). (Such elements were introduced in type A by Jimbo.) If α is a sum $\alpha_i + \alpha_j$ of two simple roots one has two candidates $-E_iE_j + v^{-1}E_jE_i$ and $-E_jE_i + v^{-1}E_iE_j$ for E_α and, unlike the case $v + 1$, these two candidates are not even proportional to each other. For roots of height ≥ 3 there are even more candidates for E_α. This difficulty is unavoidable, but we manage to keep it under control by using a braid group action in $U_{\mathscr{A}'}$ introduced in [8]. This is explained in §1 in which the main result is the construction of a basis of Poincaré-Birkhoff-Witt type for $U_{\mathscr{A}'}$. In §2 we define an algebra V over $\mathscr{A}$, by generators and relations; after some combinational preparations in §3 we show in §4 that V is isomorphic to U.

In particular, this provides a presentation of U by generators and relations. We also construct an explicit $\mathscr{A}$-basis for U.

In §5 we study the specializations of U and $U_{\mathscr{A}'}$ in which v is taken to be of finite order. We also define in this context some finite dimensional Hopf algebras $'\mathfrak{u}$ over a cyclotomic field. We classify the simple modules of $'\mathfrak{u}$.

In §6 we establish a connection between quantum groups at $\sqrt[\ell]{1}$ and the algebras $\bar{\mathfrak{u}}$, and we verify the assertions given in §0.3.

0.8. The author wishes to thank Matthew Dyer for some helpful discussions.

1. The braid group action

1.1. Any root $\alpha \in R$ defines a reflection $s_\alpha : \mathbb{Z}^n \to \mathbb{Z}^n$, $z \to z - (z, \alpha)\alpha$. We shall write s_i instead of s_{α_i} $(1 \leq i \leq n)$. Let W be the Weyl group of R; it is the subgroup of $\mathrm{GL}(\mathbb{Z}^n)$ generated by the reflections s_i $(1 \leq i \leq n)$. Let $l(w)$ be the usual length function on W with respect to the generators $\{s_1, \dots, s_n\}$.

Let R^+ (resp. R^-) be the set of positive (resp. negative) roots in R with respect to the set of simple roots Π (see §0.5).

1.2. We define two Q-algebra isomorphisms $\Omega : U_{\mathscr{A}'} \xrightarrow{\approx} U_{\mathscr{A}'}^{\mathrm{opp}}$ and $\Psi : U_{\mathscr{A}'} \xrightarrow{\approx} U_{\mathscr{A}'}^{\mathrm{opp}}$ by

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

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

(Here $U_{\mathscr{A}'}^{\mathrm{opp}}$ is $U_{\mathscr{A}'}$ with the opposite multiplication.)

1.3. For any $i \in [1, n]$ there is a unique $\mathscr{A}'$-algebra isomorphism $T_i : U_{\mathscr{A}'} \xrightarrow{\approx} U_{\mathscr{A}'}$ such that

$$T_i(E_j) = \begin{cases} -F_jK_j, & \text{if } i = j, \\ E_j, & \text{if } a_{ij} = 0, \\ -E_iE_j + v^{-1}E_jE_i, & \text{if } a_{ij} = -1. \end{cases}$$

(a1) $$T_i(F_j) = \begin{cases} -K_j^{-1}E_j, & \text{if } i = j, \\ F_j, & \text{if } a_{ij} = 0, \\ -F_jF_i + vF_iF_j, & \text{if } a_{ij} = -1. \end{cases}$$

$$T_i(K_j) = \begin{cases} K_j^{-1}, & \text{if } i = j, \\ K_j, & \text{if } a_{ij} = 0, \\ K_iK_j, & \text{if } a_{ij} = -1. \end{cases}$$

Its inverse is given by

$$T_i^{-1}(E_j) = \begin{cases} -K_j^{-1}F_j, & \text{if } i=j, \\ E_j, & \text{if } a_{ij}=0, \\ -E_jE_i + v^{-1}E_iE_j, & \text{if } a_{ij}=-1. \end{cases}$$

(a2) $$T_i^{-1}(F_j) = \begin{cases} -E_jK_j, & \text{if } i=j, \\ F_j, & \text{if } a_{ij}=0, \\ -F_iF_j + vF_jF_i, & \text{if } a_{ij}=-1. \end{cases}$$

$$T_i^{-1}(K_j) = \begin{cases} K_j^{-1}, & \text{if } i=j, \\ K_j, & \text{if } a_{ij}=0, \\ K_iK_j, & \text{if } a_{ij}=-1. \end{cases}$$

Note that

(b) $$\Omega T_i = T_i\Omega \quad \text{for all } i.$$

We have

(c) $$T_iT_jT_i = T_jT_iT_j \quad \text{if } a_{ij}=-1, \qquad T_iT_j = T_jT_i \quad \text{if } a_{ij}=0.$$

Hence the T_i define a homomorphism of the braid group of W into the group of algebra automorphisms of $U_{\mathscr{A}'}$.

It follows that for any $w \in W$ there is a well-defined algebra isomorphisms $T_w : U \to U$ such that $T_w = T_{i_1}T_{i_2}\cdots T_{i_p}$ whenever $w = s_{i_1}s_{i_2}\cdots s_{i_p}$ with $p = l(w)$. From (b) it follows that

(d) $$\Omega T_w = T_w\Omega \quad \text{for all } w \in W.$$

We have $\Psi T_i = T_i^{-1}\Psi$ for all i. It follows that

(e) $$\Psi T_w = T_{w^{-1}}^{-1}\Psi \quad \text{for all } w \in W.$$

A simple computation shows that

(f) $$T_iT_jE_i = E_j, \quad T_iT_jF_i = F_j \quad \text{if } a_{ij}=-1.$$

1.4. We define Q-algebra automorphisms $\overline{T}_i : \overline{U}_Q \to \overline{U}_Q$ $(1 \le i \le n)$ by

$$\overline{T}_i\overline{E}_j = \begin{cases} -\overline{F}_j, \\ \overline{E}_j, \\ -\overline{E}_i\overline{E}_j + \overline{E}_j\overline{E}_i, \end{cases} \qquad \overline{T}_i\overline{F}_j = \begin{cases} -\overline{E}_j, & \text{if } i=j, \\ \overline{F}_j, & \text{if } a_{ij}=0, \\ -\overline{F}_j\overline{F}_i + \overline{F}_i\overline{F}_j, & \text{if } a_{ij}=-1. \end{cases}$$

We define Q-algebra automorphisms $\overline{T}_w : \overline{U}_Q \to \overline{U}_Q$ in terms of the $\overline{T}_i$ in the same way as the T_w were defined in terms of the T_i in §1.3. Note that $\overline{T}_w : \overline{U}_Q \to \overline{U}_Q$ is induced by an automorphism of the Lie algebra $\mathfrak{g}$. We have $\overline{T}_i^4 = 1$.

If $w \in W$ and $\alpha_i \in \Pi$ satisfy $w(a_i) \in R^+$, then $\overline{T}_w(\overline{E}_i)$ and $\overline{T}_w(\overline{F}_i)$ actually belong to $\mathfrak{g} \subset \overline{U}_Q$; more precisely they are root vectors in $\mathfrak{g}$ corresponding respectively to the root $w(\alpha_i)$, $-w(\alpha_i)$. They are completely determined (up to sign) by $w(\alpha_i)$.

1.5. Let $U^+_{\mathscr{A}'}$; U^+; $\overline{U}^+$ (resp. $U^-_{\mathscr{A}'}$; U^-; $\overline{U}^-$) be the $\mathscr{A}'$-, $\mathscr{A}$-, Q-subalgebra of $U_{\mathscr{A}'}$; U; $\overline{U}$ generated by the elements E_i; $E_i^{(N)}$, $N \geq 0$; $\overline{E}_i$ (resp. F_i; $F_i^{(N)}$, $N \geq 0$; $\overline{F}_i$). Let $\mathscr{R}$ be the Q-subalgebra of $\mathscr{A}'$ consisting of those $f \in \mathscr{A}'$ which have no pole at $v = 1$. Evaluation at 1 defines a Q-algebra homomorphism $\mathscr{R} \to Q$. Let $\mathscr{U}^+$ be the $\mathscr{R}$-algebra defined by the generators E_i $(1 \leq i \leq n)$ and the relations

$$E_iE_j = E_jE_i \quad \text{if } a_{ij} = 0, \qquad E_i^2E_j - (v+v^{-1})E_iE_jE_i + E_jE_i^2 = 0 \quad \text{if } a_{ij} = -1.$$

We have natural homomorphisms

(a) $$\mathscr{U}^+ \to U^+_{\mathscr{A}'} \qquad (E_i \longmapsto E_i),$$

(b) $$\mathscr{U}^+ \to \overline{U}_Q \qquad (E_i \longmapsto \overline{E}_i)$$

induced by $\mathscr{R} \subset \mathscr{A}'$, $\mathscr{R} \to Q$ respectively.

Lemma 1.6. *Consider the $\mathscr{A}'$-algebra with two generators A, B and relations*

$$A^2B - (v+v^{-1})ABA + BA^2 = 0, \qquad AB^2 - (v+v^{-1})BAB + B^2 = 0.$$

Set $C = -AB + v^{-1}BA$. Let $k, l, m \in \mathbb{N}$. Then

(a) $$AC = vCA, \qquad vBC = CB,$$

(b) $$\frac{B^k}{[k]!}\frac{A^l}{[l]!} = \sum_{\substack{j \geq 0 \\ j \leq k,\, j \leq l}} v^{j+(k-j)(l-j)} \frac{A^{l-j}}{[l-j]!}\frac{C^j}{[j]!}\frac{B^{k-j}}{[k-j]!},$$

(c) $$A^kB^{k+l}A^l = B^lA^{k+l}B^k \quad (\textit{compare Verma } [13]),$$

(d) $$\frac{C^m}{[m]!} = \sum_{j=0}^{m} (-1)^{m-j} v^{-j} \frac{B^j}{[j]!}\frac{A^m}{[m]!}\frac{B^{m-j}}{[m-j]!}.$$

Proof. The identities (a) are obvious. To prove (b) we can assume that $k, l \geq 1$. One first proves (b) for $l = 1$ and $k \geq 1$ by induction on k, then one uses induction on l. In (c), we replace $B^{k+l}A^l$ and B^lA^{k+l} by the expressions provided by (b); we find that both sides of (c) are equal to the same expression:

$$\sum_{j=0}^{l} \frac{[l]![k+l]!}{[j]![l-j]![k+l-j]!} v^{j+(k+l-j)(l-j)} A^{k+l-j}C^jB^{k+l-j}.$$

In the right-hand side of (d) we replace $\frac{B^j}{[j]!}\frac{A^m}{[m]!}$ by the expression provided by (b); we thus obtain the identity (d).

Proposition 1.7. *Let $w \in W$. Then $T_w(U) = U$.*

Proof. It is enough to show that $T_i(U) \subset U$ and $T_i^{-1}(U) \subset U$ for any $i \in [1, n]$. We have

(a) $T_i(E_j^{(N)}) = (-1)^N v^{N-N^2} F_j^{(N)} K_j^{(N)}, \quad T_i(F_j^{(N)}) = (-1)^N v^{-N+N^2} K_j^{-N} E_j^{(N)}$ if $i = j$,

(b) $$T_i(E_j^{(N)}) = E_j^{(N)}, \quad T_i(F_j^{(N)}) = F_j^{(N)} \quad \text{if } a_{ij} = 0,$$

(c) $$T_i(E_j^{(N)}) = \frac{1}{[N]!}(-E_iE_j + v^{-1}E_jE_i)^N = \sum_{l=0}^{N}(-1)^{N-l}v^{-l}E_j^{(l)}E_i^{(N)}E_j^{(N-l)} \quad \text{if } a_{ij} = -1$$

(using Lemma 1.6(a)) and, applying to this Ω (see §1.3(b)):

(d) $$\begin{aligned} T_i(F_j^{(N)}) &= \frac{1}{[N]!}(-F_jF_i + vF_iF_j)^N \\ &= \sum_{l=0}^{N}(-1)^{N-l}v^l F_j^{(N-l)}F_i^{(N)}F_j^{(l)} \quad \text{if } a_{ij} = -1. \end{aligned}$$

Since $T_i(K_j^{\pm 1})$ is $K_j^{\pm 1}$ or $K_i^{\pm 1}K_j^{\pm 1}$ it follows that $T_iU \subset U$. An entirely similar proof shows that $T_i^{-1}U \subset U$.

Proposition 1.8. *Let $w \in W$ and $\alpha_i \in \Pi$ be such that $w(\alpha_i) \in R^+$.*

(a) *We have $T_w(E_i^{(N)}) \in U^+$, $T_w(F_i^{(N)}) \in U^-(\forall N \geq 0)$.*
(b) *We have $T_w(\overline{E}_i) \in \overline{U}_Q^+$, $T_w(\overline{F}_i) \in \overline{U}_Q^-$.*
(c) *There exists $\tau \in \mathscr{U}^+$ which maps to $T_w(E_i) \in U_{\mathscr{A}'}^+$ under* 1.5(a) *and to $T_w(E_i) \in U_Q^+$ under* 1.5(b).
(d) *Assume, in addition, that $w(\alpha_i) = \alpha_k \in \Pi$. Then $T_w(E_i) = E_k$, $T_w(F_i) = F_k$.*

Proof. The method used in Dyer [5] to study the action of the Hecke algebra in the reflection representation can also be used in this case. We shall consider only the assertions concerning E_i; those concerning F_i are proved in the same way. All the assertions are trivial when $w = e$; therefore we may assume that $l(w) \geq 1$ and that our assertions hold for elements w' with $l(w') < l(w)$. We can find $j \in [1, n]$ such that $w(\alpha_j) \in R^-$; in particular, we have $i \neq j$. Let $\langle s_i, s_j \rangle$ be the dihedral subgroup generated by s_i and s_j, and let w' be the element of minimal length in the coset $w\langle s_i, s_j \rangle$. We have $w'(\alpha_i) > 0$ and $w'(\alpha_j) > 0$, and we are in one of the following three cases:

(1) $a_{ij} = 0$, $w = w's_j$, $l(w) = l(w') + 1$.
(2) $a_{ij} = -1$, $w = w's_is_j$, $l(w) = l(w') + 2$.
(3) $a_{ij} = -1$, $w = w's_j$, $l(w) = l(w') + 1$.

The induction hypothesis provides us with an element $\tau_i' \in \mathscr{U}^+$ (attached by (c) to w', α_i) and an element $\tau_j' \in \mathscr{U}^+$ (attached by (c) to w', α_j). Assume that we are in case (1). We have (using the induction hypothesis)

$$T_w(E_i^{(N)}) = T_{w'}T_j(E_i^{(N)}) = T_{w'}(E_i^{(N)}) \in U^+ \quad \text{(see Proposition 1.7(b))}.$$

Similarly, $\overline{T}_w(\overline{E}_i) = \overline{T}_{w'}(\overline{E}_i) \in \overline{U}_Q^+$. The element $\tau = \tau_i'$ satisfies (c).

Under the assumption of (d) we have $T_w(E_i) = T_{w'}(E_i) = E_k$, since $w'(\alpha_i) = \alpha_k$. Assume now that we are in case (2). We have (using the induction hypothesis)

$$\begin{aligned} T_w(E_i^{(N)}) &= T_{w'}T_iT_j(E_i^{(N)}) = T_{w'}(T_iT_j(E_i)^N)/[N]! \\ &= T_{w'}(E_j^N)/[N]! = T_{w'}(E_j^{(N)}) \in U^+ \quad \text{(see §1.3(f))}. \end{aligned}$$

Similarly, $\overline{T}_w(\overline{E}_i) = \overline{T}_{w'}(\overline{E}_j) \in \overline{U}_Q^+$. The element $\tau = \tau_j'$ satisfies (c).

Under the assumption of (d) we have $w'(\alpha_j) = ws_js_i(\alpha_j) = w(\alpha_i) = \alpha_k$, hence

$$T_w(E_i) = T_{w'}(E_j) = E_k.$$

Finally, assume that we are in case (3). We have using the induction hypothesis

$$\begin{aligned} T_w(E_i^{(N)}) &= T_{w'}T_j(E_i^{(N)}) \\ &= T_{w'}\left(\sum_l (-1)^{N-l}v^{-l}E_j^{(l)}E_i^{(N)}E_j^{(N-l)}\right) \\ &= \sum_l (-1)^{N-l}v^{-l}T_{w'}(E_j^{(l)})T_{w'}(E_i^{(N)})T_{w'}(E_j^{(N-l)}) \in U^+ \end{aligned}$$

(see Proposition 1.7(c)). In particular,

$$T_w(E_i) = -T_{w'}(E_j)T_{w'}(E_i) + v^{-1}T_{w'}(E_i)T_{w'}(E_j).$$

Similarly, we have $\overline{T}_w(\overline{E}_i) = -\overline{T}_{w'}(\overline{E}_j)\overline{T}_{w'}(\overline{E}_i) + \overline{T}_{w'}(\overline{E}_i)\overline{T}_{w'}(\overline{E}_j) \in \overline{U}_Q^+$.

The element $\tau = -\tau_j'\tau_i' + v^{-1}\tau_i'\tau_j'$ satisfies (c).

In case (3) we cannot have $w(\alpha_i) = \alpha_k$. If we had $w(\alpha_i) = \alpha_k$, then $\alpha_k = w's_j(\alpha_i) = w'(\alpha_i + \alpha_j) = w'(\alpha_i) + w'(\alpha_j)$; but $w'(\alpha_i)$ and $w'(\alpha_j)$ are positive roots, hence their sum cannot be in Π.

This completes the proof.

1.9. We choose for each $\beta \in R^+$ an element $w_\beta \in W$ such that for some index $i_\beta \in [1, n]$ we have

(a) $$w_\beta^{-1}(\beta) = \alpha_{i_\beta}.$$

Let $\mathbb{N}^{R^+}$ be the set of all functions $R^+ \to \mathbb{N}$. We fix a total order on R^+ and define for any $\psi \in \mathbb{N}^{R^+}$:

$$E^\psi = \prod_{\beta\in R^+} T_{w_\beta}(E_{i_\beta})^{\psi(\beta)}, \qquad \overline{E}^\psi = \prod_{\beta\in R^+} \overline{T}_{w_\beta}(\overline{E}_{i_\beta})^{\psi(\beta)},$$

$$F^\psi = \prod_{\beta\in R^+} T_{w_\beta}(F_{i_\beta})^{\psi(\beta)}, \qquad \prod_{\beta\in R^+} \overline{T}_{w_\beta}(\overline{F}_{i_\beta})^{\psi(\beta)},$$

where the factors in E^ψ, $\overline{E}^\psi$ (resp. F^ψ, $\overline{F}^\psi$) are written in the given (resp. opposite to the given) order of R^+. By Proposition 1.8, we have $E^\psi \in U^+_{\mathscr{A}'}$, $F^\psi \in U^-_{\mathscr{A}'}$, $\overline{E}^\psi \in \overline{U}^+_Q$, $\overline{F}^\psi \in \overline{U}^-_Q$.

