J. Comb. Algebra. 1 (2017), 45–57
DOI 10.4171/JCA/1-1-2

Journal of Combinatorial Algebra

The canonical basis of the quantum adjoint representation

George Lusztig*

Abstract. We identify the canonical basis of the quantum adjoint representation of a quantized enveloping algebra with a basis that we defined before the theory of canonical bases was available.

Mathematics Subject Classification (2010). 20G99.

Keywords. Quantum group, canonical basis, Chevalley group.

0. Introduction

0.1. According to Drinfeld and Jimbo, the universal enveloping algebra of a simple split Lie algebra $\mathfrak{g}$ over $\mathbf{Q}$ admits a remarkable deformation $\mathbf{U}$ (as a Hopf algebra over $\mathbf{Q}(v)$, where v is an indeterminate) called a quantized enveloping algebra. Moreover, the irreducible finite dimensional $\mathfrak{g}$-modules admit quantum deformation to become simple $\mathbf{U}$-modules. In [5], I found that these quantum deformations admit canonical bases with very favourable properties (at least when $\mathfrak{g}$ is of type A, D or E) which give also rise by specialization to canonical bases of the corresponding simple $\mathfrak{g}$-modules. (Later, Kashiwara [2] found another approach to the canonical bases.) In this paper we are interested in the canonical basis of the quantum deformation Λ of the adjoint representation of $\mathfrak{g}$. Before the introduction of the canonical bases, in [3, 4], I found a basis of Λ in which the generators E_i, F_i of $\mathbf{U}$ act through matrices whose entries are polynomials in $\mathbf{N}[v]$. By specialization, this gives rise to a basis of the adjoint representation of $\mathfrak{g}$ in which the Chevalley generators e_i, f_i of $\mathfrak{g}$ act through matrices whose entries are natural numbers, in contrast with the more traditional treatments where a multitude of signs appear.

In this paper (Section 1) I will prove that the basis of Λ from [3, 4] coincides with the canonical basis of Λ. I thank Meinolf Geck for suggesting that I should write down this proof. As an application (Section 2), I will give a definition of the Chevalley group over a field k associated to $\mathfrak{g}$ which seems to be simpler than Chevalley's original definition [1].

*Supported by NSF grant DMS-1303060.

0.2. Let I be a finite set with a given $\mathbf{Z}$-valued symmetric bilinear form $y, y' \mapsto y{\cdot}y'$ on $Y = \mathbf{Z}[I]$ such that the symmetric matrix $(i \cdot j)_{i,j\in I}$ is positive definite and such that $i \cdot i/2 \in \{1, 2, 3, \dots\}$ for all $i \in I$, $i \cdot i/2 = 1$ for some $i \in I$ and $2\frac{i\cdot j}{i\cdot i} \in \{0, -1, -2, \dots\}$ for all $i, j \in I$. In the terminology of [6, 1.1.1, 2.1.3], this is a *Cartan datum* of finite type. We shall assume that our Cartan datum is irreducible (see [6, 2.1.3]). Let e be the maximum value of $i \cdot i/2$ for $i \in I$. We can assume that $e \in \{1, 2, 3\}$. Let $I^1 = \{i \in I; i \cdot i/2 = 1\}$, $I^e = \{i \in I; i \cdot i/2 = e\}$. If $e = 1$ we have clearly $I^1 = I^e = I$; if $e > 1$, we have $I = I^1 \sqcup I^e$.

Let $X = \mathrm{Hom}(Y, \mathbf{Z})$ and let $\langle , \rangle : Y \times X \to \mathbf{Z}$ be the obvious pairing. For $j \in I$ we define $j' \in X$ by $\langle i, j'\rangle = 2\frac{i\cdot j}{i\cdot i}$ for all $i \in I$. Let v be an indeterminate. For $i \in I$ we set $v_i = v^{i\cdot i/2}$; for $n \in \mathbf{Z}$ we set $[n]_i = \frac{v_i^n - v_i^{-n}}{v_i - v_i^{-1}}$; for $n \in \mathbf{N}$ we set $[n]_i^! = \prod_{s=1}^n [s]_i$.

Note that when $i \in I^1$ we have $v_i = v$ and we write $[n]$ instead of $[n]_i$.

0.3. Following Drinfeld and Jimbo we define $\mathbf{U}$ to be the associative $\mathbf{Q}(v)$-algebra with generators E_i, F_i $(i \in I)$, K_y $(y \in Y)$ and relations

$$K_y K_{y'} = K_{y+y'} \qquad \text{for } y, y' \text{ in } Y,$$
$$K_i E_j = v^{\langle i,j'\rangle} E_j K_i \qquad \text{for } i, j \text{ in } I,$$
$$K_i F_j = v^{-\langle i,j'\rangle} F_j K_i \qquad \text{for } i, j \text{ in } I,$$
$$E_i F_j - F_j E_i = \delta_{ij} \frac{K_i^{i\cdot i/2} - K_i^{-i\cdot i/2}}{v_i - v_i^{-1}},$$
$$\sum_{\substack{p,p'\in\mathbf{N};\\ p+p'=1-\langle i,j'\rangle}} (-1)^{p'} \frac{[p+p']_i^!}{[p]_i^! [p']_i^!} E_i^p E_j E_i^{p'} = 0 \text{ for } i \neq j \text{ in } I,$$
$$\sum_{\substack{p,p'\in\mathbf{N};\\ p+p'=1-\langle i,j'\rangle}} (-1)^{p'} \frac{[p+p']_i^!}{[p]_i^! [p']_i^!} F_i^p F_j F_i^{p'} = 0 \text{ for } i \neq j \text{ in } I.$$

For $i \in I, s \in \mathbf{N}$ we set $E_i^{(s)} = ([s]_i^!)^{-1} E_i^s$, $F_i^{(s)} = ([s]_i^!)^{-1} F_i^s$.

By [6, 3.1.12], there is a unique $\mathbf{Q}$-algebra isomorphism $^- : \mathbf{U} \to \mathbf{U}$ such that $\bar{E}_i = E_i$, $\bar{F}_i = F_i$ for $i \in I$, $\bar{K}_y = K_{-y}$ for $y \in Y$ and $\overline{v^n u} = v^{-n}\bar{u}$ for all $u \in \mathbf{U}$, $n \in \mathbf{Z}$.

