Invent. math. 120, 361 – 377 (1995)

Inventiones mathematicae

Hall algebras, hereditary algebras and quantum groups

James A. Green

119 Cumnor Hill, Oxford OX2 9JA, United Kingdom

Oblatum 4-VIII-1994 & 4-X-1994

1. Introduction

Let R be an associative, hereditary algebra over a finite field k, and let R-fin be the full subcategory of R-mod whose objects are those left R-modules X which are finite as sets, $|X| < \infty$. Assume also that R is *finitary* in C. Ringel's sense, i.e. that $|\mathrm{Ext}^1_R(S, S')| < \infty$ for all simple S, S' in R-fin; this condition is met, for example, if R is finitely generated as k-algebra [4, pp. 435, 436].

Let $\mathscr{P}$ be the set of all isomorphism classes in R-fin. If $\lambda \in \mathscr{P}$, then U_λ will denote an R-module in class λ. The class of all zero left R-modules is denoted 0. Let $I \subseteq \mathscr{P}$ be the set of all isomorphism classes of simple modules in R-fin. Thus $\{U_i : i \in I\}$ is a complete set of simple, finite left R-modules. We identify the Grothendieck group $K_0(R\text{-fin})$ with the free Abelian group $\mathbb{Z}I = \{\sum_i v_i i : v_i \in \mathbb{Z}\}$ having I as free basis, so that if $X \in R$-fin then the corresponding element of $K_0(R\text{-fin})$ is the "dimension vector" $\mathbf{dim} X = \sum_{i \in I} v_i i$, where for each $i \in I$, v_i is the multiplicity of the simple module U_i in any composition series of X. Clearly $\mathbf{dim} X$ lies in the subsemigroup

$$\mathbb{N}I = \left\{ \sum_{i \in I} v_i i : v_i \in \mathbb{N} \right\}$$

of $\mathbb{Z}I$. Notice that $\mathbf{dim}\, U_i = i$, for all $i \in I$.

In his paper [7], Ringel introduces an important modification of the Hall algebra associated to the category R-fin. For any $X, Y \in R$-fin, define the integer

$$e(X, Y) = \dim_k \mathrm{Hom}_R(X, Y) - \dim_k \mathrm{Ext}^1_R(X, Y)\,.$$

Since R is hereditary, $\mathrm{Ext}^n_R(-,-) = 0$ for all $n \geqq 2$; thus $e(X, Y)$ is a kind of "Euler characteristic" on the abelian category R-fin. Elementary homological arguments show that $e(X, Y)$ depends only on $\mathbf{dim} X$, $\mathbf{dim}\, Y$, and so we may define a bilinear form $\langle -,- \rangle_R : \mathbb{Z}I \times \mathbb{Z}I \to \mathbb{Z}$ by the rule: $\langle \mathbf{dim} X,\ \mathbf{dim}\, Y \rangle_R =$

$e(X, Y)$, for all $X, Y \in R$-fin. In particular, $\langle i, j \rangle_R = e(U_i, U_j)$ for all $i, j \in I$. This form $\langle -, - \rangle_R$ has been called (by Ringel) the "Euler form", or (by others) the "Ringel form". It is not in general symmetric, but we define a symmetric bilinear form ${}_{\dot{R}}$ on $\mathbb{Z}I$ by the rule: $i \,{}_{\dot{R}}\, j = \langle i, j \rangle_R + \langle j, i \rangle_R$, for $i, j \in I$. We extend these notations to arbitrary elements $\alpha, \beta \in \mathscr{P}$ as follows: $\langle \alpha, \beta \rangle_R = e(U_\alpha, U_\beta) = \langle \mathbf{dim}\, U_\alpha, \mathbf{dim}\, U_\beta \rangle_R$, and $\alpha \,{}_{\dot{R}}\, \beta = \langle \alpha, \beta \rangle_R + \langle \beta, \alpha \rangle_R$.