Proposition 1.10. *The elements E^ψ (resp. F^ψ), for $\psi \in \mathbb{N}^{R^+}$, are linearly independent in the $\mathscr{A}'$-vector space $U^+_{\mathscr{A}'}$ (resp. $U^-_{\mathscr{A}'}$).*

Proof. Assume that in $U^+_{\mathscr{A}'}$ we have a relation of the form $\sum \lambda_\psi E^\psi = 0$, where $\lambda_\psi \in \mathscr{A}' - \{0\}$ and ψ runs over a finite nonempty set $\mathfrak{S}$ of $\mathbb{N}^{R^+}$. We will show that this leads to a contradiction. Multiplying by a power of $v-1$, we can assume that all λ_ψ are in $\mathscr{R} - \{0\}$ (see §1.5) and at least one of them does not vanish at $v = 1$. Using Proposition 1.8(c) we can choose for each $\psi \in \mathbb{N}^{R^+}$ an element $\tau_\psi \in \mathscr{U}^+$ such that τ_ψ maps to E^ψ under §1.5(a) and to $\overline{E}^\psi$ under §1.5(b).

Let $\hat{\tau} = \sum_{\psi\in\mathfrak{S}} \lambda_\psi \tau_\psi \in \mathscr{U}^+$. Then $\hat{\tau}$ maps to $0 \in U^+_{\mathscr{A}'}$ under §1.5(a). Choose an integer $\mu \geq 0$ such that $\psi(\beta) \leq \mu$ for all $\beta \in R^+$ and all $\psi \in \mathfrak{S}$.

From [8] we see that there exists a $U_{\mathscr{A}'}$-module M, of finite dimension over $\mathscr{A}'$, and an $\mathscr{R}$-lattice $M_0 \subset M$ with properties (a) and (b) below.

(a) $E_1, \dots, E_n, F_1, \dots, F_n, K_1, \dots, K_n$ leave M_0 stable and induce on $\overline{M} = M_0/(v-1)M_0$ operators $\overline{E}_1, \dots, \overline{E}_n, \overline{F}_1, \dots, \overline{F}_n, 1, \dots, 1$ which define a $\overline{U}_Q$-module structure on $\overline{M}$.

(b) The $\overline{U}_Q$-module $\overline{M}$ is simple and there exists a nonzero vector $y \in \overline{M}$ such that $\overline{E}_i y = 0$ and $H_i y = \mu y$ for $i = 1, \dots, n$.

From the representation theory of $\overline{U}_Q$ it is known that

(c) the elements $\overline{E}^\psi(y)$, with $\psi \in \mathbb{N}^{R^+}$ such that $0 \leq \psi(\beta) \leq \mu$ for all $\beta \in R^+$, form a Q-basis of $\overline{M}$.

By (a), M_0 is a $\mathscr{U}^+$-module via $\mathscr{U}^+ \to U^+_{\mathscr{A}'}$ given by §1.5(a). Hence $\hat{\tau}$ acts as 0 on M_0.

On the other hand, by the definition of $\hat{\tau}$ and by (a), $\hat{\tau}: M_0 \to M_0$ induces on $\overline{M}$ the operator $\sum_{\psi\in\mathfrak{S}} \lambda_\psi(1)\overline{E}^\psi$ from the $\overline{U}_Q$-action. (Here $\lambda_\psi(1)$ is the value of λ_ψ at $v = 1$.) Hence the last operator is zero. Applying it to $y \in \overline{M}$ and using (c), we deduce that $\lambda_\psi(1) = 0$ for all $\psi \in \mathfrak{S}$. This is a contradiction.

The statement concerning F^ψ follows from that for E^ψ, by using the involution Ω (see §1.3(d)).

1.11. Let $U^0_{\mathscr{A}'}$ be the subalgebra of $U_{\mathscr{A}'}$ generated by the elements K_i and K_i^{-1} $(1 \le i \le n)$. For $\phi = \sum_i \phi(i)\alpha_i = \mathbb{Z}^n$, we define

$$K^\phi = K_1^{\phi(1)} K_2^{\phi(2)} \cdots K_n^{\phi(n)} \in U^0_{\mathscr{A}'}.$$

Lemma 1.12 (Rosso [1]). (a) *Multiplication defines an $\mathscr{A}'$-vector space isomorphism $U^-_{\mathscr{A}'} \otimes_{\mathscr{A}'} U^0_{\mathscr{A}'} \otimes_{\mathscr{A}'} U^+_{\mathscr{A}'} \xrightarrow{\approx} U_{\mathscr{A}'}$.*

(b) *The elements K^ϕ $(\phi \in \mathbb{Z}^n)$ form and $\mathscr{A}'$-basis of $U^0_{\mathscr{A}'}$.*

Proposition 1.13. *The elements $F^{\psi'} K^\phi E^\psi$ $(\psi, \psi' \in \mathbb{N}^{R^+}, \phi \in \mathbb{Z}^n)$ form an $\mathscr{A}'$-basis of $U_{\mathscr{A}'}$.*

Proof. The linear independence follows from Lemma 1.12 and Proposition 1.10. We also see that it is enough to show that the elements E^ψ $(\psi \in \mathbb{N}^{R^+})$ generate $U^+_{\mathscr{A}'}$ as an $\mathscr{A}'$-vector space. (The analogous statement for $U^-_{\mathscr{A}'}$ is proved in the same way.)

Let $\overline{\mathscr{U}}^+$ be the Q-algebra defined by the generators $\overline{E}_1, \dots, \overline{E}_n$ and the relations $\overline{E}_i\overline{E}_j = \overline{E}_j\overline{E}_i$ if $a_{ij} = 0$ and $\overline{E}_i^2\overline{E}_j - 2\overline{E}_i\overline{E}_j\overline{E}_i + \overline{E}_j\overline{E}_i^2 = 0$ if $a_{ij} = -1$. For $k \in \mathbb{N}$, let $\overline{\mathscr{U}}^+_k$ (resp. $\mathscr{U}^+_k$, $\mathscr{U}^+_{\mathscr{A}',k}$) be the subspace of $\overline{\mathscr{U}}^+$, (resp $\mathscr{U}^+$, $\mathscr{U}^+_{\mathscr{A}'}$) spanned by the products of $\overline{E}_1, \dots, \overline{E}_n$ (resp. $E_1, \dots, E_n$) involving exactly k factors.

It is clear that $\overline{\mathscr{U}}^+ = \bigoplus_{k\ge 0} \overline{\mathscr{U}}^+_k$ and $\mathscr{U}^+ = \bigoplus_{k \ge 0} \mathscr{U}^+_k$ (by the homogeneity of the defining relations.)

Clearly, $\mathscr{U}^+_k$ is an $\mathscr{R}$-module of finite type. Since $\mathscr{R}$ is a discrete valuation domain, we see that

(a) $$\dim_Q(\mathscr{U}^+_k \otimes_{\mathscr{R}} Q) \ge \dim_{Q(v)} \mathscr{U}^+_k \otimes_{\mathscr{R}} \mathscr{A}',$$

where Q is regarded as an $\mathscr{R}$-module with v acting as 1. Let

$$\mathscr{P}_k = \left\{ \psi \in \mathbb{N}^{R^+} \,\middle|\, \sum_{\beta \in R^+} \psi(\beta) h(\beta) = k \right\},$$

where $h : \mathbb{Z}^n \to \mathbb{Z}$ is given by the sum of coordinates.

Now $\overline{\mathscr{U}}^+$ is the enveloping algebra of a Lie algebra. From the Poincaré-Birkhoff-Witt theorem, we see that

(b) $$\dim_Q \overline{\mathscr{U}}^+_k = \#(\mathscr{P}_k) \qquad (k \ge 0).$$

It is clear that $\overline{\mathscr{U}}^+ = \mathscr{U}^+ \otimes_{\mathscr{R}} Q$ and this is compatible with the grading. Using this and (b), we see that

(c) $$\dim_Q \mathscr{U}^+_k \otimes_{\mathscr{R}} Q = \#(\mathscr{P}_k).$$

The obvious (surjective) homomorphism $\mathscr{U}^+ \to U^+_{\mathscr{A}'}$ induces a surjective $\mathscr{A}'$-linear map $\mathscr{U}^+_k \otimes \mathscr{A}' \longrightarrow U^+_{\mathscr{A}',k}$. It follows that

(d) $$\dim_{\mathscr{A}'}(\mathscr{U}^+_k \otimes \mathscr{A}') \ge \dim_{\mathscr{A}'} U^+_{\mathscr{A}',k} \ge \#(\mathscr{P}_k)$$

(the last inequality follows from the linear independence of the elements E^{ψ} ($\psi \in \mathscr{P}_k$) in $U_{\mathscr{A}'}$, proved in Proposition 1.10). Combining (d), (a), and (c) we see that all these inequalities must be equalities. It follows that the elements E^{ψ} ($\psi \in \mathscr{P}_k$) span the $\mathscr{A}'$-vector space $U^+_{\mathscr{A}',k}$, hence they form an $\mathscr{A}'$-basis of $U^+_{\mathscr{A}',k}$. The proposition follows.

2. THE ALGEBRA V

2.1. In this section we shall introduce and study an $\mathscr{A}$-algebra V defined by generators and relations. Eventually (§4) this algebra will be identified with U.

We shall need the following notation. For any integers m, r with $r \geq 0$ we define the Gaussian binomial coefficient

$$\begin{bmatrix} m \\ r \end{bmatrix} = \prod_{s=1}^{r} \frac{v^{m-s+1} - v^{-m+s-1}}{v^s - v^{-s}} \in \mathscr{A}.$$

If $m \geq r \geq 0$, we have $\left[\begin{smallmatrix} m \\ r \end{smallmatrix}\right] = [m]!/[r]![m-r]!$, while if $r > m \geq 0$ we have $\left[\begin{smallmatrix} m \\ r \end{smallmatrix}\right] = 0$.

We shall assume that the numbering of the $\alpha_i \in \Pi$ is

(a) that of [1, Planches I, V, VI, VII] for types A_n, E_6, E_7, E_8,
(b) that of [1, Planche V] composed with $i \to n+1-i$ for type D_n.

2.2. Let $\alpha \in R^+$. We can write uniquely $\alpha = c_i\alpha_i +$ (linear combination of α_j, $j < i$) with $c_i \geq 1$; we then set $i = g(\alpha)$ and $c_\alpha = c_i$. By our choice of numbering we have

(a) $c_\alpha = 1$, except when α is the highest root of E_8 in which case $g(\alpha) = 8$ and $c_\alpha = 2$.

Let $h(\alpha)$ be the height of α (the sum of coefficients of the various α_h in α), and let $h'(\alpha) = c_\alpha^{-1} h(\alpha)$. From (a), we see that $h'(\alpha)$ is integral (and equal to $h(\alpha)$) in all cases except when α is the highest root of E_8, when $h'(\alpha) = 29/2$. We call $h'(\alpha)$ the level of α.

We shall write $R^+_{i,l} = \{\alpha \in R^+ | g(\alpha) = i,\ h'(\alpha) = l\}$.

2.3. We shall consider the set consisting of the following variables:

(a) $$E_\alpha^{(N)} \quad (\alpha \in R^+,\ N \geq 0),$$

(b) $$F_\alpha^{(N)} \quad (\alpha \in R^+,\ N \geq 0),$$

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

Let V^+ be the $\mathscr{A}$-algebra defined by the generators (a) and the relations (d1)–(d5) below:

$$\text{(d1)} \qquad E_\alpha^{(N)} E_\alpha^{(M)} = \begin{bmatrix} N+M \\ N \end{bmatrix} E_\alpha^{(N+M)}, \qquad E_\alpha^{(0)} = 1,$$

$$\text{(d2)} \qquad E_{\alpha_i}^{(N)} E_\alpha^{(M)} = E_\alpha^{(M)} E_{\alpha_i}^{(N)} \quad \text{if } (\alpha, \alpha_i) = 0, \ i < g(\alpha), \ h'(\alpha) \in \mathbb{Z},$$

$$\text{(d3)} \qquad E_{\alpha'}^{(N)} E_\alpha^{(M)} = \sum_{j \geq 0; j \leq N; j \leq M} v^{j+(N-j)(M-j)} E_\alpha^{(M-j)} E_{\alpha+\alpha'}^{(j)} E_{\alpha'}^{(N-j)},$$

$$\text{(d4)} \qquad v^{NM} E_{\alpha'}^{(N)} E_{\alpha+\alpha'}^{(M)} = E_{\alpha+\alpha'}^{(M)} E_{\alpha'}^{(N)},$$

$$\text{(d5)} \qquad v^{NM} E_{\alpha+\alpha'}^{(M)} E_\alpha^{(N)} = E_\alpha^{(N)} E_{\alpha+\alpha'}^{(M)}.$$

In (d3), (d4), and (d5) it is assumed that $(\alpha, \alpha') = -1$ and that either (e1) or (e2) holds:

$$\text{(e1)} \qquad \alpha' = \alpha_i, \qquad i < g(\alpha),$$

$$\text{(e2)} \qquad h(\alpha') = h(\alpha) + 1, \qquad g(\alpha') = g(\alpha).$$

Let V^- be the $\mathscr{A}$-algebra defined by the generators (b) and the relations (f1)–(f5) below:

$$\text{(f1)} \qquad F_\alpha^{(N)} F_\alpha^{(M)} = \begin{bmatrix} N+M \\ N \end{bmatrix} F_\alpha^{(N+M)}, \qquad F_\alpha^{(0)} = 1,$$

$$\text{(f2)} \qquad F_{\alpha_i}^{(N)} F_\alpha^{(M)} = F_\alpha^{(M)} F_{\alpha_i}^{(N)} \quad \text{if } (\alpha, \alpha_i) = 0, \ i < g(\alpha), \ h'(\alpha) \in \mathbb{Z},$$

$$\text{(f3)} \qquad F_\alpha^{(M)} F_{\alpha'}^{(N)} = \sum_{j \geq 0; j \leq N; j \leq M} v^{-j-(N-j)(M-j)} F_{\alpha'}^{(N-j)} F_{\alpha+\alpha'}^{(j)} F_\alpha^{(M-j)},$$

$$\text{(f4)} \qquad v^{NM} F_{\alpha'}^{(N)} F_{\alpha+\alpha'}^{(M)} = F_{\alpha+\alpha'}^{(M)} F_{\alpha'}^{(N)},$$

$$\text{(f5)} \qquad v^{NM} F_{\alpha+\alpha'}^{(M)} F_\alpha^{(N)} = F_\alpha^{(N)} F_{\alpha+\alpha'}^{(M)}.$$

In (f3), (f4), and (f5) it is assumed that $(\alpha, \alpha') = -1$ and either (e1) or (e2) holds. Let V^0 be the $\mathscr{A}$-algebra defined by the generators (c) and the relations (g1)–(g5) below:

(g1) the generators (c) commute with each other,

$$\text{(g2)} \qquad K_i K_i^{-1} = 1, \qquad \begin{bmatrix} K_i; c \\ 0 \end{bmatrix} = 1,$$

$$\text{(g3)} \qquad \begin{bmatrix} K_i; 0 \\ t \end{bmatrix} \begin{bmatrix} K_i; -t \\ t' \end{bmatrix} = \begin{bmatrix} t+t' \\ t \end{bmatrix} \begin{bmatrix} K_i; 0 \\ t+t' \end{bmatrix} \qquad (t, t' \geq 0),$$

$$\text{(g4)} \qquad \begin{bmatrix} K_i; c \\ t \end{bmatrix} - v^{-t} \begin{bmatrix} K_i; c+1 \\ t \end{bmatrix} = -v^{-(c+1)} K_i^{-1} \begin{bmatrix} K_i; c \\ t-1 \end{bmatrix} \qquad (t \geq 1),$$

$$\text{(g5)} \qquad (v - v^{-1}) \begin{bmatrix} K_i; 0 \\ 1 \end{bmatrix} = K_i - K_i^{-1}.$$

An equivalent set of relations for V^0 consists of (g5) together with the relations (g6)–(g10) below:

(g6) the generators K_i, K_i^{-1}, $\begin{bmatrix} K_i ; 0 \\ t \end{bmatrix}$ commute with each other,

(g7)
$$K_iK_i^{-1} = 1, \qquad \begin{bmatrix} K_i ; 0 \\ 0 \end{bmatrix} = 1,$$

(g8)
$$\sum_{0\le j\le t'} (-1)^j v^{t(t'-j)} \begin{bmatrix} t+j-1 \\ j \end{bmatrix} K_i^j \begin{bmatrix} K_i ; 0 \\ t \end{bmatrix} \begin{bmatrix} K_i ; 0 \\ t'-j \end{bmatrix} = \begin{bmatrix} t+t' \\ t \end{bmatrix} \begin{bmatrix} K_i ; 0 \\ t+t' \end{bmatrix} \qquad (t \ge 1, t' \ge 0),$$

(g9)
$$\begin{bmatrix} K_i ; -c \\ t \end{bmatrix} = \sum_{0\le j\le t} (-1)^j v^{c(t-j)} \begin{bmatrix} c+j-1 \\ j \end{bmatrix} K_i^j \begin{bmatrix} K_i ; 0 \\ t-j \end{bmatrix} \qquad (t \ge 0, c \ge 1),$$

(g10)
$$\begin{bmatrix} K_i ; c \\ t \end{bmatrix} = \sum_{0\le j\le t} v^{c(t-j)} \begin{bmatrix} c \\ j \end{bmatrix} K_i^{-j} \begin{bmatrix} K_i ; 0 \\ t-j \end{bmatrix} \qquad (t \ge 0, c \ge 0).$$

Let V be the $\mathscr{A}$-algebra defined by the generators (a), (b), and (c) and the relations (d1)–(d5), (f1)–(f5), and (g5)–(g10) together with the relations (h1)–(h6) below:

(h1)
$$E_{\alpha_i}^{(M)} F_{\alpha_j}^{(M)} = F_{\alpha_j}^{(M)} E_{\alpha_i}^{(N)} \quad \text{if } i \ne j,$$

(h2)
$$E_{\alpha_i}^{(N)} F_{\alpha_i}^{(M)} = \sum_{t\ge 0 ; t\le N ; t\le M} F_{\alpha_i}^{(M-t)} \begin{bmatrix} K_i ; 2t-N-M \\ t \end{bmatrix} E_{\alpha_i}^{(N-t)},$$

(h3), (h4)
$$\left.\begin{aligned} K_i^{\varepsilon} E_{\alpha_j}^{(N)} &= v^{a_{ij}\varepsilon N} E_{\alpha_j}^{(N)} K_i^{\varepsilon} \\ K_i^{\varepsilon} F_{\alpha_j}^{(N)} &= v^{-a_{ij}\varepsilon N} F_{\alpha_j}^{(N)} K_i^{\varepsilon} \end{aligned}\right\} \quad (\varepsilon = \pm 1),$$

(h5)
$$\begin{bmatrix} K_i ; c \\ t \end{bmatrix} E_{\alpha_j}^{(N)} = E_{\alpha_j}^{(N)} \begin{bmatrix} K_i ; c+Na_{ij} \\ t \end{bmatrix},$$

(h6)
$$\begin{bmatrix} K_i ; c \\ t \end{bmatrix} F_{\alpha_j}^{(N)} = F_{\alpha_j}^{(N)} \begin{bmatrix} K_i ; c-Na_{ij} \\ t \end{bmatrix}.$$

Remark 2.4. We observe that $\alpha, \alpha' \in R^+$ with $(\alpha, \alpha') = -1$ can satisfy §2.3 (e2) only in type E_8. Indeed for such α and α' we have $\alpha + \alpha' \in R^+$, $c_{\alpha+\alpha'} = c_\alpha + c_{\alpha'} \ge 2$, and we then use §2.2(a). We see also that we have necessarily $\alpha \in R^+_{8,14}$, $\alpha' \in R^+_{8,15}$, and $\alpha + \alpha' = \beta_0$ (= the highest root). Note that in type E_8 we have

$$R^+_{8,14} = \{\beta_2, \beta_5, \beta_7\}, \quad R^+_{8,15} = \{\beta_2', \beta_5', \beta_7'\}, \quad R^+_{8,29/2} = \{\beta_0\},$$

where the notation is determined by the equalities

(a) $\beta_i' = \beta_j + \alpha_k$, if i, j, k is a permutation of $2, 5, 7$,

(b) $\beta_0 = \beta_i + \beta_i'$, if $i \in \{2, 5, 7\}$.