0.4. Let W be the (finite) subgroup of $\mathrm{Aut}(X)$ generated by the involutions $s_i : \lambda \mapsto \lambda - \langle i, \lambda\rangle i'$ of X $(i \in I)$. Let R be the smallest W-stable subset of X that contains $\{i'; i \in I\}$. This is a finite set. Let $R^+ = \{\alpha \in R; \alpha \in \sum_i \mathbf{N}i'\}$, $R^- = -R^+$. Let R^1 (resp. R^e be the smallest W-stable subset of X that contains I^1 (resp. I^e).

Then R^1, R^e are W-orbits. If $e = 1$ we have $R = R^1 = R^e$; if $e > 1$ we have $R = R^1 \sqcup R^e$.

For $i \in I$ and $\alpha \in R$ let $p_{i,\alpha}$ be the largest integer ≥ 0 such that α, $\alpha + i'$, $\alpha + 2i', \ldots, \alpha + p_{i,\alpha}i'$ belong to R and let $q_{i,\alpha}$ be the largest integer ≥ 0 such that $\alpha, \alpha - i', \alpha - 2i', \ldots, \alpha - q_{i,\alpha}i'$ belong to R. Then:

(a) $\langle i, \alpha \rangle = q_{i,\alpha} - p_{i,\alpha}$ and $p_{i,\alpha} + q_{i,\alpha} \leq 3$.

(b) If $p_{i,\alpha} + q_{i,\alpha} > 1$, then we must have $p_{i,\alpha} + q_{i,\alpha} = e$, $i \in I^1$; moreover, $\alpha - q_{i,\alpha}i' \in R^e$, $\alpha + p_{i,\alpha}i' \in R^e$ and $\alpha + ki' \in R^1$ for $-q_{i,\alpha} < k < p_{i,\alpha}$.

(c) If $p_{i,\alpha} + q_{i,\alpha} = 1$, then either both $\alpha - q_{i,\alpha}i'$, $\alpha + p_{i,\alpha}i'$ belong to R^e or both belong to R^1.

We define $h : R^+ \to \mathbf{N}$ by $h(\alpha) = \sum_{i \in I} n_i$ where $\alpha = \sum_{i \in I} n_i i'$ with $n_i \in \mathbf{N}$. There is a unique $\alpha_0 \in R^+$ such that $h(\alpha_0)$ is maximum. We then have $p_{i,\alpha_0} = 0$ for all $i \in I$; it follows that $\langle i, \alpha_0 \rangle \geq 0$ for any $i \in I$. We have $\alpha_0 \in R^e$.

0.5. The $\mathbf{U}$-module $\Lambda := \Lambda_{\alpha_0}$ (see [6, 3.5.6]) is well defined; it is simple, see [6, 6.2.3], and finite dimensional, see [6, 6.3.4]. Let $\eta = \eta_{\alpha_0} \in \Lambda$ be as in [6, 3.5.7]. We have a direct sum decomposition (as a vector space) $\Lambda = \oplus_{\lambda \in X} \Lambda^\lambda$ where $\Lambda^\lambda = \{x \in \Lambda;\, K_y x = v^{\langle y, \lambda \rangle} x,\ \forall y \in Y\}$. Note that for $i \in I, \lambda \in X$ we have $E_i X^\lambda \subset X^{\lambda + i'}$, $F_i X^\lambda \subset X^{\lambda - i'}$. Moreover, we have $\dim \Lambda^\alpha = 1$ if $\alpha \in R$, $\dim \Lambda^0 = \sharp(I)$ and $\Lambda^\lambda = 0$ if $\lambda \notin R \cup \{0\}$.

Let $\mathbf{B}$ be the canonical basis of Λ defined in [6, 14.4.11]. We now state the following result in which $||$ denotes absolute value.

Theorem 0.6.

(a) *Λ has a unique $\mathbf{Q}(v)$-basis $\mathfrak{E} = \{X_\alpha; \alpha \in R\} \sqcup \{t_i; i \in I\}$ such that (i)–(iii) below hold.*

(i) *$X_{\alpha_0} = \eta$;*

(ii) *for $\alpha \in R$ we have $X_\alpha \in \Lambda^\alpha$; for $i \in I$ we have $t_i \in \Lambda^0$;*

(iii) *for any $i \in I$ the linear maps $E_i : \Lambda \to \Lambda$, $F_i : \Lambda \to \Lambda$, are given by*

$$
\begin{aligned}
E_i X_\alpha &= [q_{i,\alpha} + 1]_i X_{\alpha + i'} && \text{if } \alpha \in R,\ p_{i,\alpha} > 0,\\
E_i X_{-i'} &= t_i,\\
E_i X_\alpha &= 0 && \text{if } \alpha \in R,\ p_{i,\alpha} = 0,\ \alpha \neq -i',\\
E_i t_j &= [|\langle j, i' \rangle|]_j X_{i'}, && \text{if } j \in I,\\
F_i X_\alpha &= [p_{i,\alpha} + 1]_i X_{\alpha - i'} && \text{if } \alpha \in R,\ q_{i,\alpha} > 0,\\
F_i X_{i'} &= t_i,\\
F_i X_\alpha &= 0 && \text{if } \alpha \in R,\ q_{i,\alpha} = 0,\ \alpha \neq i',\\
F_i t_j &= [|\langle j, i' \rangle|]_j X_{-i'} && \text{if } j \in I.
\end{aligned}
$$

(b) *We have $\mathfrak{E} = \mathbf{B}$.*

Note that the uniqueness of $\mathfrak{E}$ in (a) is straightforward. The existence of $\mathfrak{E}$ is proved in [3] under the assumption that $e = 1$ and is stated in [4] without assumption on e. We shall not use these results here. Instead, in 1.15 we shall give a new proof (based on results in [6]) of the existence of $\mathfrak{E}$ at the same time as proving (b).

1. Proof of Theorem 0.6

1.1. For any $\lambda \in X$, $\mathbf{B} \cap \Lambda^\lambda$ is a basis of Λ^λ. In particular, for any $\alpha \in R$, $\mathbf{B} \cap \Lambda^\alpha$ is a single element; we denote it by b^α.

Let $\mathcal{A} = \mathbf{Z}[v, v^{-1}]$ and let $\Lambda_{\mathcal{A}}$ be the $\mathcal{A}$-submodule of Λ generated by $\mathbf{B}$. It is known that $L_{\mathcal{A}}$ is stable under $E_i^{(s)}, F_i^{(s)}$ for $i \in I, s \in N$.