Let $\mathscr{A}$ be a (commutative) integral domain containing $\mathbb{Z}$, and containing also elements v, v^{-1}, where $v^2 = |k|$. The *Ringel-Hall algebra* $H = H_{\mathscr{A},v}(R)$ is by definition the free $\mathscr{A}$-module on a set of symbols $u_\lambda (\lambda \in \mathscr{P})$, with an $\mathscr{A}$-bilinear multiplication defined by setting

$$(1) \qquad u_\alpha u_\beta = \sum_{\lambda \in \mathscr{P}} v^{\langle \alpha, \beta \rangle} \cdot g^\lambda_{\alpha\beta} \cdot u_\lambda \,, \quad \text{for all } \alpha, \beta \in \mathscr{P} \,,$$

where $\langle \alpha, \beta \rangle = \langle \alpha, \beta \rangle_R$, and $g^\lambda_{\alpha\beta}$ is the number of submodules X of U_λ such that U_λ / X, X lie in the isomorphism classes α, β respectively. It is easily checked that $H = H_{\mathscr{A},v}(R)$ is an associative (but not necessarily commutative), $\mathbb{N}I$-graded $\mathscr{A}$-algebra with identity element u_0. The grading $H = \sum_v^{\oplus} H_v$ is defined as follows: for each $v \in \mathbb{N}I$, H_v is the $\mathscr{A}$-span of the set $\{u_\lambda : \lambda \in \mathscr{P}, \mathbf{dim}\, U_\lambda = v\}$.

From the work of Zelevinsky (see in particular [9, p. 116]), who considered the Hall algebra with $R = k[t]_{t-1}$ (the localization at $t-1$ of the polynomial algebra $k[t]$— notice that in this case the Ringel form $\langle -, - \rangle_R$ is identically zero [7, Sect. 3], so that the term $v^{\langle \alpha, \beta \rangle}$ in (1) becomes invisible), and of Ringel, who found that for suitable R the elements $u_i (i \in I)$ satisfy relations like the quantum Serre relations [5, 7], it seemed possible that the Ringel–Hall algebra should have a co-multiplication of interest. The main result in this paper (Theorem 1, below) is that, with a mild restriction on the coefficient domain $\mathscr{A}$, this is indeed so. The co-multiplication r on $H_{\mathscr{A},v}(R)$ is very closely modelled on Zelevinsky's. Let R be a finitary, hereditary algebra over a finite field k, and $\mathscr{A}$ an integral domain containing the rational field $\mathbb{Q}$ and an element v such that $v^2 = |k|$ (then $\mathscr{A}$ must also contain $v^{-1} = v|k|^{-1}$). Define an $\mathscr{A}$-linear map $r : H \to H \otimes H$ ($\otimes$ means $\otimes_{\mathscr{A}}$) by setting

$$(2) \qquad r(u_\lambda) = \sum_{\alpha, \beta \in \mathscr{P}} v^{\langle \alpha, \beta \rangle} \cdot g^\lambda_{\alpha\beta} \cdot \frac{a_\alpha a_\beta}{a_\lambda} \cdot (u_\alpha \otimes u_\beta)$$

for all $\lambda \in \mathscr{P}$. Here $\langle \alpha, \beta \rangle$ and $g^\lambda_{\alpha\beta}$ are as in (1), and $a_\pi = |\mathrm{Aut}_R(U_\pi)|$, for any $\pi \in \mathscr{P}$.

Theorem 1. *With the notation above, let* $H = H_{\mathscr{A},v}(R)$. *Then*

(i) H *is an associative,* $\mathbb{N}I$*-graded* $\mathscr{A}$*-algebra.*

(ii) $r : H \to H \otimes H$ *is co-associative, and* $r(u_i) = u_i \otimes 1 + 1 \otimes u_i$ *for all* $i \in I$.

(iii) r *is multiplicative, if the product in* $H \otimes H$ *is given by the rule*

$$(3) \qquad (u_\rho \otimes u_\sigma)(u_{\rho'} \otimes u_{\sigma'}) = v^{\sigma \cdot \rho'} (u_\rho u_{\rho'}) \otimes (u_\sigma u_{\sigma'}) \,,$$

for all $\rho, \sigma, \rho', \sigma' \in \mathscr{P}$, *and* $\sigma \cdot \rho' = \sigma \,{}_{\dot{R}}\, \rho'$.