We wish to derive some consequences of the relations in §2.3.

Lemma 2.5. *Let α, α' be as in* 2.3(d3)–(d5). *The following identities hold in V^+.*

(a)
$$E_\alpha^{(N)} E_{\alpha'}^{(M)} = \sum_{N-M \le r \le N} (-1)^{r+N-M} \begin{bmatrix} r-1 \\ N-M-1 \end{bmatrix} E_\alpha^{(N-r)} E_{\alpha'}^{(M)} E_\alpha^{(r)} \qquad (N > M \ge 0),$$

(b)
$$E_{\alpha'}^{(M)} E_\alpha^{(N)} = \sum_{N-M \le r \le N} (-1)^{r+N-M} \begin{bmatrix} r-1 \\ N-M-1 \end{bmatrix} E_\alpha^{(r)} E_{\alpha'}^{(M)} E_\alpha^{(N-r)} \qquad (N > M \ge 0),$$

(c)
$$E_\alpha^{(M)} E_{\alpha'}^{(M+N)} E_\alpha^{(N)} = E_{\alpha'}^{(N)} E_\alpha^{(M+N)} E_{\alpha'}^{(M)} \qquad (N, M \ge 0)$$

(*compare Verma* [13]),

(d)
$$E_{\alpha+\alpha'}^{(N)} = \sum_{j=0}^{N} (-1)^{N-j} v^{-j} E_{\alpha'}^{(j)} E_\alpha^{(N)} E_{\alpha'}^{(N-j)} \qquad (N \ge 0),$$

(e)
$$E_{\alpha+\alpha'}^{(N)} = \sum_{j=0}^{N} (-1)^{N-j} v^{-j} E_\alpha^{(N-j)} E_{\alpha'}^{(N)} E_\alpha^{(j)} \qquad (N \ge 0).$$

Proof. In the right-hand side of (a) we substitute $E_{\alpha'}^{(M)} E_\alpha^{(r)}$ by the expression provided by §2.3(d3); performing cancellations, we get the left-hand side of (a).

In the right-hand side of (b), we substitute $E_{\alpha'}^{(M)} E_\alpha^{(N-r)}$ by the expression provided by §2.3(d3), and in the left-hand side of (b) we substitute $E_{\alpha'}^{(M)} E_\alpha^{(N)}$ by the expression provided by §2.3(d3); we see that we obtain equal expressions. The same argument applies to (c): we substitute $E_{\alpha'}^{(M+N)} E_\alpha^{(N)}$ and $E_{\alpha'}^{(N)} E_\alpha^{(M+N)}$ by the expressions provided by §2.3(d3). We argue in the same way for (d): we substitute $E_{\alpha'}^{(j)} E_\alpha^{(N)}$ in the right-hand side of (d) by the expression provided by §2.3(d3) and we obtain the left-hand side. Now (e) follows directly from (c) and (d).

Lemma 2.6. *Let $\gamma \in R^+$ and $\alpha_i, \alpha_j \in \Pi$ be such that $i, j < g(\gamma)$, $(\alpha_i, \alpha_j) = 0$, and $(\gamma, \alpha_i) = (\gamma, \alpha_j) = -1$. Then $E_{\gamma+\alpha_i}^{(N)} E_{\gamma+\alpha_j}^{(M)} = E_{\gamma+\alpha_j}^{(M)} E_{\gamma+\alpha_i}^{(N)}$ in V^+.*

Proof. By Lemma 2.5(e) we have

$$E_{\gamma+\alpha_i}^{(N)} E_{\gamma+\alpha_j}^{(M)} = \left(\sum_{j=0}^{N}(-1)^{N-j}v^{-j}E_\gamma^{(N-j)}E_{\alpha_i}^{(N)}E_\gamma^{(j)}\right) \times \left(\sum_{h=0}^{M}(-1)^{M-h}v^{-h}E_\gamma^{(M-h)}E_{\alpha_j}^{(M)}E_\gamma^{(h)}\right)$$
$$= \sum_{\substack{0\le j\le N\\ 0\le h\le M}} (-1)^{M+N-j-h}v^{-j-h}\begin{bmatrix} M+j-h \\ j\end{bmatrix} E_\gamma^{(N-j)}E_{\alpha_i}^{(N)}E_\gamma^{(M+j-h)}E_{\alpha_j}^{(M)}E_\gamma^{(h)}.$$

Now let

$$\theta_{i,j} = \sum_{0\le k\le M+N} (-1)^{M+N-k}v^{-k}E_\gamma^{(M+N-k)}E_{\alpha_i}^{(N)}E_{\alpha_j}^{(M)}E_\gamma^{(k)}.$$

In the last sum we apply Lemma 2.5(a) with $\alpha=\gamma$ and $\alpha'=\alpha_i$ to the products $E_\gamma^{(M+N-k)}E_{\alpha_i}^{(N)}$ with $k<M$ and we apply Lemma 2.5(b) with $\alpha=\gamma$ and $\alpha'=\alpha_j$ to the products $E_{\alpha_j}^{(M)}E_\gamma^{(k)}$ with $k>M$: we leave the term with $k=M$ unchanged. We obtain

$$\begin{aligned}\theta_{i,j} &= \sum_{0\le k<M}(-1)^{M+N-k}v^{-k}\sum_{M-k\le r\le M+N-k}(-1)^{r+M-k}\begin{bmatrix} r-1 \\ M-k-1\end{bmatrix} \\ &\qquad \times E_\gamma^{(M+N-k-r)}E_{\alpha_i}^{(N)}E_\gamma^{(r)}E_{\alpha_j}^{(M)}E_\gamma^{(k)} \\ &\quad + \sum_{M<k\le M+N}(-1)^{M+N-k}v^{-k}\sum_{k-M\le r\le k}(-1)^{r+k-M}\begin{bmatrix} r-1 \\ k-M-1\end{bmatrix} \\ &\qquad \times E_\gamma^{(M+N-k)}E_{\alpha_i}^{(N)}E_\gamma^{(r)}E_{\alpha_j}^{(M)}E_\gamma^{(k-r)} \\ &\quad + (-1)^N v^{-M}E_\gamma^{(N)}E_{\alpha_i}^{(N)}E_{\alpha_j}^{(M)}E_\gamma^{(M)} \\ &= \sum_{\substack{0\le j\le N\\ 0\le h\le M}}(-1)^{M+N-j-h}v^{-j-h}\left(v^j\begin{bmatrix} M+j-h-1 \\ j\end{bmatrix}\right. \\ &\qquad \left. +v^{h-M}\begin{bmatrix} M+j-h-1 \\ j-1\end{bmatrix}\right) \\ &\qquad \times E_\gamma^{(N-j)}E_{\alpha_i}^{(N)}E_\gamma^{(M+j-h)}E_{\alpha_j}^{(M)}E_\gamma^{(h)} \\ &= E_{\gamma+\alpha_i}^{(N)}E_{\gamma+\alpha_j}^{(M)}.\end{aligned}$$

(We have used the following convention: $\left[\begin{smallmatrix} m \\ -1\end{smallmatrix}\right]=0$ for $m\ge 0$, $\left[\begin{smallmatrix} -1 \\ -1\end{smallmatrix}\right]=1$.)

Interchanging the roles of α_i, N and α_j, M, we see by the same computation that $E_{\gamma+\alpha_j}^{(M)} E_{\gamma+\alpha_i}^{(N)}$ is equal to the expression obtained from θ_{ij} by interchanging $E_{\alpha_i}^{(N)}$ and $E_{\alpha_j}^{(M)}$. But that expression is again θ_{ij} since $E_{\alpha_i}^{(N)}$, $E_{\alpha_j}^{(M)}$ commute by §2.3(d2). (Recall that $(\alpha_i, \alpha_j) = 0$.) Hence $E_{\gamma+\alpha_i}^{(N)} E_{\gamma+\alpha_j}^{(M)} = E_{\gamma+\alpha_j}^{(M)} E_{\gamma+\alpha_i}^{(N)} = \theta_{ij}$. The lemma is proved.

Proposition 2.7 (Type E_8). *Let* i, k, l *be a permutation of* $\{2, 5, 7\}$. *With the notation in Remark* 2.4 *we have for any* $N, M \geq 0$:

(a) $$E_{\beta_l'}^{(N)} E_{\beta_k'}^{(M)} = E_{\beta_k'}^{(M)} E_{\beta_l'}^{(N)},$$

(b) $$E_{\alpha_i}^{(N)} E_{\beta_0}^{(M)} = \sum_{s\geq 0} \psi_s E_{\beta_0}^{(M-s)} E_{\beta_k'}^{(s)} E_{\beta_l'}^{(s)} E_{\alpha_i}^{(N-s)},$$

where $\psi_s = v^{-s(N+M-s)} \cdot \prod_{j=1}^{s}(1 - v^{2j})$, *and*

(c) $$E_{\alpha_h}^{(N)} E_{\beta_0}^{(M)} = E_{\beta_0}^{(M)} E_{\alpha_h}^{(N)} \quad \textit{if } h \in \{1, 3, 4, 6\}.$$

Proof. If we set $\gamma = \beta_i$, we have $\beta_l' = \gamma + \alpha_k$ and $\beta_k' = \gamma + \alpha_l$ (see Remark 2.4(a)), hence (a) follows directly from Lemma 2.6.

We not prove (c). Let h be as in (c). We write $E_{\beta_0}^{(M)}$ as an $\mathscr{A}$-linear combination of products $E_{\beta_5'}^{(t)} E_{\beta_5}^{(M)} E_{\beta_5'}^{(M-t)}$, using Lemma 2.5(d) with $\alpha = \beta_5$, $\alpha' = \beta_5'$, and $\alpha + \alpha' = \beta_0$. Note that $E_{\alpha_h}^{(N)}$ commutes with all three factors in such a product (by §2.3(d2) since $(\alpha_h, \beta_5') = (\alpha_h, \beta_5) = 0$); (c) follows.

We compute the left-hand side ($= \Gamma$) of (b) by substituting $E_{\beta_0}^{(M)}$ by the expression given in Lemma 2.5(d), with $\alpha = \beta_k$, $\alpha' = \beta_k'$, and $\alpha + \alpha' = \beta_0$:

$$\Gamma = \sum_t (-1)^{M-t} v^{-t} E_{\alpha_i}^{(N)} E_{\beta_k'}^{(t)} E_{\beta_k}^{(M)} E_{\beta_k'}^{(M-t)}.$$

Using the commutation formulas

$$E_{\alpha_i}^{(N)} E_{\beta_k'}^{(t)} = v^{-Nt} E_{\beta_k'}^{(t)} E_{\alpha_i}^{(N)} \quad \text{(see §2.3(d4); } \beta_k' = \beta_l + \alpha_i\text{)},$$

(d) $$E_{\alpha_i}^{(N)} E_{\beta_k}^{(M)} = \sum_s v^{s+(N-s)(M-s)} E_{\beta_k}^{(M-s)} E_{\beta_l'}^{(s)} E_{\alpha_i}^{(N-s)}$$

$$\text{(see §2.3(d3); } \beta_l' = \beta_k + \alpha_i\text{)},$$

we see that

$$\Gamma = \sum_{t,s} (-1)^{M-t} v^{-t+s+(N-s)(M-s)-Nt} E_{\beta_k'}^{(t)} E_{\beta_k}^{(M-s)} E_{\beta_l'}^{(s)} E_{\alpha_i}^{(N-s)} E_{\beta_k'}^{(M-t)}.$$

We interchange the last two factors (and introduce an appropriate power of v) using (d), and we use (a) to interchange $E_{\beta_l'}^{(s)}$ and $E_{\beta_k'}^{(M-t)}$; we obtain

$$\Gamma = \sum_{t,s} (-1)^{M-t} v^{-t+s+(N-s)(t-s)-Nt} E_{\beta_k'}^{(t)} E_{\beta_k}^{(M-s)} E_{\beta_k'}^{(M-t)} E_{\beta_l'}^{(s)} E_{\alpha_i}^{(N-s)}.$$

This shows that to prove (b) it is enough to prove that for any $0 \leq s \leq M$, we have

$$\text{(e)} \qquad \sum_t (-1)^{M-t} v^{-t+s+(N-s)(t-s)-Nt} E_{\beta_k'}^{(t)} E_{\beta_k}^{(M-s)} E_{\beta_k'}^{(M-t)} = \psi_s E_{\beta_0}^{(M-s)} E_{\beta_k'}^{(s)}.$$

Let Γ' be the left-hand side of (e). We substitute $E_{\beta_k'}^{(t)} E_{\beta_k}^{(M-s)}$ by the expression given by §2.3(d3); we see that

$$\Gamma' = \sum_{t,r} (-1)^{M-t} v^{-t+s+(N-s)(t-s)-Nt+r+(t-r)(M-s-r)} E_{\beta_k}^{(M-s-r)} E_{\beta_0}^{(r)} E_{\beta_k'}^{(t-r)} E_{\beta_k'}^{(M-t)}.$$

We replace $E_{\beta_k'}^{(t-r)} E_{\beta_k'}^{(M-t)}$ by $\left[\begin{smallmatrix} M-r \\ M-t \end{smallmatrix}\right] E_{\beta_k'}^{(M-r)}$; then Γ' is a linear combination of monomials $E_{\beta_k}^{(a)} E_{\beta_0}^{(b)} E_{\beta_k'}^{(c)}$ with coefficients in $\mathscr{A}$, and it is enough to show that each of these coefficients is zero except in the case where $a = 0$, $b = M-s$, and $c = s$, when it is ψ_s.

Thus, we are reduced to showing that for any $s \in [0, M]$ and any $r \in [0, M-s]$ we have

$$\sum_{0 \leq t \leq M-r} (-1)^{M-t} v^{f(t)} \begin{bmatrix} M-r \\ M-r \end{bmatrix} = \begin{cases} \psi_s & \text{if } r = M-s, \\ 0 & \text{if } r < M-s, \end{cases}$$

where $f(t) = -t+s+(N-s)(t-s)-Nt+r+(t-r)(M-s-r)$, or equivalently, that:

$$\text{(f)} \qquad v^{f_0} \sum_{0 \leq t' \leq M-r} \begin{bmatrix} M-r \\ t' \end{bmatrix} v^{t'(M-r-1)} \left(-v^{2(s+r+1-M)}\right)^{t'} = \begin{cases} \prod_{j=1}^{s} (1 - v^{2j}) & \text{if } r = M-s, \\ 0 & \text{if } r < M-s, \end{cases}$$

where $f_0 = (s+r-M)(1+r-M)$.

The left-hand side of (f) is equal to the value of

$$v^{f_0} \prod_{h=0}^{M-r-1} (1 + v^{2h} x) \quad \text{for } x = -v^{2(s+r+1-M)}.$$

Hence it is zero precisely when $0 \leq -(s+r+1-M)$, i.e. when $r < M-s$. Hence (f) holds and the proposition is proved.

Proposition 2.8. *Let $\alpha \in R_{i,l}^+$ and $\alpha' \in R_{i,l'}^+$, $\alpha \neq \alpha'$. Assume that $l' = l$ or $l+1$. In the case where $l' = l+1$, assume further that $R_{i,l+1/2}^+ = \varnothing$. Let $N, M \geq 0$.*

(a) *If $l' = l$, we have $(\alpha, \alpha') = 0$.*

(b) *If $l' = l+1$, we have either $(\alpha, \alpha') = 0$ or $(\alpha, \alpha') = 1$; in the latter case, we have $\alpha' = \alpha + \alpha_h$ for some $h < i$.*

(c) *If* $(\alpha, \alpha') = 1$, *then* $E_\alpha^{(N)} E_{\alpha'}^{(M)} = v^{NM} E_{\alpha'}^{(M)} E_\alpha^{(N)}$.