By [6, 19.3.4], there is a unique $\mathbf{Q}$-linear isomorphism $\bar{}: \Lambda \to \Lambda$ such that $\overline{u\eta} = \bar{u}\eta$ for all $u \in \mathbf{U}$. By [6, 19.1.2], there is a unique bilinear form $(,) : \Lambda \times \Lambda \to \mathbf{Q}(v)$ such that $(\eta, \eta) = 1$ and $(E_i x, x') = (x, v_i K_i^{i\cdot i/2} F_i x')$, $(F_i x, x') = (x, v_i K_i^{-i\cdot i/2} E_i x')$, $(K_y x, x') = (x, K_y x')$ for all $i \in I$, $y \in Y$ and x, x' in Λ.

1.2. By [6, 19.3.5],

(a) an element $b \in \Lambda$ satisfies $\pm b \in \mathbf{B}$ if and only if $b \in \Lambda_{\mathcal{A}}$, $\bar{b} = b$ and $(b, b) \in 1 + v^{-1}\mathbf{Z}[v^{-1}]$.

1.3. By [2] (see also [6, 16.1.4]), for any $i \in I$ there is a unique $\mathbf{Q}(v)$-linear map $\tilde{F}_i : \Lambda \to \Lambda$ such that the following holds: if $x \in \Lambda^\lambda$, $E_i x = 0$ and $s \in \mathbf{N}$, then $\tilde{F}_i(F_i^{(s)}x) = F_i^{(s+1)}x$. Moreover, there is a unique $\mathbf{Q}(v)$-linear map $\tilde{E}_i : \Lambda \to \Lambda$ such that the following holds: if $x \in \Lambda^\lambda$, $F_i x = 0$ and $s \in \mathbf{N}$, then $\tilde{E}_i(E_i^{(s)}x) = E_i^{(s+1)}x$. Let $\mathbf{A} = \mathbf{Q}(v) \cap \mathbf{Q}[[v^{-1}]]$. Let $\Lambda_{\mathbf{A}}$ be the $\mathbf{A}$-submodule of Λ generated by $\mathbf{B}$. For any $x \in \Lambda_{\mathbf{A}}$ let $\underline{x}$ be the image of x in $\underline{\Lambda} := \Lambda_{\mathbf{A}}/v^{-1}\Lambda_{\mathbf{A}}$. Note that $\{\underline{b}; b \in \mathbf{B}\}$ is a $\mathbf{Q}$-basis of $\underline{\Lambda}$. By [2] (see also [6, 20.1.4]), for any $i \in I$, $\tilde{F}_i, \tilde{E}_i$ preserve $\Lambda_{\mathbf{A}}, v^{-1}\Lambda_{\mathbf{A}}$ hence they induce $\mathbf{Q}$-linear maps $\underline{\Lambda} \to \underline{\Lambda}$ (denoted again by $\tilde{F}_i, \tilde{E}_i$). From [2] (see also [6, 20.1.4]) we see also that

(a) $\tilde{F}_i : \underline{\Lambda} \to \underline{\Lambda}$, $\tilde{E}_i : \underline{\Lambda} \to \underline{\Lambda}$ act in the basis $\{\underline{b}; b \in \mathbf{B}\}$ by matrices with all entries in $\{0, 1\}$.

In the case where $e = 1$, the results in this subsection are not needed; in this case, instead of (a), we could use the positivity of the matrix entries of $E_i : \Lambda \to \Lambda$, $F_i : \Lambda \to \Lambda$ proved in [6, 22.1.7].

1.4. Let $\alpha \in R$, $i \in I$ be such that $q_{i,\alpha} = 0$, $p = p_{i,\alpha} \geq 1$. Then we have $\langle i, \alpha \rangle = -p$. Let $Z^0 = b^\alpha \in \Lambda^\alpha$. We have $F_i Z^0 \in \Lambda^{\alpha - i'}$ hence $F_i Z^0 = 0$. We define $Z^k \in \Lambda^{\alpha + ki'}$ for $k = 1, \dots, p$ by the inductive formula

(a) $Z^k = [k]_i^{-1} E_i Z^{k-1} = \tilde{E}_i^k Z^0$.

Using $F_i Z^0 = 0$ together with (a) and the commutation formula between E_i, F_i we see by induction on k that for $k = 1, \dots, p$ we have

(b) $F_i Z^k = [p-k+1]_i Z^{k-1}$.

1.5. We preserve the setup of 1.4. We show that for $k \in [0, p-1]$ we have

(a) $$(Z^{k+1}, Z^{k+1}) = \frac{1 - v_i^{-2p+2k}}{1 - v_i^{-2k-2}} (Z^k, Z^k).$$

We have $E_i Z^k = [k+1]_i Z^{k+1}$ hence using 1.4(b):

$$\begin{aligned}
&[k+1]_i^2 (Z^{k+1}, Z^{k+1}) \\
&\quad = (E_i Z^k, E_i Z^k) = (Z^k, v_i K_i^{i\cdot i/2} F_i E_i Z^k) \\
&\quad = (Z^k, v_i K_i^{i\cdot i/2} E_i F_i Z^k) - \left(Z^k, v_i K_i^{i\cdot i/2} \frac{K_i^{i\cdot i/2} - K_i^{-i\cdot i/2}}{v_i - v_i^{-1}} Z^k\right) \\
&\quad = \left(v_i^{\langle i, \alpha + k i'\rangle + 1} [k]_i [p-k+1]_i - \frac{v_i^{2\langle i, \alpha + k i'\rangle + 1} - v_i}{v_i - v_i^{-1}}\right)(Z^k, Z^k) \\
&\quad = \left(v_i^{-p+2k+1} [k]_i [p-k+1]_i - \frac{v_i^{-2p+4k+1} - v_i}{v_i - v_i^{-1}}\right)(Z^k, Z^k).
\end{aligned}$$

We have

$$\begin{aligned}
&(v_i - v_i^{-1})^2 \left(v_i^{-p+2k+1} [k]_i [p-k+1]_i - \frac{v_i^{-2p+4k+1} - v_i}{v_i - v_i^{-1}}\right) \\
&\quad = v_i^{-p+2k+1} (v_i^k - v_i^{-k})(v_i^{p-k+1} - v_i^{-p+k-1}) - (v_i^{-2p+4k+1} - v_i)(v_i - v_i^{-1}) \\
&\quad = v_i^{2k+2} - v_i^2 - v_i^{-2p+4k} + v_i^{-2p+2k} - v_i^{-2p+4k+2} + v_i^2 + v_i^{-2p+4k} - 1 \\
&\quad = v_i^{2k+2} + v_i^{-2p+2k} - v_i^{-2p+4k+2} - 1 \\
&\quad = (v_i^{-2p+2k} - 1)(1 - v_i^{2k+2}).
\end{aligned}$$

Thus

$$(Z^{k+1}, Z^{k+1}) = \frac{(v_i^{-2p+2k} - 1)(1 - v_i^{2k+2})}{(v_i^{k+1} - v_i^{-k-1})^2} (Z^k, Z^k)$$

and (a) follows.