(d) *If* $(\alpha, \alpha') = 0$, *then* $E_\alpha^{(N)} E_{\alpha'}^{(M)} = E_{\alpha'}^{(M)} E_\alpha^{(N)}$.

Proof. If $(\alpha, \alpha') = -1$, then $\alpha + \alpha' \in R^+$. We have $g(\alpha + \alpha') = i$ and $c_{\alpha+\alpha'} = c_\alpha + c_{\alpha'} \geq 1 + 1 = 2$. By §2.2(a), it follows that we are in type E_8 and $i = 8$, $\alpha + \alpha' = \beta_0$.

Hence $h(\alpha) + h(\alpha') = 29$. This is impossible in case (a) since $h(\alpha) = h(\alpha')$ is an integer; in case (b), we have $h(\alpha) = l$ and $h(\alpha') = l + 1$, hence $\alpha \in R^+_{8,14}$ and $\alpha' \in R^+_{8,15}$, contradicting our assumption. (We have $R^+_{8,29/2} \neq \varnothing$.) Thus, $(\alpha, \alpha') \in \{0, 1\}$.

Assume that $(\alpha, \alpha') = 1$. Then $\alpha' - \alpha$ is a (positive) root, hence α and α' have different heights; in particular, we must be in case (b). Then $\alpha' - \alpha$ has height 1 so $\alpha' = \alpha + \alpha_h$ for some $\alpha_h \in \Pi$. Clearly, $h \leq i$. If $h = i$, then $c_{\alpha'} > c_\alpha$, so $c_{\alpha'} \geq 2$. By §2.2(a), we see that we are in type E_8 and $\alpha' = \beta_0$, so $l + 1 = 29/2$. But then α would have level $27/2$, which is impossible. Thus $h < i$ and (a) and (b) are proved. Now (c) follows directly from (a), (b), and §2.3(d5).

We prove (d) by induction on $N = h(\alpha) + h(\alpha') \geq 2$.

When $N = 2$, then both α and α' are in Π and, since $g(\alpha) = g(\alpha')$, we have $\alpha = \alpha'$ and there is nothing to prove. Assume now that α and α' (as in (d)) have $N \geq 3$ and that (d) is already known for smaller values of N. We can assume that

(e) in type E_8, we have $\alpha' \notin R^+_{8,15}$.

(Otherwise, we would also have $\alpha \in R^+_{8,15}$ and we could use Proposition 2.7(a).)

Moreover, it is clear that

(f) in type E_8, neither α nor α' can be in $R^+_{8,29/2}$.

Since $N \geq 3$, we can assume that $h(\alpha') \geq 2$. We can write $\alpha' = \gamma + \alpha_k$ for some $k < i$ and $\gamma' \in R^+$. We have $h(\alpha) + h(\gamma) = N - 1$, $\gamma \in R^+_{i,l'-1}$, and $l = l' - 1$ or l'; moreover, in the case where $l = l'$, we have $R^+_{i,l-1/2} = \varnothing$ by (e). We have $\gamma \neq \alpha$; otherwise, $\alpha' = \alpha + \alpha_k$, contradicting $(\alpha, \alpha') = 0$.

Assume first that $(\alpha, \gamma) = 0$. Then the induction hypothesis applies to γ, α and gives

(g) $E_\gamma^{(M)} E_\alpha^{(N)} = E_\alpha^{(N)} E_\gamma^{(M)}$.

We have $(\alpha, \alpha_k) = (\alpha, \alpha' - \gamma') = (\alpha, \alpha') = 0$. Hence, by (f) and §2.3(d2) we have

(h) $E_{\alpha_k}^{(P)} E_\alpha^{(N)} = E_\alpha^{(N)} E_{\alpha_k}^{(P)}$ for any $P \geq 0$.

By Lemma 2.5(d) we have

$$E_{\alpha'}^{(M)} = \sum_{j=0}^{M} (-1)^{M-j} v^{-j} E_{\alpha_k}^{(j)} E_\gamma^{(M)} E_{\alpha_k}^{(M-j)}.$$

This, together with (g) and (h) shows that $E_{\alpha'}^{(M)}$ and $E_\alpha^{(N)}$ commute.

Assume now that $(\alpha, \gamma) \neq 0$. Since (a) and (b) are applicable to γ and α, it follows that $\alpha = \gamma + \alpha_j$ for some $j < i$. We have $\alpha_j \neq \alpha_k$ since

$\alpha \neq \alpha'$. Hence $(\alpha_j, \alpha_k) \in \{0, -1\}$. If we had $(\alpha_j, \alpha_k) = -1$, then from $(\gamma, \alpha_j) = (\gamma, \alpha_k) = -1$ it would follow that the mutual inner products of γ, α_j, and α_k form a singular matrix

$$\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix},$$

hence γ, α_j, and α_k are linearly dependent so $\gamma \in \{\alpha_j, \alpha_k, \alpha_j + \alpha_k\}$; this contradicts $(\gamma, \alpha_j) = (\gamma, \alpha_k) = -1$. Thus, we have $(\alpha_j, \alpha_k) = 0$. We may apply Lemma 2.6 and deduce that $E_{\alpha'}^{(M)}$ and $E_{\alpha}^{(N)}$ commute. This proposition is proved.

2.9. A nonempty subset of R^+ is said to be a *box* if it is of the form $R^+_{i,l}$ for some i, l. We arrange the boxes in a sequence as follows:

(a) $R^+_{n,1}, R^+_{n,2}, \ldots ; R^+_{n-1,1}, R^+_{n-1,2}, \ldots ; \ldots ; R_{2,1}, R_{2,2}, \ldots ; R_{1,1}$.

(Note that in type E_8 we place the box $R^+_{8,29/2}$ between the boxes $R^+_{8,14}$ and $R^+_{8,15}$.)

We shall give the product $\prod_{\alpha \in R^+} E_\alpha^{(m_\alpha)}$ the following meaning: we compute it using any total order on R^+ which is compatible with the order (a) of the boxes, i.e. if $\alpha, \alpha' \in R^+$ and the box of α' is to the right of the box of α, then $\alpha < \alpha'$. This is well defined since $E_\alpha^{(m)}$ and $E_{\alpha'}^{(m')}$ commute when α and α' are in the same box (see Proposition 2.8).

We define similarly a product $\prod E_\alpha^{(m_\alpha)}$ where α runs over a subset of R^+; this is a special case of the previous product, with $m_\alpha = 0$ for certain α.

2.10. We introduce a number of subspaces of V^+. We fix a box $R^+_{i,l}$ with l integral.

$X_{i,l}$ is the $\mathscr{A}$-subalgebra of V^+ generated by the $E_\alpha^{(N)}$ $(\alpha \in R^+_{i,l},\ N \geq 1)$ and by the $E_{\alpha_j}^{(M)}$ $(j < i, M \geq 1)$.

$\widetilde{X}_{i,l}$ is the $\mathscr{A}$-subalgebra of V^+ generated by the $E_\alpha^{(N)}$ $(\alpha \in R^+_{i,l} \cup R^+_{i,i+1/2} \cup R^+_{i,i+1}, N \geq 1)$ and by the $E_{\alpha_j}^{(M)}$ $(j < i, M \geq 1)$.

$Y_{i,l}$ is the $\mathscr{A}$-submodule of V^+ generated by all monomials $\prod_\alpha E_\alpha^{(N_\alpha)}$ $(N_\alpha \geq 0)$ with α restricted to the roots in boxes strictly to the left of $R^+_{i,l}$.

$Z_{i,l}$ is the $\mathscr{A}$-subalgebra of V^+ generated by all monomials $\prod_\alpha E_\alpha^{(N_\alpha)}$ $(N_\alpha \geq 0)$ with α restricted to the roots in $R^+_{i,l} \cup R^+_{i,l+1/2}$.

With this notation we can state

Lemma 2.11. *Assume that $R^+_{i,l}$ is a box with l integral $(i, l) \neq (1, 1)$. Let $R^+_{i',l'}$ be the first box with integral l' which is to the right of $R^+_{i,l}$. Then*

(a) $\widetilde{X}_{i,l} \subset Z_{i,l} \cdot X_{i',l'}$,

(b) $Y_{i,l} \cdot X_{i,l} \subset Y_{i',l'} \cdot X_{i',l'}$.
(The product of two subsets of V^+ is the set of sums of products of an element in the first set with one in the second set.)

Proof. (a) $\widetilde{X}_{i,l}$ is spanned as an $\mathscr{A}$-module by monomials $\xi_1\xi_2\cdots\xi_L$, where each ξ_t is one of the algebra generators of $\widetilde{X}_{i,l}$ given in §2.10. For such a monomial we define the *content* to be $\sum_t N_{\alpha_t}$, where t runs over all indices in $[1, L]$ such that $\xi_t = E_{\alpha_t}^{(N_{\alpha_t})}$ with $\alpha_t \in R_{i,l}^+ \cup R_{i,l+1/2}^+$ and $N_{\alpha_t} \geq 1$. (Such a generator ξ_t is said to be distinguished.)

We define the *defect* of a monomial as above to be the number of pairs $t < t'$ in $[1, L]$ such that $\xi_{t'}$ is distinguished and ξ_t is not distinguished. (Thus $\xi_t = E_\alpha^{(N)}$ with $\alpha \in R_{i,l+1}^+$ or $\alpha = \alpha_j$, $j < 1$, and $N \geq 1$.) Such pairs $t < t'$ are said to be bad pairs. Consider a monomial $\xi_1\xi_2\cdots\xi_L$ as above and assume that it has content c and defect $d \geq 1$. We can find for it a bad pair $t < t'$ with $t' = t + 1$. Using §2.3(d2)–(d5) and Propositions 2.7(b), (c) and 2.8, we see that $\xi_t\xi_{t'}$ is equal to an $\mathscr{A}$-multiple of $\xi_{t'}\xi_t$ plus an $\mathscr{A}$-linear combination of monomials with content strictly smaller than that of $\xi_t\xi_{t'}$. Hence $\xi_1\xi_2\cdots\xi_L$ is an $\mathscr{A}$-linear combination of monomials, one of which has content c and defect $< d$, and the remaining ones, if defined, have content $< c$. This shows by double induction on (c, d) that any monomial is an $\mathscr{A}$-linear combination of monomials of defect 0.

Now the distinguished generators commute with each other (only up to a power of v if one is in $R_{8,14}^+$ and one is in $R_{8,15/2}^+$); using this and §2.3(d1) we see that any monomial of defect 0 is contained in $Z_{i,l}X_{i',l'}$ and (a) is proved.

From (a) it follows that $Y_{i,l} \cdot \widetilde{X}_{i,l} \subset Y_{i,l} \cdot Z_{i,l} \cdot X_{i',l'}$. It is clear that $Y_{i,l}Z_{i,l} = Y_{i',l'}$ and $X_{i,l} \subset \widetilde{X}_{i,l}$. Hence $Y_{i,l}X_{i,l} \subset Y_{i,l}\widetilde{X}_{i,l} \subset Y_{i,l}Z_{i,l}X_{i',l'} = Y_{i',l'}X_{i',l'}$, proving (b).

Proposition 2.12. (a) *V^+ is generated as an $\mathscr{A}$-algebra by the elements $E_{\alpha_i}^{(N)}$ ($i \in [1, n]$, $N \geq 1$).*

(b) *V^+ is generated as an $\mathscr{A}$-module by the monomials $\prod_{\alpha\in R^+} E_\alpha^{(N_\alpha)}$ ($N_\alpha \geq 0$).*

Proof. Let V_1^+ be the $\mathscr{A}$-subalgebra of V^+ generated by the $E_{\alpha_i}^{(N)}$ ($i \in [i, n]$, $N \geq 1$). We prove by induction on $h(\beta)$ that $E_\beta^{(N)} \in V_1^+$ for all $\beta \in R^+$. This is clear if $h(\beta) = 1$, hence we can assume that $h(\beta) > 1$ and that our assertion is already proved for all $\beta' \in R^+$ with $h(\beta') < h(\beta)$. Assume first that $c_\beta = 1$ (see §2.2). We can find $i \in [1, n]$ such that $i < g(\beta)$ and $(\beta, \alpha_i) = 1$. Then $\beta - \alpha_i \in R^+$ and $E_{\beta-\alpha_i}^{(M)} \in V_1^+$ for all $M \geq 1$ by the induction hypothesis. We apply Lemma 2.5(d) with $\alpha = \beta - \alpha_i$ and $\alpha' = \alpha_i$; we are in the situation of §2.3(e1) since $(\alpha, \alpha') = -1$ and $i < g(\alpha) = g(\beta)$. We see that $E_\beta^{(N)} \in V_1^+$ for all $N \geq 1$.

Assume next that $c_\beta \geq 2$. Then by §2.2(a) we must be in type E_8 and β must be the highest root β_0. We can apply Lemma 2.5(d) with $\alpha = \beta_5$, $\alpha' = \beta'_5$, and $\alpha + \alpha' = \beta_0$, and we see that $E_{\beta_0}^{(N)}$ is an $\mathscr{A}$-linear combination of products $E_{\beta'_5}^{(t)} E_{\beta_5}^{(N)} E_{\beta'_5}^{(N-t)}$. By the induction hypothesis, the factors of these products are in V_1^+. Hence $E_{\beta_0}^{(N)} \in V_1^+$. This proves (a)

We now prove (b). Applying repeatedly Lemma 2.11(b), we see that $Y_{n,1} \cdot X_{n,1} \subset Y_{1,1} X_{1,1}$. ($R_{n,1}^+$ is the first box in §2.9(a), $R_{1,1}^+$ is the last box.) Clearly, $Y_{1,1} \cdot X_{1,1}$ is the $\mathscr{A}$-module spanned by the monomials in the proposition. On the other hand, $Y_{n,1} X_{n,1} = X_{n,1}$ is V_1^+ and, by (a), this equals V^+. The proposition is proved.

2.13. It is clear that there is a unique ring isomorphism

(a) $$V^- \xrightarrow{\approx} (V^+)^{\mathrm{opp}}$$

which takes $F_\alpha^{(N)}$ to $E_\alpha^{(N)}$ $(\alpha \in R^+)$ and v to v^{-1}. Hence from Proposition 2.12 we deduce:

(b) V^- is generated as an $\mathscr{A}$ -algebra by the elements $F_{\alpha_i}^{(N)}$ $(i \in [1, n], N \geq 1)$,

(c) the products $\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)}$ (defining using the order on R^+ opposite to that defining $\prod_\alpha E_\alpha^{(N_\alpha)}$) generate V^- as an $\mathscr{A}$-module.

Proposition 2.14. *V^0 is generated as an $\mathscr{A}$-module by the elements*

(a) $$K_1^{\delta_1} K_2^{\delta_2} \cdots K_n^{\delta_n} \begin{bmatrix} K_1 ; 0 \\ t_1 \end{bmatrix} \cdots \begin{bmatrix} K_n ; 0 \\ t_n \end{bmatrix},$$

where $\delta_i \in \{0, 1\}$ and $t_i \in \mathbb{N}$.

Proof. Let V_1^0 (resp. V_2^0) be the $\mathscr{A}$-submodule of V^0 generated by the elements (a) (resp. by the elements (a) with δ_i allowed to be arbitrary integers). Then V_2^0 is stable under left multiplication by K_i and K_i^{-1}, and also by $\left[\begin{smallmatrix} K_i ; c \\ t' \end{smallmatrix}\right]$ (the last assertion follows from §2.3(g9), (g10)). Since V_2^0 contains 1, we have $V^0 = V_2^0$. From §2.3(g1)–(g5), we see that from $m \geq 0$:

$$K_i^{m+2} \begin{bmatrix} K_i ; 0 \\ t \end{bmatrix} = v^t (v^{t+1} - v^{-t-1}) K_i^{m+1} \begin{bmatrix} K_i ; 0 \\ t+1 \end{bmatrix} + v^{2t} K_i^m \begin{bmatrix} K_i ; 0 \\ t \end{bmatrix},$$
$$K_i^{-m-1} \begin{bmatrix} K_i ; 0 \\ t \end{bmatrix} = -v^{-t} (v^{t+1} - v^{-t-1}) K_i^{-m} \begin{bmatrix} K_i ; 0 \\ t+1 \end{bmatrix} + v^{-2t} K_i^{-m+1} \begin{bmatrix} K_i ; 0 \\ t \end{bmatrix}.$$

This shows that by induction on $m \geq 0$

$$K_i^{\pm m} \begin{bmatrix} K_i ; 0 \\ t \end{bmatrix} \in V_1^0 \quad \text{for all } m \geq 0,$$

hence $V_2^0 \subset V_1^0$. The reverse inclusion is clear and the proposition follows.

2.15. We have obvious $\mathscr{A}$-algebra homomorphisms $V^- \to V$, $V^0 \to V$, and $V^+ \to V$ (identity on generators). Using multiplication in $\mathscr{A}$, we obtain an $\mathscr{A}$-linear map

(a) $$V^- \otimes V^0 \otimes V^+ \to V.$$

Lemma 2.16. *The map* (a) *in* §2.15 *is surjective.*

Proof. From Proposition 2.12(a) we see that V is generated as an $\mathscr{A}$-module by monomials $\xi_1\xi_2\cdots\xi_L$, where each ξ_i is a generator of type I (one of $E_{\alpha_i}^{(N)}$, $i \in [1, n]$, $N \geq 1$), or type II (one of $F_{\alpha_i}^{(N)}$, $i \in [1, n]$, $N \geq 1$) or of type III (as in §2.3(c)). We define the defect of such a monomial as the number of pairs $t < t'$ in $[1, L]$ such that ξ_t is of type I and $\xi_{t'}$ is of type II. (We say that such a pair $t < t'$ is *bad*). Assume that we have a monomial as above, with defect > 1. Applying to it the relations §2.3(h3)–(h6) we see that our monomial is equal to one of the same defect which has some bad pair of form $t < t+1$. We apply to the generators on the position t, $t+1$ the identity §2.3(h1) or (h2). We see that our monomial is equal to an $\mathscr{A}$-linear combination of monomials of strictly smaller defect. Iterating this, we see that V is generated as an $\mathscr{A}$-module by monomials of defect 0. Using again §2.3(h3)–(h6) we see that any monomial of defect 0 is equal to one in which all generators of type II precede those of type III, which in turn precede those of type I. Such a monomial is in the image of §2.15(a). The proposition is proved.

Proposition 2.17. (a) *V is generated as an $\mathscr{A}$-algebra by the elements $E_{\alpha_i}^{(N)}$, $F_{\alpha_i}^{(N)}$, $K_i^{\pm 1}$ $(i \in [1, n],\ N \geq 0)$.*

(b) *V is generated as an $\mathscr{A}$-module by the elements*

$$\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)} \prod_{i=1}^{n} \left(K_i^{\delta_i} \begin{bmatrix} K_i;0 \\ t_i \end{bmatrix} \right) \prod_{\alpha \in R^+} E_\alpha^{(N'_\alpha)}$$

(*where $N_\alpha, N'_\alpha, t_i \geq 0$ and $\delta_i \in \{0, 1\}$*).

Proof. (b) follows from Lemma 2.16, Propositions 2.12(b) and 2.14, and §2.13(c). Using Lemma 2.16, Proposition 2.12(a), and §2.13(b) we see that V is generated as an $\mathscr{A}$-algebra by the elements $E_{\alpha_i}^{(N)}$, $F_{\alpha_i}^{(N)}$, $K_i^{\pm 1}$, and $\left[\begin{smallmatrix} K_i;c \\ t \end{smallmatrix}\right]$ $(i \in [1, n],\ N \geq 0,\ t \geq 0,\ c \in \mathbb{Z})$. Let V_1 be the $\mathscr{A}$-subalgebra of V generated by the elements $E_{\alpha_i}^{(N)}$, $F_{\alpha_i}^{(N)}$, and $K_i^{\pm 1}$ $(i \in [1, n],\ N \geq 0)$. We show by induction on $t \geq 0$ that $\left[\begin{smallmatrix} K_i;c \\ t \end{smallmatrix}\right] \in V_1$. When $t = 0$, this follows from §2.3(g2). For $t \geq 1$, we use §2.3(h2) and we see using the induction hypothesis that $\left[\begin{smallmatrix} K_i;0 \\ t \end{smallmatrix}\right] \in V_1$. Using now §2.3(g4) and the induction hypothesis it follows that $\left[\begin{smallmatrix} K_i;c \\ t \end{smallmatrix}\right] \in V_1$ for all c. This proves (a).

2.18. Using the natural imbedding $\mathscr{A} \subset \mathscr{A}'$ we form the $\mathscr{A}'$-algebras $V_{\mathscr{A}'}^+$, $V_{\mathscr{A}'}^-$, $V_{\mathscr{A}'}^0$, and $V_{\mathscr{A}'}$ by applying $(\ )\otimes_{\mathscr{A}} \mathscr{A}'$ to V^+, V^-, V^0, and V. We shall write E_α and F_α instead of $E_\alpha^{(1)}$ and $F_\alpha^{(1)}$.

Proposition 2.19. *$V_{\mathscr{A}'}$ is the $\mathscr{A}'$-algebra defined by the generators E_α, F_α ($\alpha \in R^+$), and K_i, K_i^{-1} ($1 \le i \le n$), and the following relations:*

$$\text{(a1)} \qquad E_{\alpha_i}E_\alpha = E_\alpha E_{\alpha_i} \quad \textit{if } (\alpha, \alpha_i) = 0, \; i < g(\alpha), \; h'(\alpha) \in \mathbb{Z},$$

$$\left.\begin{array}{ll} \text{(a2)} & E_{\alpha'}E_\alpha = vE_\alpha E_{\alpha'} + vE_{\alpha+\alpha'} \\ \text{(a3)} & vE_{\alpha'}E_{\alpha+\alpha'} = E_{\alpha+\alpha'}E_{\alpha'} \\ \text{(a4)} & vE_{\alpha+\alpha'}E_\alpha = E_\alpha E_{\alpha+\alpha'} \end{array}\right\} \begin{array}{l} \text{if } (\alpha, \alpha') = -1 \text{ and} \\ i < g(\alpha) \text{ satisfy §2.3(e1)} \\ \text{or (e2),} \end{array}$$

$$\text{(b1)} \qquad F_{\alpha_i}F_\alpha = F_\alpha F_{\alpha_i} \quad \textit{if } (\alpha, \alpha_i) = 0, \; i < g(\alpha), \; h'(\alpha) \in \mathbb{Z},$$

$$\left.\begin{array}{ll} \text{(b2)} & F_\alpha F_{\alpha'} = v^{-1}F_{\alpha'}F_\alpha + v^{-1}F_{\alpha+\alpha'} \\ \text{(b3)} & vF_{\alpha'}F_{\alpha+\alpha'} = F_{\alpha+\alpha'}F_{\alpha'} \\ \text{(b4)} & vF_{\alpha+\alpha'}F_\alpha = F_\alpha F_{\alpha+\alpha'} \end{array}\right\} \begin{array}{l} \text{if } (\alpha, \alpha') = -1 \text{ and} \\ i < g(\alpha) \text{ satisfy §2.3(e1)} \\ \text{or (e2),} \end{array}$$

$$\text{(c1)} \qquad K_iK_j = K_jK_i,$$

$$\text{(c2)} \qquad K_iK_i^{-1} = 1,$$

$$\text{(d1)} \qquad E_{\alpha_i}F_{\alpha_j} - F_{\alpha_j}E_{\alpha_i} = \delta_{ij}\frac{K_i - K_i^{-1}}{v - v^{-1}},$$

$$\text{(d2)} \qquad K_iE_{\alpha_j} = v^{a_{ij}}E_{\alpha_j}K_i,$$

$$\text{(d3)} \qquad K_iF_{\alpha_j} = v^{-a_{ij}}F_{\alpha_j}K_i.$$

Proof. Clearly, $V_{\mathscr{A}'}$ is the $\mathscr{A}'$-algebra defined by the generators (a), (b), and (c) and the relations (d1)–(d5), (f1)–(f5), (g1)–(g5), and (h1)–(h6) in §2.3. This set ($= \mathscr{M}$) of relations contains the set of relations (a1)–(d3) above as a subset, $\mathscr{M}_0$. In $V_{\mathscr{A}'}$, we have the following identities:

$$\text{(e)} \qquad \begin{gathered} E_\alpha^{(N)} = E_\alpha^N/[N]!, \quad F_\alpha^{(N)} = F_\alpha^{(N)}/[N]! \qquad (\alpha \in R^+), \\ \begin{bmatrix} K_i; c \\ t \end{bmatrix} = \prod_{s=1}^{t} \frac{K_iv^{c-s+1} - K_i^{-1}v^{-c+s-1}}{v^s - v^{-s}} \end{gathered}$$

($i \in [1, n]$, $N, t \ge 0$, $c \in \mathbb{Z}$), which are consequences of §2.3(d1), (f1), (g2), (g4), (g5). It is then enough to show that the relations in $\mathscr{M} - \mathscr{M}_0$ with $E_\alpha^{(N)}$, $F_\alpha^{(N)}$, and $\left[\begin{smallmatrix} K_i; c \\ t \end{smallmatrix}\right]$ replaced by the expression above, are consequences of the relations in $\mathscr{M}_0$. This is routine for most relations except perhaps for §2.3(d3), (f3), (h2) with N or $M \ge 2$. For §2.3(d3) we can make use of Lemma 1.6(b); an analogous argument applies to §2.3(f3); we leave §2.3(h2) to the reader.

2.20. The same argument as in Proposition 2.19 gives the following.

(a) $V_{\mathscr{A}'}^+$ (resp. $V_{\mathscr{A}'}^-$) is the $\mathscr{A}'$-algebra defined by the generators E_α (resp. F_α) ($\alpha \in R^+$) and the relations 2.19(a1)–(a4) (resp. 2.19(b1)–(b4)).

(b) $V_{\mathscr{A}'}^0$ is the $\mathscr{A}'$-algebra defined by the generators K_i and K_i^{-1} ($i \in [1, n]$) and the relations 2.19(c1), (c2).

Lemma 2.21. *The elements in Proposition* 2.14(a) *form an* $\mathscr{A}'$*-basis for* $V^0_{\mathscr{A}'}$.

Proof. They generate $V^0_{\mathscr{A}'}$ by Proposition 2.14. Fix an integer $q \geq 1$. Consider the elements of $V^0_{\mathscr{A}'}$ of the form given in Proposition 2.14(a) with index subject to $\delta_i \in \{0, 1\}$, $0 \leq t_i \leq q$. (There are $2^n(q+1)^n$ such indices.) It is enough to show that they span an $\mathscr{A}'$-subspace X_q of dimension $2^n(q+1)^n$. Let X'_q be the subspace of $V^0_{\mathscr{A}'}$ spanned by the elements $K_1^{i_1}K_2^{i_2}\cdots K_n^{i_n}$ with $-q \leq i_1 \leq q+1, \dots, -q \leq i_n \leq q+1$. By §2.20(b) we have $\dim X'_q = 2^n(q+1)^n$. It is clear that $X_q = X'_q$. Hence $\dim X_q = 2^n(q+1)^n$ and the lemma is proved.

2.22. Since $V^0_{\mathscr{A}'}$ is isomorphic (by Lemma 1.12(b) and §2.20(b)) to $U^0_{\mathscr{A}'}$, we see that we have the following variant of Proposition 1.13:

(a) The elements

$$F^{\psi'}\prod_{i=1}^{n}\left(K_i^{\delta_i}\begin{bmatrix}K_i;0\\t_i\end{bmatrix}\right)E^{\psi} \qquad (\psi, \psi' \in \mathbf{N}^{R^+}, \delta_i \in \{0, 1\}, t_i \geq 0)$$

form an $\mathscr{A}'$-basis of $U_{\mathscr{A}'}$. (Here $\left[\begin{smallmatrix}K_i;0\\t_i\end{smallmatrix}\right] \in U_{\mathscr{A}'}$ is defined by §2.20(e).)

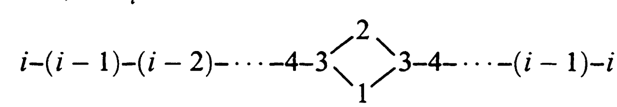
3. Properties of roots

3.1. For any $i \in [1, n]$, we define a graph Γ_i with a label in $[1, n]$ placed at each vertex as follows.

Type A_n: Γ_i is

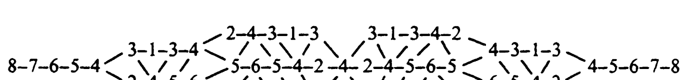
$$i\text{–}(i-1)\text{–}(i-2)\text{–}\cdots\text{–}2\text{–}1$$

Type D_n $(n \geq 4)$: Γ_i is

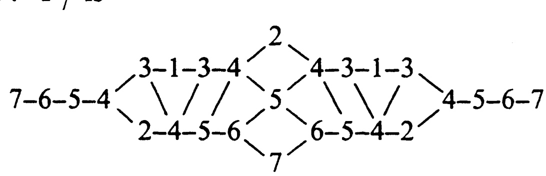


if $i \geq 3$, and $\{i\}$ if $i = 1$ or 2.

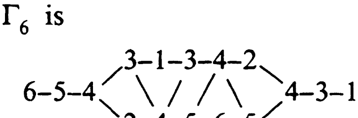
Type E_8: Γ_8 is



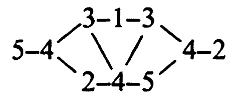
Types E_8, E_7: Γ_7 is



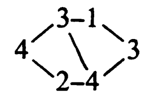
Types E_8, E_7, E_6: Γ_6 is



Γ_5 is



Γ_4:



Γ_3 is 3–1, Γ_2 is $\{2\}$, and Γ_1 is $\{1\}$.
The vertices of Γ_i are arranged in columns as shown, and we see that

(a) If $k \neq l$ are the labels attached to two vertices in the same column of Γ_i, then $a_{k,l} = 0$.

(b) Two vertices of Γ_i (with labels k, l) are joined in Γ_i if and only if they lie in consecutive columns and $a_{k,l} = -1$.

3.2. For any subset Z of the set $\mathscr{V}$ of vertices of Γ_i we define an element $w_Z \in W$ as follows. For each $\pi \in Z$, let $s(\pi)$ be $s_k \in W$ where k is the label of π. Then $w_Z = \prod_{\pi \in Z} s(\pi)$; the factors are written in the natural order of columns of Γ_i (first the factors with π in $Z \cap$ (first column), then the factors with π in $Z \cap$ (second column), etc.). The s_π with π in the same column commute with each other by §3.1(a).

3.3. We define a partial order $\leq$ on the set $\mathscr{V}$. If $\pi, \pi' \in \mathscr{V}$, we say that $\pi \leq \pi'$ if there exists a sequence of vertices $\pi_0, \pi_1, \dots, \pi_m$ with $\pi = \pi_0$ and $\pi' = \pi_m$ such that for any $0 \leq j \leq m-1$, π_{i+1} is joined with π_i and lies to the right of π_i.

The following property of $\leq$ can be easily verified.

(a) *Let $\pi, \pi' \in \mathscr{V}$ be such that $\pi \not\leq \pi'$ and the column containing π is to the left of the column containing π'; let k, k' be the labels of π, π'. Then $a_{k,k'} = 0$.*

From this and the definition in §3.2 we deduce the following.

(b) *Let Z' and Z be two disjoint subsets of $\mathscr{V}$ such that $\pi \not\leq \pi'$ whenever $\pi' \in Z'$, $\pi \in Z$, and π is in a column to the left of that of π'. Then $w_{Z'} w_Z = w_{Z' \cup Z}$.*

3.4. Let π_1 be a vertex of Γ_i. We define some subsets of $\mathscr{V}$:

$$[\geq \pi_1] = \{\pi \in \mathscr{V} | \pi \geq \pi_1\}, \qquad [\not\geq \pi_1] = \{\pi \in \mathscr{V} | \pi \not\geq \pi_1\}.$$

If $\pi_1 \leq \pi_2$ are joined in Γ_i, we also define

$$A = \{\pi \in \mathscr{V} | \pi \not\geq \pi_2, \pi \geq \pi_1\}, \qquad B = \{\pi \in \mathscr{V} | \pi \not\geq \pi_2, \pi \geq \pi_1, \pi \neq \pi_1\}.$$

Now §3.3(b) is clearly applicable with $(Z', Z) = ([\not\geq \pi_1], [\geq \pi_1])$, or $([\not\geq \pi_1], A)$, or $(\{\pi_1\}, B)$ and it yields

(a) $$w_{[\not\geq \pi_1]} \cdot w_{[\geq \pi_1]} = w_{\mathscr{V}},$$

(b) $$w_{[\not\geq \pi_1]} \cdot w_A = [w_{\not\geq \pi_2}],$$

(c) $$w_{\{\pi_1\}} \cdot w_B = w_A.$$

From (b) and (c) we deduce

(d) $$w_{[\ngeq \pi_2]} = w_{[\ngeq \pi_1]} \cdot w_{\{\pi_1\}} \cdot w_B .$$

We also note that

(e) if $\pi \in B$ has label k and π_2 has label l, then $a_{k,l} = 0$.

(Indeed, if π is in the same column as π_2, then we may use §3.1(a) since $\pi \neq \pi_2$. If π is not in the same column as π_2, then it is in a column to the right of that of π_2, since $\pi \geq \pi_1$ and $\pi \neq \pi_1$; using $\pi \ngeq \pi_2$ and §3.3(a) it again follows that $a_{k,l} = 0$.)

One can easily verify that

(f) $$l(w_{\mathscr{Y}}) = \#\mathscr{Y} .$$

Hence from (a), we see that both inequalities $l(w_{[\ngeq \pi_1]}) \leq \#[\ngeq \pi_1]$ and $l(w_{[\geq \pi_1]}) \leq \#[\geq \pi_1]$ must be equalities. Thus, we have

(g) $$l(w_{[\ngeq \pi_1]}) = \#[\ngeq \pi_1], \quad \text{and similarily,} \quad l(w_{[\ngeq \pi_2]}) = \#[\ngeq \pi_2].$$

From this and (b) we see that the inequality $l(w_B) \leq \#B$ must be an equality

(h) $$l(w_B) = \#(B).$$

3.5. With the notation in 3.4, we see from §3.4(d), (h) that

$$l(w_{[\ngeq \pi_1]} s_q) = l(w_{[\ngeq \pi_1]}) + 1 ,$$

where q is the label of π_1. It follows that

(a) $$\beta = w_{[\ngeq \pi_1]}(\alpha_q)$$

is a positive root.

One can verify that the correspondence $\pi_1 \longmapsto \beta$, given by (a), defines a bijection

(b) $$\mathscr{Y} \xrightarrow{\approx} \{\beta \in R^+ | g(\beta) = i\} .$$

For any $\beta \in R^+$ with $g(\beta) = i$, we shall denote by π_β the corresponding vertex of Γ_i, by i_β the label of π_β, and by w_β the element $w_{[\ngeq \pi_\beta]}$ of W. Thus, (a) can be rewritten as

(c) $$\beta = w_\beta(\alpha_{i_\beta}) .$$

The bijection (b) has the following property:

(d) the equivalence relation on $\mathscr{Y}$ defined by the columns of Γ_i corresponds to the equivalence relation on $\{\beta \in R^+ | g(\beta) = i\}$ defined by the boxes; moreover the natural order of the columns of Γ_i is compatible with the order in §2.9(a) on the set of boxes.

For example, in type E_8, the middle vertex of Γ_8 (with label 4) corresponds to the highest root. Moreover,

(e) if $\beta = \alpha_i$, then $w_\beta = e$, $i_\beta = i$, and $\pi_\beta =$ minimal element of $\mathscr{Y}$ for $\leq$.

3.6. Let $\beta \in R^+$ be such that $g(\beta) = i$ and let $j \in [1, n]$ be such that $j < i$ and $(\beta, \alpha_j) \in \{0, -1\}$. Assume that, in type E_8, β is not the highest root. One can verify that

(a) $w_\beta^{-1}(\alpha_j) \in \Pi$; if, in addition $(\beta, \alpha_j) = -1$ and $\beta' = \beta + \alpha_j$, then $w_\beta^{-1}(\alpha_j) = \alpha_{i_{\beta'}}$.

3.7. Assume that we are in type E_8, and that $i = 8$. Let $\beta \in R^+_{8,14}$ and $\beta' \in R^+_{8,15}$ be such that $\beta + \beta' = \beta_0$ (the highest root). Then $i_\beta = i_{\beta'}$; we denote this common value by l. We have $l \in \{2, 3, 5\}$. Let l', l'' be such that l, l', l'' is a permutation of $2, 3, 5$.