1.6. We preserve the setup of 1.4. We must have $p \in \{1, 2, 3\}$.

Assume first that $p = 1$. From 1.5(a) we have $(Z^1, Z^1) = (Z^0, Z^0)$. Assume now that $p = 2$. Then from 0.4(b) we have $v_i = v$ and from 1.5(a) we have

$$(Z^1, Z^1) = \frac{1 - v^{-4}}{1 - v^{-2}}(Z^0, Z^0),$$
$$(Z^2, Z^2) = \frac{1 - v^{-2}}{1 - v^{-4}}(Z^1, Z^1) = (Z^0, Z^0).$$

Assume next that $p = 3$. Then from 0.4(b) we have $v_i = v$ and from 1.5(a) we have

$$(Z^1, Z^1) = \frac{1 - v^{-6}}{1 - v^{-2}}(Z^0, Z^0),$$
$$(Z^2, Z^2) = (Z^1, Z^1),$$
$$(Z^3, Z^3) = \frac{1 - v^{-2}}{1 - v^{-6}}(Z^2, Z^2) = (Z^0, Z^0).$$

1.7. We preserve the setup of 1.6. We show:

(a) We have $Z^k = b^{\alpha + ki'}$ for $k = 0, 1, \dots, p$.

Since $Z^0 \in \mathbf{B}$, we have $Z^0 \in \Lambda_{\mathcal{A}}$, $\bar{Z}^0 = Z^0$, $(Z^0, Z^0) \in 1 + v^{-1}\mathbf{Z}(v^{-1})$. From the formulas in 1.6 we see that $(Z^k, Z^k) \in 1 + v^{-1}\mathbf{Z}(v^{-1})$ for $k = 0, 1, \dots, p$. For $k = 1, \dots, p$ we have $E_i Z^{k-1} = [k]_i Z^k$ hence for $k = 0, 1, \dots, p$ we have $Z^k = E_i^{(k)} Z^0 \in \Lambda_{\mathcal{A}}$. From $Z^k = E_i^{(k)} Z^0$ we see also that $\bar{Z}^k = \overline{E_i^{(k)} Z^0} = E_i^{(k)} Z^0 = Z^k$. Using 1.2(a) we see that $\epsilon Z^k \in \mathbf{B}$ for some $\epsilon \in \{1, -1\}$. By 1.4(a), we have $\underline{Z^k} = \tilde{E}_i^k \underline{Z^0}$. Using this together with and 1.3(a), we see that $\epsilon = 1$ so that $Z^k \in \mathbf{B}$. Since $Z^k \in \Lambda^{\alpha + ki'}$, we see that $Z^k = b^{\alpha + ki'}$.

1.8. Let $i \in I, \tilde{\alpha} \in R$ be such that $p_{i,\tilde{\alpha}} > 0$ (or equivalently such that $\tilde{\alpha} + i' \in R$). We show:

(a) $$E_i b^{\tilde{\alpha}} = [q_{i,\tilde{\alpha}} + 1]_i b^{\tilde{\alpha} + i'}$$

Let $\alpha = \tilde{\alpha} - q_{i,\tilde{\alpha}} i' \in R$. We have $q_{i,\alpha} = 0$, $p_{i,\alpha} = p_{i,\tilde{\alpha}} + q_{i,\tilde{\alpha}} > 0$. We set $Z^0 = b^\alpha$. We then define Z^k with $k \in [1, p_{i,\alpha}]$ in terms of α, Z^0 as in 1.4. Note that $E_i Z^{k-1} = [k]_i Z^k$ for any $k \in [1, p_{i,\alpha}]$. Taking $k = q_{i,\tilde{\alpha}} + 1$ (so that $k \in [1, p_{i,\alpha}]$) we deduce

$$E_i Z^{q_{i,\tilde{\alpha}}} = [q_{i,\tilde{\alpha}} + 1]_i Z^{q_{i,\tilde{\alpha}} + 1}.$$

By 1.7(a) we have $Z^{q_{i,\tilde{\alpha}}} = b^{\tilde{\alpha}}$, $Z^{q_{i,\tilde{\alpha}} + 1} = b^{\tilde{\alpha} + i'}$. This proves (a).

Here is a special case of (a); we assume that $i \neq j$ in I:

(b) If $\langle j, i' \rangle < 0$ then $E_j b^{i'} = b^{i' + j'}$; if $\langle j, i' \rangle = 0$ then $E_j b^{i'} = 0$.

It is enough to use that $p_{j,i'} = -\langle j, i' \rangle$ (we have $q_{j,i'} = 0$ since $i' - j' \notin R$).

1.9. Let $i \in I, \tilde{\alpha} \in R$ be such that $q_{i,\tilde{\alpha}} > 0$ (or equivalently such that $\tilde{\alpha} - i' \in R$). We show:

(a) $$F_i b^{\tilde{\alpha}} = [p_{i,\tilde{\alpha}} + 1]_i b^{\tilde{\alpha}-i'}.$$

Let $\alpha = \tilde{\alpha} - q_{i,\tilde{\alpha}} i' \in R$. We have $q_{i,\alpha} = 0$, $p_{i,\alpha} = p_{i,\tilde{\alpha}} + q_{i,\tilde{\alpha}} > 0$. We set $Z^0 = b^\alpha$. We then define Z^k with $k \in [1, p_{i,\alpha}]$ in terms of α, Z^0 as in 1.4. Note that $F_i Z^k = [p_{i,\alpha} - k + 1]_i Z^{k-1}$ for $k \in [1, p_{i,\alpha}]$. Taking $k = q_{i,\tilde{\alpha}}$ (so that $k \in [1, p_{i,\alpha}]$) we deduce

$$F_i Z^{q_{i,\tilde{\alpha}}} = [p_{i,\tilde{\alpha}} + 1]_i Z^{q_{i,\tilde{\alpha}}-1}.$$

By 1.7(a) we have $Z^{q_{i,\tilde{\alpha}}} = b^{\tilde{\alpha}}$, $Z^{q_{i,\tilde{\alpha}}-1} = b^{\tilde{\alpha}-i'}$. This proves (a).

Here is a special case of (a); we assume that $i \neq j$ in I:

(b) If $\langle j, i' \rangle < 0$ then $F_j b^{-i'} = b^{-i'-j'}$; if $\langle j, i' \rangle = 0$, then $F_j b^{-i'} = 0$.

It is enough to use that $q_{j,-i'} = \langle j, -i' \rangle$ (we have $p_{j,-i'} = 0$ since $-i' + j' \notin R$).

1.10. Let $i \in I$; we set $t_i = E_i b^{-i'} \in \Lambda^0$. We show

(a) $$F_i t_i = (v_i + v_i^{-1}) b^{-i'}.$$

Indeed,

$$\begin{aligned} F_i t_i = F_i E_i b^{-i'} &= E_i F_i b^{-i'} - \frac{K_i^{i\cdot i/2} - K_i^{-i\cdot i/2}}{v_i - v_i^{-1}} b^{-i'} \\ &= \frac{v_i^2 - v_i^{-2}}{v_i - v_i^{-1}} b^{i'} = (v_i + v_i^{-1}) b^{-i'}. \end{aligned}$$

We show:

(b) $$(t_i, t_i) = (1 + v_i^{-2})(b^{-i'}, b^{-i'}).$$

Indeed, using (a) we have

$$\begin{aligned} (t_i, t_i) = (E_i b^{-i'}, t_i) &= (b^{-i'}, v_i K_i^{i\cdot i/2} F_i t_i) \\ &= (b^{-i'}, v_i K_i^{i\cdot i/2} (v_i + v_i^{-1}) b^{-i'}) \\ &= (v_i + v_i^{-1}) v_i^{-\langle i, i' \rangle + 1} (b^{-i'}, b^{-i'}) \\ &= (1 + v_i^{-2})(b^{-i'}, b^{-i'}). \end{aligned}$$

From (b) we see that $(t_i, t_i) \in 1 + v^{-1}\mathbf{Z}[v^{-1}]$; from the definitions we have also $t_i \in \Lambda_{\mathcal{A}}$ and $\bar{t_i} = t_i$; it follows that $\epsilon t_i \in \mathbf{B}$ for some $\epsilon \in \{1, -1\}$. Now from $t_i = E_i b^{-i'}$ and $F_i b^{-i'} = 0$ we see that $t_i = \tilde{E}_i b^{-i'}$ hence $\underline{t_i} = \tilde{E}_i \underline{b^{-i'}}$. Using this together with 1.3(a) and we see that $\epsilon = 1$ hence

(c) $$t_i \in \mathbf{B}.$$

We show:

(d) $$\text{If } i \neq j, \text{ then } F_i t_j = [-\langle j, i' \rangle]_j b^{-i'}.$$

We have $F_i t_j = F_i E_j b^{-j'} = E_j F_i b^{-j'}$. This is 0 if $\langle i, j' \rangle = 0$ since by 1.9(b) we have $F_i b^{-j'} = 0$ (so in this case (a) holds). Now assume that $\langle i, j' \rangle < 0$. Then using 1.9(b) and 1.8(a) we have

$$E_j F_i b^{-j'} = E_j b^{-i'-j'} = \left[q_{j,-i'-j'} + 1\right]_j b^{-i'}.$$

Note that $p_{j,-i'-j'} = 1$ since $-i' - j' + j' \in R$, $-i' - j' + 2j' \notin R$. Hence $q_{j,-i'-j'} - 1 = \langle j, -i' - j' \rangle = -2 - \langle j, i' \rangle$ that is, $q_{i,-i'-j'} + 1 = -\langle j, i' \rangle$. This completes the proof of (d).

We show:

(e) $$\left(E_i t_i, E_i t_i\right) = [2]_i^2 \left(b^{-i'}, b^{-i'}\right).$$

Indeed, using (b) we have

$$\begin{aligned}
\left(E_i t_i, E_i t_i\right) &= \left(t_i, v_i K_i^{i\cdot i/2} F_i E_i t_i\right) \\
&= \left(t_i, v_i K_i^{i\cdot i/2} E_i F_i t_i\right) - \left(t_i, v_i K_i^{i\cdot i/2} \frac{K_i^{i\cdot i/2} - K_i^{-i\cdot i/2}}{v_i - v_i^{-1}} t_i\right) \\
&= [2]_i \left(t_i, v_i K_i^{i\cdot i/2} E_i b^{-i'}\right) \\
&= [2]_i \left(t_i, v_i K_i^{i\cdot i/2} t_i\right) \\
&= [2]_i \left(t_i, v_i t_i\right) = [2]_i^2 \left(b^{-i'}, b^{-i'}\right),
\end{aligned}$$

proving (e).

From (e) we get $\left([2]_i^{-1} E_i t_i, [2]_i^{-1} E_i t_i\right) \in 1 + v^{-1}\mathbf{Z}[v^{-1}]$. We have $[2]_i^{-1} E_i t_i = E_i^{(2)} b^{-i'} \in \Lambda_{\mathcal{A}}$. Moreover, we have clearly $\overline{[2]_i^{-1} E_i t_i} = [2]_i^{-1} E_i t_i$. Using 1.2(a) we deduce that $\epsilon [2]_i^{-1} E_i t_i \in \mathbf{B}$ for some $\epsilon \in \{1, -1\}$. Since $[2]_i^{-1} E_i t_i \in \Lambda^{i'}$, we must have $\epsilon [2]_i^{-1} E_i t_i = b^{i'}$. Thus we have $\epsilon E_i^{(2)} b^{-i'} = b^{i'}$. Since $F_i b^{-i'} = 0$ it follows that $\tilde{E}_i^2 b^{-i'} = \epsilon b^{i'}$ and $\tilde{E}_i^2 \underline{b^{-i'}} = \epsilon \underline{b^{i'}}$. Using 1.3(a), we deduce that $\epsilon = 1$. Thus,