Let Z be the set of all $\pi \in \mathscr{V}$ which are in one of the first 13 columns of Γ_8; let $w' = w_Z$. We have

(a) $$w_\beta = w'y, \quad l(w_\beta) = l(w') + l(y), \quad y = s_{l'}s_{l''},$$

(b) $$w_{\beta'} = w's_2s_3s_5s_4z, \qquad l(w_{\beta'}) = l(w') + 4 + l(z),$$

(c) $$w_{\beta_0} = w's_2s_3s_5, \qquad l(w_{\beta_0}) = l(w') + 4,$$

where

(d) z is a product of various s_k with $a_{k,l} = 0$.

4. The isomorphism $V \xrightarrow{\approx} U$

Proposition 4.1. *There is a unique $\mathscr{A}'$-algebra homomorphism $V^+_{\mathscr{A}'} \to U_{\mathscr{A}'}$ which takes any E_β $(\beta \in R^+)$ to $T_{w_\beta}(E_{i_\beta})$ (w_β and i_β as in* §3.5).

Proof. We must only verify that the relations in Proposition 2.19(a1)–(a4) are verified.

Let $\beta \in R^+$ and $j \in [1, n]$ be such that $h'(\beta) \in \mathbb{Z}$, $j \in [1, n]$, $j < i$, and $(\beta, \alpha_j) \in \{0, -1\}$.

By §3.6(a) there exists $h \in [1, n]$ such that

(a) $$w_\beta(\alpha_h) = \alpha_j.$$

From Proposition 1.8(d) and §3.5(e) we see that

(b) $$T_{w_\beta}(E_h) = E_j = T_{w_{\alpha_j}}(E_j).$$

We have

(c) $$(\beta, \alpha_j) = (w_\beta(\alpha_{i_\beta}), w_\beta(\alpha_k)) = (\alpha_{i_\beta}, \alpha_h) = a_{h, i_\beta}.$$

Assume first that $(\beta, \alpha_j) = 0$. Then $a_{h, i_\beta} = 0$, hence $E_hE_{i_\beta} = E_{i_\beta}E_h$ in $U_{\mathscr{A}'}$. Applying to this the algebra homomorphism $T_{w_\beta} : U_{\mathscr{A}'} \to U_{\mathscr{A}'}$ and using (b), we deduce

$$T_{w_{\alpha_j}}(E_j)T_{w_\beta}(E_{i_\beta}) = T_{w_\beta}(E_{i_\beta})T_{w_{\alpha_j}}(E_j).$$

This shows that the relation in Proposition 2.19(a1) is preserved.

Assume next that $(\beta, \alpha_j) = -1$. Then $a_{h,i_\beta} = -1$ by (c), hence we have the following identities in $U_{\mathscr{A}'}$:

$$\begin{cases} E_h E_{i_\beta} = vE_{i_\beta} E_h + vT_{i_\beta}(E_h), \\ vE_h T_{i_\beta}(E_h) = T_{i_\beta}(E_h)E_h, \\ vT_{i_\beta}(E_h)E_{i_\beta} = E_{i_\beta} T_{i_\beta}(E_h). \end{cases}$$

Applying to these identities the algebra homomorphism $T_{w_\beta} : U \to U$ and using (b), we deduce

$$\text{(d)} \qquad \begin{cases} T_{w_{\alpha_j}}(E_j) \cdot T_{w_\beta}(E_{i_\beta}) = vT_{w_\beta}(E_{i_\beta}) \cdot T_{w_{\alpha_j}}(E_j) + vT_{w_\beta}T_{i_\beta}(E_h), \\ vT_{w_{\alpha_j}}(E_j) \cdot T_{w_\beta}T_{i_\beta}(E_h) = T_{w_\beta}T_{i_\beta}(E_h) \cdot T_{w_{\alpha_j}}(E_j), \\ vT_{w_\beta}T_{i_\beta}(E_h) \cdot T_{w_\beta}(E_{i_\beta}) = T_{w_\beta}(E_{i_\beta}) \cdot T_{w_\beta}T_{i_\beta}(E_h). \end{cases}$$

Let $\beta' = \beta + \alpha_j$. By §3.6(a) we have

$$\text{(e)} \qquad h = i_{\beta'}.$$

We can apply the discussion in §3.4 to $\pi_1 = \pi_\beta$ and $\pi_2 = \pi_{\beta'}$. (These are joined in the graph since $a_{i_{\beta'}, i_\beta} = -1$, by (e) and (c).) If B is as in that discussion, we have (by §3.4(e))

$$\text{(f)} \qquad T_{w_B}(E_{i_{\beta'}}) = E_{i_{\beta'}}.$$

By §3.4(d), (g), (h), we have $T_{w_{\beta'}}(E_{i_{\beta'}}) = T_{w_\beta} T_{i_\beta} T_{w_B}(E_{i_{\beta'}})$, hence

$$\text{(g)} \qquad T_{w_\beta} T_{i_\beta}(E_h) = T_{w_{\beta'}}(E_{i_{\beta'}}) \quad \text{(by (f) and (e))}.$$

Substituting (g) into (d), we obtain three identities which show that the relations in Proposition 2.19(a2)–(a4) (in the situation of Proposition 2.19(e1)) are preserved. It remains to show that the relations in Proposition 2.19(a2)–(a4) (in the situation of Proposition 2.19(e2)) are preserved. By Remark 2.4 we can assume that we are in type E_8. Let β and β' be as in §3.7. In the rest of this proof, we use the notation in §3.7. In $U_{\mathscr{A}'}$ we have the identities

$$\begin{cases} E_4 E_l = vE_l E_4 + vT_l(E_4), \\ vE_4 \cdot T_l(E_4) = T_l(E_4) \cdot E_4, \\ vT_l(E_4) \cdot E_l = E_l \cdot T_l(E_4). \end{cases}$$

Applying the algebra homomorphism $T_{w_\beta} : U_{\mathscr{A}'} \to U_{\mathscr{A}'}$ and using $i_\beta = l$ (see §3.7) we obtain the identities

$$\text{(h)} \qquad \begin{cases} T_{w_\beta}(E_4) T_{w_\beta}(E_{i_\beta}) = vT_{w_\beta}(E_{i_\beta}) T_{w_\beta}(E_4) + vT_{w_\beta} T_l(E_4), \\ vT_{w_\beta}(E_4) \cdot T_{w_\beta} T_l(E_4) = T_{w_\beta} T_l(E_4) \cdot T_{w_\beta}(E_4), \\ vT_{w_\beta} T_l(E_4) \cdot T_{w_\beta}(E_{i_\beta}) = T_{w_\beta}(E_{i_\beta}) \cdot T_{w_\beta} T_l(E_4). \end{cases}$$

We have

$$\begin{aligned} T_{w_{\beta'}}(E_{i_{\beta'}}) &= T_{w_\beta s_l s_4 z}(E_l) = T_{w_\beta} T_{s_l} T_{s_4} T_z(E_l) \quad \text{(see §3.7(a), (b))} \\ &= T_{w_\beta} T_{s_l} T_{s_4}(E_l) \quad \text{(see §3.7(d))} \\ &= T_{w_\beta}(E_4) \quad \text{(see §1.3(f))}, \\ T_{w_{\beta_0}}(E_{i_{\beta_0}}) &= T_{w_\beta s_l}(E_4) = T_{w_\beta} T_l(E_4). \end{aligned}$$

Substituting in (h), we obtain

$$\begin{cases} T_{w_{\beta'}}(E_{i_{\beta'}}) T_{w_\beta}(E_{i_\beta}) = v T_{w_\beta}(E_{i_\beta}) T_{w_{\beta'}}(E_{i_{\beta'}}) + v T_{w_{\beta_0}}(E_{i_{\beta_0}}), \\ v T_{w_{\beta'}}(E_{i_{\beta'}}) T_{w_{\beta_0}}(E_{i_{\beta_0}}) = T_{w_{\beta_0}}(E_{i_{\beta_0}}) \cdot T_{w_{\beta'}}(E_{i_{\beta'}}), \\ v T_{w_{\beta_0}}(E_{i_{\beta_0}}) T_{w_\beta}(E_{i_\beta}) = T_{w_\beta}(E_{i_\beta}) T_{w_{\beta_0}}(E_{i_{\beta_0}}), \end{cases}$$

which shows that the relations in Proposition 2.19(a2)–(a4) are verified in the situation of Proposition 2.19(e2). The proposition is proved.

Proposition 4.2. *There is a unique $\mathscr{A}'$-algebra homomorphism $V_{\mathscr{A}'} \to U_{\mathscr{A}'}$ which takes E_β to $T_{w_\beta}(E_{i_\beta})$, F_β to $T_{w_\beta}(F_{i_\beta})$ ($\beta \in R^+$, notation of* §3.5), *and $K_i^{\pm 1}$ to $K_i^{\pm 1}$ for all i.*

Proof. The uniqueness is clear. To prove existence, we first define an $\mathscr{A}'$-algebra homomorphism $V^-_{\mathscr{A}'} \to U_{\mathscr{A}'}$ as a composition $V^-_{\mathscr{A}'} \to (V^+_{\mathscr{A}'})^{\text{opp}} \to U^{\text{opp}}_{\mathscr{A}'} \to U_{\mathscr{A}'}$ (the first map as in §2.3(a), the second one as in Proposition 4.1, and the third one given by Ω in Lemma 1.2(a)). This homomorphism takes F_β to $T_{w_\beta}(F_{i_\beta})$. It follows that the map on generators given in the statement respects the relations in Proposition 2.19(b1)–(b4) of $V_{\mathscr{A}'}$; by Proposition 4.1 it also respects the relations in Proposition 2.19(a1)–(a4) of $V_{\mathscr{A}'}$. The remaining relations in Proposition 2.19(c1)–(d3) of $V_{\mathscr{A}'}$ are clearly respected in $E_{\alpha_i} \to E_i$, $F_{\alpha_i} \to F_i$. The proposition is proved.

Corollary 4.3. *There is a unique $\mathscr{A}$-algebra homomorphism $\Phi : V \to U$ which take $E_\beta^{(N)}$ to $T_{w_\beta}(E_{i_\beta}^{(N)})$, $F_\beta^{(N)}$ to $T_{w_\beta}(F_{i_\beta}^{(N)})$ ($\beta \in R^+$, $N \geq 0$), and $K_i^{\pm 1}$ to $K_i^{\pm 1}$ for all i.*

Proof. The uniqueness follows from Proposition 2.17(a). To prove existence, we consider the composition $V \to V_{\mathscr{A}'} \to U_{\mathscr{A}'}$ (the first map is $\xi \to \xi \otimes 1$, the second one is given by Proposition 4.2). This satisfies the requirements, with U replaced by $U_{\mathscr{A}'}$. It remains to show that the image of our homomorphism $V \to U_{\mathscr{A}'}$ is contained in U; this follows from the fact that the images of the indicated $\mathscr{A}$-algebra generators are contained in U, by Proposition 1.7.

4.4. Assume for example that we are in type A_n. Any $\beta \in R^+$ can be written uniquely as $\beta = s_l s_{l-1} \cdots s_{l-m+1}(\alpha_{l-m})$ for some $m < l$ in $[1, n]$. The homomorphism in Proposition 4.2 takes E_β to $T_{s_l} T_{s_{l-1}} \cdots T_{s_{l-m+1}}(E_{l-m})$, F_β to $T_{s_l} T_{s_{l-1}} \cdots T_{s_{l-m+1}}(F_{l-m})$, and $K_i^{\pm 1}$ to $K_i^{\pm 1}$.

Theorem 4.5. (a) *The elements in Proposition* 2.17(b) *form a basis of* V *as an* $\mathscr{A}$*-module; their images under* $\Phi: V \to U$ *(in Corollary* 4.3) *form a basis of* U *as an* $\mathscr{A}$*-module and of* $U_{\mathscr{A}'}$ *as an* $\mathscr{A}'$*-module.*

(b) Φ *is an* $\mathscr{A}$*-algebra isomorphism; it induces an* $\mathscr{A}'$*-algebra isomorphism*

$$V_{\mathscr{A}'} \xrightarrow{\approx} U_{\mathscr{A}'}.$$

(c) *We have* $U \otimes_{\mathscr{A}} \mathscr{A}' \xrightarrow{\approx} U_{\mathscr{A}'}$.

Proof. The image of Φ contains the set of $\mathscr{A}$-algebra generators of U consisting of $E_i^{(N)}$, $F_i^{(N)}$, and $K_i^{\pm 1}$ $(i \in [1, n], N \geq 0)$, hence Φ is surjective. The elements in Proposition 2.17(b) form a set of $\mathscr{A}$-module generators of V (see Proposition 2.17); they are mapped by Φ to a basis of $U_{\mathscr{A}'}$ by the variant in §2.22(a) of Proposition 1.13. The theorem follows.

4.6. One can interpret Theorem 4.5(b) as providing a presentation of U by generators and relations (those of V).

4.7. The same argument shows that Φ defines isomorphisms $V^+ \xrightarrow{\approx} U^+$ and $V^- \xrightarrow{\approx} U^-$, and that the elements in Proposition 2.12(b) (resp. §2.13(c)) form an $\mathscr{A}$-basis for V^+ (resp. V^-).

From now on we shall identify $V = U$, $V^+ = U^+$, and $V^- = U^-$ using the previous isomorphisms. We shall write U^0 for the subalgebra of U corresponding to $V^0 \subset V$.

Proposition 4.8. *There is a unique Hopf algebra structure on the* $\mathscr{A}$*-algebra* U *with comultiplication defined by*

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

(*Here* $i \in [1, n]$, $N \geq 0$.)

Proof. From §0.4(b) we see that Δ satisfies the identities above on $U_{\mathscr{A}}$. The proposition therefore follows from Theorem 4.5(c).

5. The algebras u, $'\mathrm{u}$

5.1. We fix an integer $l' \geq 1$. Let $\mathscr{B}$ be the quotient ring of $\mathscr{A}$ by the ideal generated by the l'th cyclotomic polynomial $\phi_{l'} \in \mathbb{Z}[v]$. (Thus, $\phi_1 = v - 1$, $\phi_2 = v + 1$, etc.) We shall denote the image of $v \in \mathscr{A}$ and of $\left[\begin{smallmatrix} m \\ r \end{smallmatrix}\right] \in \mathscr{A}$ in $\mathscr{B}$ by the same letters. Let $l \geq 1$ be defined by

$$l = \begin{cases} l' & \text{if } l' \text{ is odd}, \\ l'/2 & \text{if } l' \text{ is even}. \end{cases}$$

We then have (in $\mathscr{B}$)

(a) $$\phi_l(v^2) = 0, \qquad v^l = (-1)^{l'+1}, \qquad v^{2l} = 1.$$

We shall need the following result.

(b) If $0 \le N < l$, $0 \le M < l$, $N + M \ge l$, then $\begin{bmatrix} N+M \\ N \end{bmatrix} = 0$ in $\mathscr{B}$.

Indeed, $\left[\begin{smallmatrix} N+M \\ N \end{smallmatrix}\right] \cdot [N]![M]! = [N+M]!$ in $\mathscr{A}$. In $\mathscr{B}$, we have $[N]! \ne 0$, $[M]! \ne 0$, and $[N+M]! = 0$. Since $\mathscr{B}$ is an integral domain, (b) follows.

5.2. We define the $\mathscr{B}$-algebras $U_{\mathscr{B}}^+$, $U_{\mathscr{B}}^-$, $U_{\mathscr{B}}^0$, and $U_{\mathscr{B}}$ by applying $(\ )\otimes_{\mathscr{A}}\mathscr{B}$ to U^+, U^-, U^0, and U. (We regard $\mathscr{B}$ as an $\mathscr{A}$-algebra via the canonical map $\mathscr{A} \to \mathscr{B}$.) We could equally well define $U_{\mathscr{B}}^+$, $U_{\mathscr{B}}^-$, $U_{\mathscr{B}}^0$, and $U_{\mathscr{B}}$ as the $\mathscr{B}$-algebras defined by the generators and relations of V^+, V^-, V^0, and V respectively.

Let $\mathfrak{u}^+$, $\mathfrak{u}^-$, $\mathfrak{u}^0$, and $\mathfrak{u}$ be the $\mathscr{B}$-subalgebras of $U_{\mathscr{B}}^+$, $U_{\mathscr{B}}^-$, $U_{\mathscr{B}}^0$, and $U_{\mathscr{B}}$ generated respectively by the elements $E_i^{(N)}$ $(1 \le i \le n,\ 0 \le N \le l-1)$; $F_i^{(N)}$ $(1 \le i \le n,\ 0 \le N \le l-1)$; $K_i^{\pm 1}$, $\left[\begin{smallmatrix} K_i;0 \\ t_i \end{smallmatrix}\right]$ $(1 \le i \le n,\ 0 \le t_i \le l-1)$; and $E_i^{(N)}$, $F_i^{(N)}$, $K_i^{\pm 1}$ $(1 \le i \le n,\ 0 \le N \le l-1)$.

5.3. We want to describe the algebras $\mathfrak{u}^+$, $\mathfrak{u}^-$, $\mathfrak{u}^0$, and $\mathfrak{u}$ in terms of generators and relations. For this purpose, we define $\mathscr{B}$-algebras $\hat{\mathfrak{u}}^+$, $\hat{\mathfrak{u}}^-$, $\hat{\mathfrak{u}}^0$, and $\hat{\mathfrak{u}}$ by the generators and relations shown below.

$\hat{\mathfrak{u}}^+$: generators $E_\alpha^{(N)}$ $(\alpha \in R^+,\ 0 \le N \le l-1)$; relations (d1) from §2.3 with M and N satisfying $M + N \le l-1$ and (d2)–(d5) from §2.3 with M and N satisfying $M, N \le l-1$, and the additional relations

(a) $$E_\alpha^{(N)} E_\alpha^{(M)} = 0 \quad \text{if } N, M \le l-1,\ N+M \ge l.$$

$\hat{\mathfrak{u}}^-$: generators $F_\alpha^{(N)}$ $(\alpha \in R^+,\ 0 \le N \le l-1)$; relations (f1) from §2.3 with M and N satisfying $M + N \le l-1$ and (f2)–(f5) from §2.3 with M and N satisfying $M, N \le l-1$, and the additional relations

(b) $$F_\alpha^{(N)} F_\alpha^{(M)} = 0 \quad \text{if } N, M \le l-1,\ N+M \ge l.$$

$\hat{\mathfrak{u}}^0$: generators K_i, K_i^{-1}, $\left[\begin{smallmatrix} K_i;c \\ t \end{smallmatrix}\right]$ $(0 \le t \le l-1,\ c \in \mathbb{Z},\ 1 \le i \le n)$; relations (from §2.3)(g7); (g5) (only if $l \ge 2$); (g6), (g9), (g10) with $t \le l-1$; (g8) (with $t + t' \le l-1$); and the additional relations (also from §2.3): if $t, t' \le l-1$, $t + t' \ge l$, the left-hand side of (g8) is zero; if $l = 1$, the right-hand side of (g5) is zero.