(f) $$E_i t_i = [2]_i b^{i'}.$$

1.11. Let $i \in I$. We set $\tilde{t}_i = F_i b^{i'} \in \Lambda^0$. We show:

(a) $$E_i \tilde{t}_i = [2]_i b^{i'}.$$

Indeed,

$$E_i \tilde{t}_i = E_i F_i b^{i'} = F_i E_i b^{i'} + \frac{K_i^{i\cdot i/2} - K_i^{-i\cdot i/2}}{v_i - v_i^{-1}} b^{i'} = \frac{v_i^2 - v_i^{-2}}{v_i - v_i^{-1}} b^{i'} = [2]_i b^{i'}.$$

We show:

(b) $$\big(\tilde{t}_i, \tilde{t}_i\big) = [2]_i v_i^{-1}\big(b^{i'}, b^{i'}\big).$$

Indeed, using (a) we have:

$$\begin{aligned}\big(\tilde{t}_i, \tilde{t}_i\big) = \big(F_i b^{i'}, \tilde{t}_i\big) &= \big(b^{i'}, v_i K_i^{-i\cdot i/2} E_i \tilde{t}_i\big)\\ &= \big(b^{i'}, v_i K_i^{-i\cdot i/2}[2]_i b^{i'}\big) = [2]_i v_i^{-1}\big(b^{i'}, b^{i'}\big).\end{aligned}$$

From (b) we see that $(\tilde{t}_i, \tilde{t}_i) \in 1 + v^{-1}\mathbf{Z}[v^{-1}]$; from the definitions we have also $\tilde{t}_i \in \Lambda_{\mathcal{A}}$ and $\bar{\tilde{t}}_i = \tilde{t}_i$; using 1.2(a) we see that $\epsilon\tilde{t}_i \in \mathbf{B}$ for some $\epsilon \in \{1, -1\}$. From $\tilde{t}_i = F_i b^{i'}$, $E_i b^{i'} = 0$ we see that $\tilde{t}_i = \tilde{F}_i b^{i'}$ hence $\underline{\tilde{t}_i} = \tilde{F}_i \underline{b^{i'}}$. Using this and 1.3(a) we deduce that $\epsilon = 1$ so that

(c) $$\tilde{t}_i \in \mathbf{B}.$$

We show:

(d) $$\big(\tilde{t}_i, t_i\big) = \pm\big(1 + v_i^{-2}\big)\big(b^{i'}, b^{i'}\big).$$

Indeed, using 1.10(f) we have

$$\begin{aligned}\big(\tilde{t}_i, t_i\big) = \big(F_i b^{i'}, t_i\big) &= \big(b^{i'}, v_i K_i^{-i\cdot i/2} E_i t_i\big)\\ &= \big(b^{i'}, v_i K_i^{-i\cdot i/2}[2]_i b^{i'}\big)\\ &= v_i^{-1}[2]_i\big(b^{i'}, b^{i'}\big) = \big(1 + v_i^{-2}\big)\big(b^{i'}, b^{i'}\big)\end{aligned}$$

hence $(\tilde{t}_i, t_i) \in 1 + v^{-1}\mathbf{Z}[v^{-1}]$. If $\tilde{t}_i \neq t_i$ then, since $\tilde{t}_i \in \mathbf{B}$ and $t_i \in \mathbf{B}$, we would have $(\tilde{t}_i, t_i) \in v^{-1}\mathbf{Z}[v^{-1}]$ (see [6, 19.3.3]), contradicting (d). Thus we have $\tilde{t}_i = t_i$ and

(e) $$F_i b^{i'} = t_i.$$

We show:

(f) If $i \neq j$, then $E_i t_j = [-\langle j, i'\rangle]_j b^{i'}$.

Using (e) we have $E_i t_j = E_i F_j b^{j'} = F_j E_i b^{j'}$. This is 0 if $\langle i, j'\rangle = 0$ since by 1.8(b) we have $E_i b^{j'} = 0$ (so in this case (f) holds). Now assume that $\langle i, j'\rangle < 0$. Then using 1.8(b) and 1.9(a) we have

$$F_j E_i b^{j'} = F_j b^{i'+j'} = [p_{j,i'+j'} + 1]_j b^{i'}.$$

Note that $q_{j,i'+j'} = 1$ since $i' + j' - j' \in R$, $i' + j' - 2j' \notin R$. Hence

$$1 - p_{j,i'+j'} = \langle j, i' + j'\rangle = 2 + \langle j, i'\rangle$$

that is,

$$p_{i,i'+j'} + 1 = -\langle j, i'\rangle.$$

This completes the proof of (f).

1.12. We show:

(a) If $\alpha \in R^1$, then $(b^\alpha, b^\alpha) = 1 + v^{-2} + \cdots + v^{-2(e-1)} = v^{-e+1}[e]$. If $\alpha \in R^e$, then $(b^\alpha, b^\alpha) = 1$.

Note that when $e = 1$ we have $R^1 = R^e$ and the two formulas in (a) are compatible with each other.

We first prove (a) for $\alpha \in R^+$ by descending induction on $h(\alpha)$. If $h(\alpha) = h(\alpha_0)$ then $\alpha = \alpha_0$ and we have $b^\alpha = \eta$ so that $(b^\alpha, b^\alpha) = (\eta, \eta) = 1$. Now assume that $\alpha \in R^+$, $h(a) < h(\alpha_0)$. We can find $\alpha' \in R^+$, $i \in I$ such that $q_{i,\alpha'} = 0$, $p = p_{i,\alpha'} \geq 1$ and $\alpha = \alpha' + ki'$ where $k \in \{0, 1, \dots, p-1\}$. Then $h(\alpha' + pi') > h(\alpha)$ hence $(\alpha' + pi', \alpha' + pi')$ is given by the formula in (a). Assume first that $p = 1$. Then $\alpha = \alpha'$ and by 1.6 and 1.7(a) we have $(b^\alpha, b^\alpha) = (b^{\alpha'+i'}, b^{\alpha'+i'})$. By 0.4(c), either both $\alpha, \alpha + i'$ belong to R^e or both belong to R^1; (a) follows in this case. Next assume that $p > 1$. By 0.4(b) we have $p = e$ and $\alpha' + pi' \in R^e$. Hence $(b^{\alpha'+pi'}, b^{\alpha'+pi'}) = 1$. If $k = 0$ then $\alpha \in R^e$ (see 0.4(b)) and by 1.6 and 1.7(a) we have $(b^\alpha, b^\alpha) = (b^{\alpha'+pi'}, b^{\alpha'+pi'})$; (a) follows in this case. If $k > 0$, $k < p$ then $\alpha \in R^1$ (see 0.4(b)) and by 1.6 and 1.7(a) we have $(b^\alpha, b^\alpha) = (1 + v^{-2} + \cdots + v^{-2(e-1)})(b^{\alpha'+pi'}, b^{\alpha'+pi'})$; (a) follows in this case. This completes the proof of (a) assuming that $\alpha \in R^+$.

We now prove (a) for $\alpha \in R^-$ by induction on $h(-\alpha) \geq 1$. Let $i \in I$. Recall that $\tilde{t}_i, t_i$ satisfy $\tilde{t}_i = t_i$ (see 1.11), $(t_i, t_i) = [2]_i v_i^{-1}(b^{-i'}, b^{-i'})$ (see 1.10(b)) and $(\tilde{t}_i, \tilde{t}_i) = [2]_i v_i^{-1}(b^{i'}, b^{i'})$ (see 1.11(b)). It follows that

(b) $$\left(b^{-i'}, b^{-i'}\right) = \left(b^{i'}, b^{i'}\right).$$

In particular, (a) holds when $h(-\alpha) = 1$. We now assume that $\alpha \in R^-$ and $h(-\alpha) \geq 2$. We can find $\alpha' \in R^-$, $i \in I$ such that $q_{i,\alpha'} = 0$, $p = p_{i,\alpha'} \geq 1$ and $\alpha = \alpha' + ki'$ where $k \in \{0, 1, \dots, p-1\}$. Then $h(-(\alpha' + pi')) < h(-\alpha)$ hence $(\alpha' + pi', \alpha' + pi')$ is given by the formula in (a). The rest of the proof is a repetition of the first part of the proof. Assume first that $p = 1$. Then $\alpha = \alpha'$ and by 1.6 and 1.7(a) we have $(b^\alpha, b^\alpha) = (b^{\alpha'+i'}, b^{\alpha'+i'})$. By 0.4(c), either both $\alpha, \alpha + i'$ belong to R^e or both belong to R^1; (a) follows in this case. Next assume that $p > 1$. By 0.4(b) we have $p = e$ and $\alpha' + pi' \in R^e$. Hence $(b^{\alpha'+pi'}, b^{\alpha'+pi'}) = 1$. If $k = 0$ then $\alpha \in R^e$ (see 0.4(b)) and by 1.6 and 1.7(a) we have $(b^\alpha, b^\alpha) = (b^{\alpha'+pi'}, b^{\alpha'+pi'})$; (a) follows in this case. If $k > 0$, $k < p$ then $\alpha \in R^1$ (see 0.4(b)) and by 1.6 and 1.7(a) we have $(b^\alpha, b^\alpha) = (1 + v^{-2} + \cdots + v^{-2(e-1)})(b^{\alpha'+pi'}, b^{\alpha'+pi'})$; (a) follows in this case. This completes the proof of (a) assuming that $\alpha \in R^-$; hence (a) is proved in all cases.

1.13. We show:

(a) If $i \in I^1$ then $(t_i, t_i) = \left(1 + v^{-2}\right)\left(1 + v^{-2} + \cdots + v^{-2(e-1)}\right)$.
If $i \in I^e$ then $(t_i, t_i) = 1 + v_i^{-2} = 1 + v^{-2e}$.

Note that when $e = 1$ we have $I^1 = I^e$ and the two formulas in (a) are compatible with each other.

From 1.10(b) we have $(t_i, t_i) = [2]_i v_i^{-1}(b^{-i'}, b^{-i'})$. Using 1.12(a) we see that (a) holds.

In the remainder of this subsection we fix $i \neq j$ in I. We show:

(b) If at least one of i, j is in I^1 and $i \cdot j \neq 0$ then $(t_i, t_j) = v^{-e}[e]$.
If both i, j are in I^e and $i \cdot j \neq 0$ then $(t_i, t_j) = v^{-e}$.
If $i \cdot j = 0$ then $(t_i, t_j) = 0$.

Using 1.10(d), we have

$$\begin{aligned}(t_i, t_j) = (E_i b^{-i'}, t_j) &= (b^{-i'}, v_i K_i^{i \cdot i/2} F_i t_j) \\ &= [-\langle j, i'\rangle]_j (b^{-i'}, v_i K_i^{i \cdot i/2} b^{-i'}) \\ &= v_i^{-1}[-\langle j, i'\rangle]_j (b^{-i'}, b^{-i'}).\end{aligned}$$

We see that if $\langle j, i'\rangle = 0$ then $(t_i, t_j) = 0$.

Now assume that $\langle j, i'\rangle \neq 0$.

If $i \in I^e, j \in I^e$ then $\langle j, i'\rangle = -1$ and $(t_i, t_j) = v^{-e}$.
If $i \in I^e, j \in I^1$ then $\langle j, i'\rangle = -e$ and $(t_i, t_j) = v^{-e}[e]$.
If $i \in I^1, j \in I^e$ then $(t_i, t_j) = (t_j, t_i) = v^{-e}[e]$.
If $i \in I^1, j \in I^1$ then $\langle j, i'\rangle = -1$ and
$(t_i, t_j) = v^{-1}(1 + v^{-2} + \cdots + v^{-2(e-1)}) = v^{-e}[e]$.

This completes the proof of (b).

1.14. We show:

(a) The elements $\{t_i; i \in I\}$ are distinct.

Let $i \neq j$ in I. If we had $t_i = t_j$, then we would have $(t_i, t_j) \in 1 + v^{-1}\mathbf{Z}[v^{-1}]$, see 1.13(a). But 1.13(b) shows that $(t_i, t_j) \in v^{-1}\mathbf{Z}[v^{-1}]$. This completes the proof of (a).

Let $\mathfrak{C} = \{b^\alpha; \alpha \in R\} \sqcup \{t_i, i \in I\}$. By (a), this is a subset of Λ rather than a multiset. We show:

(b) We have $\mathbf{B} = \mathfrak{C}$.

Since $t_i \in \mathbf{B}$ for any $i \in I$, we have $\mathfrak{C} \subset \mathbf{B}$. Clearly we have $\sharp(\mathfrak{C}) = \sharp(R) + \sharp(I)$. Since we have also $\sharp(\mathbf{B}) = \sharp(R) + \sharp(I)$, it follows that $\mathfrak{C} = \mathbf{B}$, proving (b).