$\hat{\mathfrak{u}}$: generators are those of $\hat{\mathfrak{u}}^+$, $\hat{\mathfrak{u}}^-$, $\hat{\mathfrak{u}}^0$ together; relations are those satisfied in $\hat{\mathfrak{u}}^+$, $\hat{\mathfrak{u}}^-$, $\hat{\mathfrak{u}}^0$; in addition we have the relations (h1)–(h6) from §2.3 in which N, M, and t are restricted to be $\le l-1$.

5.4. We have the following results.

(a) $\hat{\mathrm{u}}^+$ is generated as a $\mathscr{B}$-algebra by the elements $E_{\alpha_i}^{(N)}$ $(1 \le i \le n,$ $0 \le N \le l-1)$ and as a $\mathscr{B}$-module by the elements $\prod_{\alpha \in R^+} E_\alpha^{(N_\alpha)}$ $(0 \le N_\alpha \le l-1)$.

(b) $\hat{\mathrm{u}}^-$ is generated as a $\mathscr{B}$-algebra by the elements $F_{\alpha_i}^{(N)}$ $(1 \le i \le n,$ $0 \le N \le l-1)$ and as a $\mathscr{B}$-module by the elements $\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)}$ $(0 \le N_\alpha \le l-1)$.

(c) $\hat{\mathrm{u}}^0$ is generated as a $\mathscr{B}$-module by the elements $\prod_{i=1}^n (K_i^{\delta_i}\left[{K_i;0 \atop t_i}\right])$, $0 \le t_i \le l-1$, $\delta_i = 0, 1$.

(d) $\hat{\mathrm{u}}$ is generated as a $\mathscr{B}$-algebra by the elements $E_{\alpha_i}^{(N)}$, $F_{\alpha_i}^{(N)}$, and $K_i^{\pm 1}$ $(0 \le N \le l-1,\ 1 \le i \le n)$ and as a $\mathscr{B}$-module by the elements

$$\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)} \prod_{i=1}^n \left(K_i^{\delta_i}\begin{bmatrix} K_i;0 \\ t_i \end{bmatrix}\right) \prod_{\alpha \in R^+} E_\alpha^{(N'_\alpha)}$$

$$(0 \le N_\alpha \le l-1,\ 0 \le N'_\alpha \le l-1,\ 0 \le t_i \le l-1,\ \delta = 0, 1).$$

(The products over α are defined as in §§2.9 and 2.13(c).)

Although these results are not consequences of those in §2, they are proved by repeating essentially word by word the proofs of the corresponding results in §2.

5.5. There are unique $\mathscr{B}$-algebra homomorphisms $\hat{\mathrm{u}}^+ \to U_{\mathscr{B}}$, $\hat{\mathrm{u}}^- \to U_{\mathscr{B}}$, $\hat{\mathrm{u}}^0 \to U_{\mathscr{B}}$, and $\hat{\mathrm{u}} \to U_{\mathscr{B}}$ which take the generators given in §5.3 to the generators with the same name of $U_{\mathscr{B}}$. (This follows immediately from the definitions and from §5.1(b); here we think of $U_{\mathscr{B}}$ as $V \otimes_{\mathscr{A}} \mathscr{B}$.) These homomorphisms carry the set of $\mathscr{B}$-module generators of the four algebras, described in §5.4, onto a part of a $\mathscr{B}$-basis of $U_{\mathscr{B}}$ (see Theorem 4.5(a)). Hence these homomorphisms are injective and the sets of $\mathscr{B}$-module generators given in §5.4 are actually $\mathscr{B}$-bases. It is clear from the definition in §5.2, that their image is respectively u^+, u^-, u^0, u. Hence we have proved the following result.

Theorem 5.6. (a) *The homomorphisms in* §5.5 *define* $\mathscr{B}$*-algebra isomorphisms* $\hat{\mathrm{u}}^+ \xrightarrow{\approx} \mathrm{u}^+$, $\hat{\mathrm{u}}^- \xrightarrow{\approx} \mathrm{u}^-$, $\hat{\mathrm{u}}^0 \xrightarrow{\approx} \mathrm{u}^0$, *and* $\hat{\mathrm{u}} \xrightarrow{\approx} \mathrm{u}$.

(b) u^+, u^-, u^0, *and* u *are free* $\mathscr{B}$*-modules of rank* $l^{|R^+|}$, $l^{|R^+|}$, $(2l)^n$, *and* $2^n l^{|R|+n}$ *respectively.*

This can be regarded as providing a presentation of u^+, u^-, u^0 and u by generators and relations.

5.7. We denote the quotient field $\mathscr{B} \otimes_Z Q$ of $\mathscr{B}$ by $\mathscr{B}'$ (a cyclotomic field). Using the inclusion $\mathscr{B} \subset \mathscr{B}'$ we can form the $\mathscr{B}'$-algebras $'\mathrm{u}^+$, $'\mathrm{u}^-$, $'\mathrm{u}^0$, $'\mathrm{u}$, and $U_{\mathscr{B}'}$ by applying $(\ ) \otimes_{\mathscr{B}} \mathscr{B}'$ to u^+, u^-, u^0, u, and $U_{\mathscr{B}}$.

From the presentations in Theorem 5.6, we can deduce, as in Proposition 2.19, and §2.20 the following presentations:

$'\mathrm{u}^+$ is defined by generators E_α $(\alpha \in R^+)$ and relations (a1)–(a4) in Proposition 2.19 and $E_\alpha^l = 0$.

$'\mathrm{u}^-$ is defined by generators F_α $(\alpha \in R^+)$ and relations (b1)–(b4) in Proposition 2.19 and $F_\alpha^l = 0$.

$'\mathrm{u}^0$ is defined by generators K_i $(i \in [1, n])$ and relations (c1), (c2) in Proposition 2.19 and $K_i^{2l} = 1$.

$'\mathrm{u}$ is defined by generators E_α, F_α $(\alpha \in R^+)$, and K_i $(1 \le i \le n)$ and relations (a1)—(d3) in Proposition 2.19 and $E_\alpha^l = 0$, $F_\alpha^l = 0$, $K_i^{2l} = 1$.

5.8. From §§5.4 and 5.5 we deduce that $'\mathrm{u}^+$, $'\mathrm{u}^-$, $'\mathrm{u}^0$, and $'\mathrm{u}$ may be regarded as $\mathscr{B}'$-subalgebras of $U_{\mathscr{B}'}$ which admit the following bases as $\mathscr{B}'$-vector spaces:

$$'\mathrm{u}^+: \quad \prod_{\alpha\in R^+} E_\alpha^{N_\alpha} \qquad (0 \le N_\alpha \le l-1),$$

$$'\mathrm{u}^-: \quad \prod_{\alpha\in R^+} F_\alpha^{N_\alpha} \qquad (0 \le N_\alpha \le l-1),$$

$$'\mathrm{u}^0: \quad \prod_{i=1}^{n} K_i^{N_i} \qquad (0 \le N_i \le 2l-1),$$

$$'\mathrm{u}: \quad \prod_{\alpha\in R^+} F_\alpha^{N_\alpha} \prod_{i=1}^{n} K_i^{N_i} \prod_{\alpha\in R^+} E_\alpha^{N'_\alpha} \qquad (0 \le N_\alpha \le l-1, 0 \le N'_\alpha \le l-1,$$
$$0 \le N_i \le 2l-1).$$

In particular, $'\mathrm{u}^+$, $'\mathrm{u}^-$, and u^0 are subalgebras of $'\mathrm{u}$.

5.9. We wish to study the $'\mathrm{u}$-modules. They will be assumed to be finite dimensional over $\mathscr{B}'$. We shall assume that $l > 1$. Much of our treatment will imitate that in Curtis [3]. Let $v' = (-1)^{l'} v \in \mathscr{B}$; then v' is a primitive $(2l)$th root of 1.

Since the K_i commute with $K_i^{2l} = 1$ in $'\mathrm{u}$, any $'\mathrm{u}$-module M has a canonical decomposition $M = \oplus_{\underline{h}} M_{\underline{h}}$, where $\underline{h} = (h_1, \dots, h_n) \in (\mathbb{Z}/2l)^n$ and $\mathscr{M}_{\underline{h}} = \{x \in M | K_i x = v'^{h_i} x,\ 1 \le i \le n\}$.

The $\mathscr{M}_{\underline{h}}$ are the "weight spaces" of M and the $\underline{h}$ are the weights.

Let $M^0 = \{x \in M | E_\alpha x = 0\ \forall \alpha \in R^+\}$.

Lemma 5.10. (a) *Let I^+ (resp. I^-) be the ideal in $'\mathrm{u}^+$ (resp. $'\mathrm{u}^-$) spanned as a $\mathscr{B}'$-vector space by the nonempty words in E_α (resp. F_α), $\alpha \in R^+$. Then any element in I^+ (resp. I^-) is nilpotent.*

(b) *If $M \ne 0$, then $M^0 \cap M_{\underline{h}} \ne 0$ for some weight $\underline{h}$.*

Proof. Let us consider a sequence $\alpha^1, \alpha^2, \dots, \alpha^r$ in R^+ where $r > (l-1)\sum_{\alpha\in R^+} h(\alpha)$. By §4.7 we can write an identity in $U_{\mathscr{A}}^+$ expressing the product $E_{\alpha^1} E_{\alpha^2} \cdots E_{\alpha_r}$ as an $\mathscr{A}$-linear combination of basis elements $\prod_{\alpha\in R^+} E_\alpha^{(N_\alpha)}$;

moreover from the homogeneity of the relations defining $U^+_{\mathscr{A}}$ it is clear that we may assume that only basis elements satisfying $\sum_{\alpha\in R^+} N_\alpha h(\alpha) = \sum h(\alpha^i)$ will occur in the linear combination. For such basis elements we have $\sum_{\alpha\in R^+} N_\alpha h(\alpha) \geq r > (l-1)\sum_{\alpha\in R^+} h(\alpha)$, hence $N_\alpha > l$ for at least one α. Our identity in $U^+_{\mathscr{A}}$ gives rise to an identity in $U^+_{\mathscr{B}}$. But then $E_{\alpha^1}E_{\alpha^2}\cdots E_{\alpha^r}$ is in u, hence is a $\mathscr{B}$-linear combination of elements $\prod_{\alpha\in R^+} E_\alpha^{(N_\alpha)}$ with all $N_\alpha \leq l-1$. It follows that $E_{\alpha^1}E_{\alpha^2}\cdots E_{\alpha^r} = 0$ in $U^+_{\mathscr{B}}$. Hence the product of any r elements in I^+ is zero. In particular, any element of I^+ is nilpotent. The same argument applies to I^-, and (a) is proved. We now prove (b). By (a), the operators $1+\xi : M \to M$ ($\xi \in I^+$) form a group consisting of unipotent elements. Hence, by Kolchin's theorem there exists a nonzero vector $x \in M$ such that $(1+\xi)x = x$ for all $\xi \in I^+$. In particular we have $E_\alpha x = 0$ for all $\alpha \in R^+$. Thus $M^0 \neq 0$. Since M^0 is clearly stable under all $K_i : M \to M$, we deduce that $M^0 \cap M_{\underline{h}} \neq 0$ for some $\underline{h}$. The lemma is proved.

Proposition 5.11. *For any simple $'$u-module M there is a unique $\underline{h} \in (\mathbb{Z}/2l)^n$ such that $M^0 \cap M_{\underline{h}} \neq 0$. The correspondence $M \to \underline{h}$ defines a bijection between the set of isomorphism classes of simple $'$u-modules and the set $(\mathbb{Z}/2l)^n$.*

Proof. Let $\underline{h} = (h_1, \dots, h_n) \in (\mathbb{Z}/2l)^n$. Consider the $'$u-module $\mathscr{M}^{\underline{h}} = {}'\mathrm{u}/\mathscr{J}$, where $\mathscr{J}$ is the left ideal of $'$u generated by the elements E_α $(\alpha \in R^+)$ and $K_i - v'^{h_i}$ $(1 \leq i \leq n)$.

From §5.8 we see that $\mathscr{M}^{\underline{h}}$ is a free $'\mathrm{u}^-$-module with generator $\mathbf{1}$, the image of $1 \in {}'\mathrm{u}$ in $\mathscr{M}^{\underline{h}}$. Let $\widehat{\mathscr{M}} = I^- \cdot \mathbf{1} \subset \mathscr{M}^{\underline{h}}$ (I^- as in Lemma 5.10). We have $\mathscr{M}^{\underline{h}} = \widehat{\mathscr{M}} \oplus \mathscr{B}'\mathbf{1}$. Any element $x \in \mathscr{M}^{\underline{h}} - \widehat{\mathscr{M}}$ generates $\mathscr{M}^{\underline{h}}$ as a $'\mathrm{u}^-$-module. (Indeed we can write $x = \lambda(\xi+1)\mathbf{1}$, where $\lambda \in \mathscr{B}' - \{0\}$ and $\xi \in I^-$. Now ξ is nilpotent by Lemma 5.10(a), hence $\lambda(\xi+1)$ is invertible in $'\mathrm{u}^-$; we reduced to the case where $x = \mathbf{1}$, which is obvious.)

It follows that any $'$u-submodule of $\mathscr{M}^{\underline{h}}$ is contained in $\widehat{\mathscr{M}}$; hence so is the sum of all proper $'$u-submodules. Therefore $\mathscr{M}^{\underline{h}}$ has a unique maximal $'$u-submodule $\mathscr{M}^{\underline{h}}_{\max}$; it is contained in $\widehat{\mathscr{M}}$. Hence $\mathscr{L}^{\underline{h}} = \mathscr{M}^{\underline{h}}/\mathscr{M}^{\underline{h}}_{\max}$ is a simple $'$u-module. It satisfies $(\mathscr{L}^{\underline{h}})^0 \cap (\mathscr{L}^{\underline{h}})_{\underline{h}} \neq 0$; this intersection contains the image of $\mathbf{1}$.

Assume that $h' \in (\mathbb{Z}/2l)^n$ satisfies $(\mathscr{L}^{\underline{h}})^0 \cap (\mathscr{L}^{\underline{h}})_{\underline{h}'} \neq 0$ and let $\overline{x}$ be a nonzero vector in this intersection. We can find $x \in (\mathscr{M}^{\underline{h}})_{\underline{h}'}$ such that $x \longmapsto \overline{x}$ under the canonical map $\mathscr{M}^{\underline{h}} \to \mathscr{L}^{\underline{h}}$. Clearly $\overline{x}$ generates $\mathscr{L}^{\underline{h}}$ as a $'\mathrm{u}^-$-module, hence $'\mathrm{u}^- \cdot x + \mathscr{M}^{\underline{h}}_{\max} = \mathscr{M}^{\underline{h}}$. If $\underline{h}' \neq \underline{h}$ then $x \in \widehat{\mathscr{M}}$, hence $'\mathrm{u}^- \cdot x \in \widehat{\mathscr{M}}$; we have also $\mathscr{M}^{\underline{h}}_{\max} \subset \widehat{\mathscr{M}}$, hence the previous sum is contained in $\widehat{\mathscr{M}}$. This contradiction shows that $\underline{h}' = \underline{h}$.

In particular, we see that $\mathscr{L}^{\underline{h}}$ and $\mathscr{L}^{\underline{h}'}$ are isomorphic as $'$u-modules if and only if $\underline{h} = \underline{h}'$.

Now let M be any simple $'\mathrm{u}$-module. Choose $\underline{h}$ as in Lemma §5.10(b) and choose $x \in M^0 \cap M_{\underline{h}}$, $x \neq 0$. Then $'\mathrm{u} \to M$, $\xi \longmapsto \xi x$, factors through a nonzero $'\mathrm{u}$-module homomorphism $\phi : \mathscr{M}^{\underline{h}} \to M$. Since M is simple, ϕ must be onto and must vanish on $\mathscr{M}^{\underline{h}}_{\max}$. Hence ϕ defines a surjective homomorphisms $\mathscr{L}^{\underline{h}} \to M$ which is necessarily an isomorphism of $'\mathrm{u}$-modules. This completes the proof.

5.12. The formulas in Proposition 4.8 define Hopf algebra structures on $U_{\mathscr{B}}$, $U_{\mathscr{B}'}$, u, and $'\mathrm{u}$.

6. Relation with the algebra $\bar{\mathrm{u}}$

6.1. Let $K_{i,t} = K_i^{-t}\left[{K_i;0 \atop t}\right] \in U^0$ $(i \in [1, n],\ t \geq 0)$; and let $\widetilde{U}^0$ be the $\mathscr{A}$-submodule of U^0 spanned by the elements $\prod_{i=1}^n K_{i,t_i}$, where $t_i \geq 0$.

Lemma 6.2. (a) *$\widetilde{U}^0$ is an $\mathscr{A}$-subalgebra of U^0.*

(b) *For any integer $m \geq 0$, we have*

$$K_i^{2m+1} \sum_{t=0}^{m} (-1)^t \frac{[m]!}{[m-t]!} v^{-t(m-1)+t(t-1)/2} K_{i,t} = K_i \quad (in\ U^0).$$

Proof. From §2.3(g8) we see that for $t \geq 0$ and $t' \geq 1$,

$$\text{(c)}\quad K_{i,t}K_{i,t'} = \sum_{j=1}^{t'} (-1)^{j+1} v^{-tj} \begin{bmatrix} t+j-1 \\ j \end{bmatrix} K_{i,t}K_{i,t'-j} + v^{-tt'} \begin{bmatrix} t+t' \\ t \end{bmatrix} K_{i,t+t'}.$$

This shows by induction on t' that $K_{i,t}K_{i,t'} \in \widetilde{U}^0$ and (a) follows.

The proof of (b) is left to the reader.

6.3. We now fix l' and l as in §5.1 *and assume that $l' = l$ is odd*; $\mathscr{B}$ and $\mathscr{B}'$ are as in §§5.1 and 5.7.