1.15. We prove the existence part of 0.6(a). It is enough to prove that the elements $X_\alpha = b^\alpha$ and t_i satisfy the requirements of 0.6(a). Now 0.6(a)(i) holds by definition; 0.6(a)(ii) is immediate; 0.6(a)(iii) has been verified earlier in this section. This proves the existence part of 0.6(a) and at the same time proves 0.6(b) (see 1.14(b)).

2. Applications

2.1. Let $i \in I$, $k \in \mathbf{Z}_{>0}$. From 0.6 we see that the action of $E_i^{(k)}$, $F_i^{(k)}$ in the basis $\mathfrak{C}$ of Λ is given by the following formulas.

$$
\begin{aligned}
E_i^{(k)} X_\alpha &= \frac{[q_{i,\alpha}+k]_i^!}{[q_{i,\alpha}]_i^! [k]_i^!} X_{\alpha+ki'} && \text{if } \alpha \in R, \alpha \neq -i', k \le p_{i,\alpha},\\
E_i^{(k)} X_\alpha &= 0 && \text{if } \alpha \in R, \alpha \neq -i', k > p_{i,\alpha},\\
E_i X_{-i'} &= t_i,\ E_i^{(2)} X_{-i'} = X_{i'},\ E_i^{(k)} X_{-i'} = 0 && \text{if } k \ge 3,\\
E_i t_j &= [|\langle j, i'\rangle|]_j X_{i'},\ E_i^{(k)} t_j = 0 && \text{if } k \ge 2,\\
F_i^{(k)} X_\alpha &= \frac{[p_{i,\alpha}+k]_i^!}{[p_{i,\alpha}]_i^! [k]_i^!} X_{\alpha-ki'} && \text{if } \alpha \in R, \alpha \neq i', k \le q_{i,\alpha},\\
F_i^{(k)} X_\alpha &= 0 && \text{if } \alpha \in R, \alpha \neq i', k > q_{i,\alpha},\\
F_i X_{i'} &= t_i,\ F_i^{(2)} X_{i'} = X_{-i'},\ F_i^{(k)} X_{i'} = 0 && \text{if } k \ge 3,\\
F_i t_j &= [|\langle j, i'\rangle|]_j X_{-i'},\ F_i^{(k)} t_j = 0 && \text{if } k \ge 2.
\end{aligned}
$$

In particular, we see that $E_i^{(k)}$, $F_i^{(k)}$ act through matrices with all entries in $\mathbf{N}[v, v^{-1}]$. (In the case where $e = 1$ this is already known from [6, 22.1.7].)

2.2. If v is specialized to 1, the $\mathbf{U}$-module Λ becomes a simple module over the universal enveloping algebra of a simple Lie algebra $\mathfrak{g}$ corresponding to the adjoint representation $\Lambda|_{v=1}$ of $\mathfrak{g}$; this module inherits a $\mathbf{Q}$-basis $\{X_\alpha; \alpha \in R\} \sqcup \{t_i; i \in I\}$ in which the elements e_i, f_i of $\mathfrak{g}$ defined by E_i, F_i act by matrices with entries in $\mathbf{N}$. Let $z \in \mathbf{Q}$. Then for $i \in I$, the exponentials $x_i(z) = \exp(ze_i)$, $y_i(z) = \exp(zf_i)$ are well defined endomorphisms of $\Lambda|_{v=1}$. Their action in the basis above can be described using the formulas in 2.1:

$$
\begin{aligned}
x_i(z) X_\alpha &= \sum_{0 \le k \le p_{i,\alpha}} \frac{(q_{i,\alpha}+k)!}{q_{i,\alpha}! k!} z^k X_{\alpha+ki'} && \text{if } \alpha \in R, \alpha \neq -i',\\
x_i(z) X_{-i'} &= X_{-i'} + z t_i + z^2 X_{i'}, &&\\
x_i(z) t_j &= t_j + |\langle j, i'\rangle| z X_{i'} && \text{if } j \in I,\\
y_i(z) X_\alpha &= \sum_{0 \le k \le q_{i,\alpha}} \frac{(p_{i,\alpha}+k)!}{p_{i,\alpha}! k!} z^k X_{\alpha-ki'} && \text{if } \alpha \in R, \alpha \neq i',\\
y_i(z) X_{i'} &= X_{i'} + z t_i + z^2 X_{-i'}, &&\\
y_i(z) t_j &= t_j + |\langle j, i'\rangle| z X_{-i'} && \text{if } j \in I.
\end{aligned}
$$

2.3. Now let k be any field and let V be the k-vector space with basis

$$\{X_\alpha; \alpha \in R\} \sqcup \{t_i; i \in I\}.$$

For any $i \in I$ and $z \in k$ we define $x_i(z) \in GL(V)$, $y_i(z) \in GL(V)$ by the formulas in 2.2 (which involve only integer coefficients). The subgroup of $GL(V)$ generated by the elements $x_i(z), y_i(z)$ for various $i \in I, z \in k$ is the Chevalley group [1] over k associated to $\mathfrak{g}$.

References

[1] C. Chevalley, Sur certains groupes simples, *Tohoku Math. J.*, **7** (1955), 14–66. Zbl 0066.01503 MR 73602

[2] M. Kashiwara, On crystal bases of the q-analogue of universal enveloping algebras, *Duke Math. J.*, **63** (1991), 465–516. Zbl 0739.17005 MR 1115118

[3] G. Lusztig, On quantum groups, *J. Alg.*, **131** (1990), 466–475. Zbl 0698.16007 MR 1058558

[4] G. Lusztig, Quantum groups at roots of 1, *Geom. Ded.*, **35** (1990), 89–114. Zbl 0714.17013 MR 1066560

[5] G. Lusztig, Canonical bases arising from quantized enveloping algebras, *J. Amer. Math. Soc.*, **3** (1990), 447–498. Zbl 0703.17008 MR 1035415

[6] G. Lusztig, *Introduction to quantum groups*, Progr. in Math., 110, Birkhäuser, Boston, 1993. Zbl 0788.17010 MR 1227098

Received 30 April, 2016

G. Lusztig, Department of Mathematics, MIT, Cambridge, MA 02139, USA
E-mail: gyuri@math.mit.edu