Lemma 6.4. (a) *Assume $t = t' + t''l$, $0 \leq t' \leq l-1$, $t'' \geq 0$. Then*

$$K_{i,t} = K_{i,t'}K_{i,t''l} \quad (in\ U^0_{\mathscr{B}}).$$

(b) *The elements $\prod_{i=1}^n K_i^{l\delta_i} \prod_{i=1}^n K_{i,t_i}$ $(t_i \geq 0, \delta_i \in \{0, 1\})$ (of $U^0_{\mathscr{B}}$) form a $\mathscr{B}$-basis of $U^0_{\mathscr{B}}$.*

Proof. (a) follows immediately from §2.3(g3) with t and t' replaced by $t''l$ and t'; note that

$$\begin{bmatrix} t''l + t' \\ t''l \end{bmatrix} = 0 \quad \text{in } \mathscr{B},$$

and

$$\begin{bmatrix} K_i; -t''l \\ t' \end{bmatrix} = \begin{bmatrix} K_i; 0 \\ t' \end{bmatrix} \quad \text{in } U^0_{\mathscr{B}}.$$

We now prove (b). Let $\mathscr{M}$ be the $\mathscr{B}$-submodule of $U^0_{\mathscr{B}}$ generated by the elements in (b). From the identity $K_i^{2l} = 1$ in $U^0_{\mathscr{B}}$ and from Lemma 6.2(a) we see that $\mathscr{M}$ is a $\mathscr{B}$-subalgebra of $U^0_{\mathscr{B}}$. By Lemma 6.2(b) with $m = \frac{1}{2}(l-1)$, we have $K_1, \dots, K_n \in \mathscr{M}$. Hence $\mathscr{M}$ contains also $\left[{K_i;0 \atop t}\right] = K_i^t \cdot K_{i,t}$ $(t \geq 0)$. Since $U^0_{\mathscr{B}}$ is generated as a $\mathscr{B}$-algebra by the elements K_i and $\left[{K_i;0 \atop t}\right]$ $(1 \leq i \leq n, t \geq 0)$, it follows that $\mathscr{M}$ contains $U^0_{\mathscr{B}}$, hence $M = U^0_{\mathscr{B}}$. It remains to show that the elements in (b) are linearly independent. It is enough to show that they are linearly independent over $\mathscr{B}'$ in $U^0_{\mathscr{B}'}$.

For any sequence $\tau = (t_1'', \dots, t_n'')$ in $\mathbb{N}^n$, let ${}_\tau U^0_{\mathscr{B}'}$ be the $\mathscr{B}'$-subspace of $U^0_{\mathscr{B}'}$ spanned by the basis elements

(c) $$\prod_{i=1}^n K_i^{\delta_i} \prod_{i=1}^n \begin{bmatrix} K_i;0 \\ lt_i'' + t_i' \end{bmatrix} \qquad (0 \leq t_i' < l, \delta_i \in \{0, 1\}).$$

Clearly $U^0_{\mathscr{B}'} = \bigoplus_\tau ({}_\tau U^0_{\mathscr{B}'})$ and $\dim_{\mathscr{B}'}({}_\tau U^0_{\mathscr{B}'}) = 2^n l^n$.

Consider the $2^n l^n$ elements

(d) $$\prod_{i=1}^n K_i^{l\delta_i} \prod_{i=1}^n K_{i, lt_i''+t_i'} \qquad (0 \leq t_i' < l, \delta_i \in \{0, 1\})$$

for fixed τ. We will show that

(e) the elements (d) are contained in ${}_\tau U^0_{\beta'}$.

This implies that the elements (c) for various τ form a $\mathscr{B}'$-basis of $U^0_{\beta'}$, since we already know that they span $U^0_{\mathscr{B}'}$.

Let $\mathscr{N}_\tau$ be the $\mathscr{B}'$-subspace of $U^0_{\mathscr{B}'}$ spanned by the $2^n l^n$ elements $\prod_{i=1}^n K_i^{c_i} \times \prod_{i=1}^n K_{i, lt_i''}$ $(0 \leq c_i < 2l)$.

From (a) we see that ${}_\tau U^0_{\mathscr{B}'}$ is contained in $\mathscr{N}_\tau$; for dimension reasons, we must have ${}_\tau U^0_{\mathscr{B}'} = \mathscr{N}_\tau$. From (a) we also see that the elements (d) are contained in $\mathscr{N}_\tau$; hence they are contained in ${}_\tau U^0_{\mathscr{B}'}$. The lemma is proved.

6.5. We note that the elements $K_1^l - 1, K_2^l - 1, \dots, K_n^l - 1$ are central in $U_{\mathscr{B}}$, u, $U_{\mathscr{B}'}$, 'u, since $v^l = 1$ in $\mathscr{B}$ (we are using our assumption $l' = l =$ odd). Therefore the left ideal generated by these elements in one of our four rings is a two-sided ideal; factoring out by this two-sided ideal we get respectively the $\mathscr{B}$-algebras $\widetilde{U}_B$, ũ, and the $\mathscr{B}'$-algebras $\widetilde{U}_{\mathscr{B}'}$, 'ũ.

We shall denote the images of E_α, F_α, etc. in $\widetilde{U}_{\mathscr{B}}$, ũ, $\widetilde{U}_{\mathscr{B}'}$, 'ũ by the same letters. From the results in §5 and from Lemma 6.4(b) we deduce:

(a) the elements $\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)} \prod_{i=1}^n K_{i,t_i} \prod_{\alpha \in R^+} E_\alpha^{(N_\alpha')}$ $(N_\alpha, N_\alpha', t_i \geq 0)$ form a $\mathscr{B}$-basis of $\widetilde{U}_{\mathscr{B}}$ and a $\mathscr{B}'$-basis of $\widetilde{U}_{\mathscr{B}'}$.

(b) The elements $\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)} \prod_{i=1}^n K_{i,t_i} \prod_{\alpha \in R^+} E_\alpha^{(N_\alpha')}$ $(0 \leq N_\alpha, N_\alpha', t_1 < l)$ form a $\mathscr{B}$-basis of ũ and a $\mathscr{B}'$-basis of 'ũ.

In particular, we have

$$\tilde{U}_{\mathscr{B}} \otimes_{\mathscr{B}} \mathscr{B}' = \tilde{U}_{\mathscr{B}'}, \qquad \tilde{\mathrm{u}} \otimes_{\mathscr{B}} \mathscr{B}' = {}'\tilde{\mathrm{u}},$$
$$\tilde{\mathrm{u}} \subset \tilde{U}_{\mathscr{B}}, \qquad {}'\tilde{\mathrm{u}} \subset \tilde{U}_{\mathscr{B}'}.$$

It is clear that $\tilde{U}_{\mathscr{B}}$, $\tilde{\mathrm{u}}$, $\tilde{U}_{\mathscr{B}'}$, ${}'\tilde{\mathrm{u}}$ have natural Hopf-algebra structure so that the canonical maps $U_{\mathscr{B}} \to \tilde{U}_{\mathscr{B}}$, $\mathrm{u} \to \tilde{\mathrm{u}}$, $U_{\mathscr{B}'} \to \tilde{U}_{\mathscr{B}'}$, and ${}'\mathrm{u} \to {}'\tilde{\mathrm{u}}$ are compatible with the comultiplication.

6.6. From the definition of ${}'\tilde{\mathrm{u}}$, we see that the simple ${}'\tilde{\mathrm{u}}$-modules may be identified with the simple ${}'\mathrm{u}$-modules in which $K_1^l, K_2^l, \dots, K_n^l$ act as identity.

Hence, using Proposition 5.11, we have a commutative diagram

$$\begin{array}{ccc} \text{set of simple } {}'\tilde{\mathrm{u}}\text{-modules up to isomorphism} & \xrightarrow{\approx} & (\mathbb{Z}/l)^n \\ \big\downarrow & & \big\downarrow j \\ \text{set of simple } {}'\mathrm{u}\text{-modules up to isomorphism} & \xrightarrow[5.11]{\approx} & (\mathbb{Z}/2l)^n \end{array}$$

where $j(h_1, \dots, h_2) = (2h_1, \dots, 2h_n)$.

6.7. Let $U_{\mathbb{Z}}$ and U_Q be the rings obtained from U by applying $\bigotimes_{\mathscr{A}} \mathbb{Z}$ and $\bigotimes_{\mathscr{A}} Q$, where $\mathbb{Z}$ and Q are regarded as $\mathscr{A}$-algebras with v acting as 1. These are special cases of $U_{\mathscr{B}}$ and $U_{\mathscr{B}'}$ in the case where $l = l' = 1$. The definition of §6.5 is applicable and gives two rings $\tilde{U}_{\mathbb{Z}}$, $\tilde{U}_Q = \tilde{U}_{\mathbb{Z}} \otimes Q$ obtained by dividing $U_{\mathbb{Z}}$ and U_Q by the left (or two-sided) ideal generated by $K_1 - 1, K_2 - 1, \dots, K_n - 1$.

Let $\overline{U}$ and $\overline{U}_Q$ be as in §0.1.

(a) *There is a unique Q-algebra homomorphism $\overline{U}_Q \to \tilde{U}_Q$ such that $\overline{E}_i \to E_i$, $\overline{F}_i \to F_i$, and $H_i \to E_iF_i - F_iE_i$ $(1 \le i \le n)$.*

We must verify that the relations in §0.1(b1)–(b5) are preserved. The only nontrivial verification is that of §0.1(b2).

In $U_{\mathscr{A}}$ we have

$$\begin{aligned}(v+1)&\left(\frac{K_i - K_i^{-1}}{v - v^{-1}} E_j - E_j \frac{K_i - K_i^{-1}}{v - v^{-1}}\right) \\ &= (v+1)a_{ij}E_j + (v+1)E_j\left(\frac{v^{a_{ij}} - v^{-a_{ij}}}{v - v^{-1}} - a_{ij}\right) \\ &\quad + E_j(K_i - 1)\left(\frac{v^{a_{ij}} - 1}{1 - v^{-1}} + K_i^{-1}\frac{v^{-a_{ij}} - 1}{1 - v^{-1}}\right).\end{aligned}$$

This gives rise to an identity in $\tilde{U}_Q$ which shows that §0.1(b2) (for E_j) is preserved; an analogous argument applies to §0.1(b2) for F_j.

The homomorphism (a) takes $\frac{1}{t!}H_i(H_i - 1)\cdots(H_i - t + 1)$ to

$$\frac{1}{t!}\left(\begin{bmatrix} K_i; 0 \\ t \end{bmatrix}\right)\left(\begin{bmatrix} K_i; 0 \\ t \end{bmatrix} - 1\right)\cdots\left(\begin{bmatrix} K_i; 0 \\ t \end{bmatrix} - t + 1\right)$$

which by [9, 4.3] is equal to $K_{i,t}$ in $\widetilde{U}_Q$. Hence (a) takes a basis of $\overline{U}_Q$ given by the Poincaré-Birkhoff-Witt theorem onto the basis of $\widetilde{U}_Q$ given by §6.5(a) (for $l = 1$). It follows that

(b) *the homomorphism* (a) *is an algebra isomorphism*.

It is clear that (a) takes $\overline{E}_i^{(N)}$ to $E_i^{(N)}$ and $\overline{F}_i^{(N)}$ to $F_i^{(N)}$, hence it defines an isomorphism of the subring generated by the $\overline{E}_i^{(N)}$ and $\overline{F}_i^{(N)}$ onto the subring generated by the $E_i^{(N)}$ and $F_i^{(N)}$. Thus

(c) *the isomorphism* (a) *restricts to a ring isomorphism* $\overline{U} \xrightarrow{\approx} \widetilde{U}_{\mathbb{Z}}$.

It is clear that this is compatible with the comultiplications.

In the remainder of this section we assume that l and l' in §6.3 are both equal to p, an odd prime. Applying $\otimes_{\mathbb{Z}} F_p$ to the isomorphism (c), we get an F_p-algebra isomorphism:

(d) $$\overline{U}_{F_p} \xrightarrow{\approx} \widetilde{U}_{F_p}, \quad \text{where } \overline{U} = \overline{U} \otimes_{\mathbb{Z}} F_p \text{ and } \widetilde{U}_{F_p} = \widetilde{U}_{\mathbb{Z}} \otimes_{\mathbb{Z}} F_p.$$

Consider the ring homomorphism $\mathscr{B} \to F_p$ which takes $z \in \mathbb{Z}$ to $z \bmod p \in F_p$ and v to 1. This is well defined since the value at 1 of the cyclotomic polynomial ϕ_p is p, hence is zero in F_p.

Let $\mathbf{m}$ be the kernel of $\mathscr{B} \to F_p$ (a maximal ideal of $\mathscr{B}$). Tensoring the exact sequence $0 \to \mathbf{m} \to \mathscr{B} \to F_p \to 0$ with $\widetilde{U}_{\mathscr{B}}$ or $\tilde{\mathfrak{u}}$ over $\mathscr{B}$ we obtain isomorphisms of F_p-algebras:

(e) $$\widetilde{U}_{\mathscr{B}}/\mathbf{m}\widetilde{U}_{\mathscr{B}} \xrightarrow{\approx} \widetilde{U}_{\mathscr{B}} \otimes_{\mathscr{B}} F_p,$$

(f) $$\tilde{\mathfrak{u}}/\mathbf{m}\tilde{\mathfrak{u}} \xrightarrow{\approx} \tilde{\mathfrak{u}} \otimes_{\mathscr{B}} F_p.$$

Let $U_{F_p} = U \otimes_{\mathscr{A}} F_p$ where v acts trivially on F_p. By definition,

(g)
$$\begin{cases} U_{\mathscr{B}} \otimes_{\mathscr{B}} F_p = U_{F_p} \text{ modulo ideal generated by } K_1^p - 1, K_2^p - 1, \dots, K_n^p - 1, \\ \widetilde{U}_{F_p} = U_{F_p} \text{ modulo ideal generated by } K_1 - 1, K_2 - 1, \dots, K_n - 1. \end{cases}$$

In $U_{\mathbb{Z}}$, hence in $U_{F_p} = U_{\mathbb{Z}} \otimes_{\mathbb{Z}} F_p$, we have $K_i^2 = 1$ (since $K_i - K_i^{-1} = (v - v^{-1})\left[{K_i;0 \atop 1}\right] = 0$). It follows that $K_i^p - 1 = K_i - 1$ in U_{F_p} and from (g) we obtain an F_p-algebra isomorphism

(h) $$\widetilde{U}_{\mathscr{B}} \otimes_{\mathscr{B}} F_p \xrightarrow{\approx} \widetilde{U}_{F_p}.$$

The subalgebra $\bar{\mathfrak{u}}$ of $\overline{U}_{F_p}$ (see §0.1) and the subalgebra $\tilde{\mathfrak{u}} \otimes_{\mathscr{B}} F_p$ of $\widetilde{U}_{\mathscr{B}} \otimes F_p$ are mapped by (d) and (h) onto the same subalgebra of $\widetilde{U}_{F_p}$, namely the one spanned as an F_p-vector space by the elements

$$\prod_{\alpha \in R^+} F_\alpha^{(N_\alpha)} \prod_{i=1}^n K_{i,t_i} \prod_{\alpha \in R^+} E_\alpha^{(N'_\alpha)} \qquad (0 \le N_\alpha, N'_\alpha, t_i < p).$$

Combining these two maps we obtain an isomorphism of F_p-algebras

(i) $$\tilde{\mathfrak{u}} \otimes F_p \xrightarrow{\approx} \bar{\mathfrak{u}}.$$

Using (d), (h), (e), (f), and (i) we obtain the following result.

Theorem 6.8. *There are canonical (Hopf algebra) isomorphisms*

$$\widetilde{U}_{\mathscr{B}}/\mathbf{m}\widetilde{U}_{\mathscr{B}} \xrightarrow{\approx} U_{F_p}, \qquad \tilde{\mathfrak{u}}/\mathbf{m}\tilde{\mathfrak{u}} \xrightarrow{\approx} \bar{\mathfrak{u}}.$$

(Here the left-hand sides are defined in terms of quantum groups and the right-hand sides are classical algebras.)

6.9. From Theorem 6.9 and §§6.5(b) and 6.6, we see easily that the assertions in §0.3 hold.

References

1. N. Bourbaki, *Groupes et algèbres de Lie*, Chapitres 4, 5, et 6, Masson, Paris, 1981.
2. C. Chevalley, *Certains schémas de groupes semi-simples*, Sém. Bourbaki 1960/61, no 219.
3. C. W. Curtis, *Representations of Lie algebras of classical type with applications to linear gorups*, J. Math. Mech. **9** (1960), 307–326.
4. V. G. Drinfel′d, *Hopf algebras and the quantum Yang-Baxter equation*, Soviet Math. Dokl. **32** (1985), 254–258.
5. M. Dyer, *Hecke algebras and reflections in Coxeter groups*, Ph. D. thesis, University of Sydney, 1987.
6. M. Jimbo, *A q-difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation*, Lett. Math. Phys. **10** (1985), 63–69.
7. B. Kostant, *Groups over $\mathbb{Z}$*, Proc. Sympos. Pure Math., Vol. 9, Amer. Math. Soc., Providence, R. I., 1966, pp. 90–98.
8. G. Lusztig, *Quantum deformations of certain simple modules over enveloping algebras*, Adv. in Math. **70** (1988), 237–249.
9. ——, *Modular representations and quantum groups*, Contemp. Math., Vol. 82, Amer. Math. Soc., Providence, R. I., 1989, pp. 59–77.
10. ——, *On quantum groups*, J. Algebra (to appear).
11. M. Rosso, *Finite dimensional representations of the quantum analog of the enveloping algebra of a complex simplex Lie algebra*, Comm. Math. Phys. **117** (1988), 581–593.
12. R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33-56.
13. D. N. Verma, *Structure of certain induced representations of complex semisimple Lie algebras*, Bull. Amer. Math. Soc. **74** (1968), 160–168.
14. L. Alvarez-Gaumé, C. Gomez, and G. Sierra, *Quantum group interpretation of some conformal filed theories*, preprint CERN-TH-5267/88, Cern, Geneva, 1988.
15. G. Moore and N. Reshetikhin, *A comment on quantum group symmetry in conformal field theory*, preprint IASSNS-HEP-89, Inst. for Adv. Study, Princeton, N. J., 1989.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139