(iv) *There is a symmetric, bilinear, non-degenerate form* $(-,-) : H \times H \to \mathscr{A}$ *defined by* $(u_\alpha, u_\beta) = \delta_{\alpha\beta}\frac{1}{a_\alpha}$ *(all* $\alpha, \beta \in \mathscr{P}$*), and there holds*

$$(x, yz) = (r(x), y \otimes z), \text{ for all } x, y, z \in H . \tag{4}$$

(In (4)*, the form* $(-,-)$ *on* $H \otimes H$ *is defined by* $(x \otimes y,\ x' \otimes y') = (x, x')(y, y')$*, for all* $x, y, x', y' \in H$*.)*

The special case of Theorem 1 where $R = k[t]_{t-1}$ is due to Zelevinsky [9, Proposition 10.1]. Everything asserted in Theorem 1 is easily proved from the definitions, except the multiplicativity of r, whose proof occupies section 2 of this paper. This proof is based on a universal formula concerning pairs of submodules of finite R-modules, where R is a finitary, hereditary k-algebra; this formula is stated as Theorem 2 (see 2.2).

The structure of $H = H_{\mathscr{A},v}(R)$ which is revealed by Theorem 1 is strikingly similar to that of an algebra **f** defined by G. Lusztig in his book [2], and which turns out to be isomorphic to the positive part U^+ of a Drinfeld–Jimbo quantum group $U = U^- \otimes U^0 \otimes U^+$ [2, Chapters 1 and 33]. In both cases there is a combinatorial datum consisting of a set I and a symmetric bilinear form $(i, j) \mapsto i \cdot j$ on the free Abelian group $\mathbb{Z}I$ (in Lusztig's case, the pair $(I, \cdot)$ is a "Cartan datum" [2, p. 2]); there is an associative, $\mathbb{N}I$-graded algebra L; there is a co-multiplication $r : L \mapsto L \otimes L$, which is multiplicative provided the product in $L \otimes L$ is given by a twisted version of the usual rule (the "twisting" depends on the datum $(I, \cdot)$); finally, multiplication and co-multiplication in L are adjoint to each other with respect to a suitable symmetric bilinear form on L. These features are axiomatized in section 3, and the resulting theory is used to prove one half of Theorem 3 (see 3.5). This theorem generalizes a theorem of Ringel, which says that in appropriate circumstances, the "quantum algebra" U^+ is isomorphic to a suitable "generic" version of the subalgebra ("composition algebra") generated by the elements $u_i (i \in I)$ of a Ringel–Hall algebra.

2. The proof of Theorem 1

2.1. Preliminaries

All statements in parts (i), (ii) and (iv) of Theorem 1 follow easily from the definitions, and their proofs are left to the reader. The rest of this section is devoted to the proof of part (iii). Throughout the section the finitary, hereditary k-algebra R is fixed. The suffix R will be dropped from $\langle -,- \rangle_R$ and $\cdot_R$. Thus $\langle \alpha, \beta \rangle = e(U_\alpha, U_\beta)$ and $\alpha \cdot \beta = \langle \alpha, \beta \rangle + \langle \beta, \alpha \rangle$, for all $\alpha, \beta \in \mathscr{P}$.

2.2. The equation $N_1 = N_2$

Since $r : H \to H \otimes H$ is $\mathscr{A}$-linear, it will be enough to prove that $r(u_{\alpha'} u_{\beta'}) = r(u_{\alpha'}) r(u_{\beta'})$, for all $\alpha', \beta' \in \mathscr{P}$. From the definitions (1), (2) in section 1

$$r(u_{\alpha'} u_{\beta'}) = \sum_{\lambda, \alpha, \beta} v^{\langle \alpha, \beta \rangle + \langle \alpha', \beta' \rangle} \cdot g^{\lambda}_{\alpha' \beta'} g^{\lambda}_{\alpha\beta} \cdot a_\alpha a_\beta \frac{1}{a_\lambda} \cdot (u_\alpha \otimes u_\beta) , \tag{2.2a}$$

and

(2.2b)
$$r(u_{\alpha'})r(u_{\beta'}) = \sum_{\substack{\rho,\sigma,\rho',\sigma',\\ \alpha,\beta}} v^D \cdot g^{\alpha'}_{\rho\sigma} g^{\beta'}_{\rho'\sigma'} g^{\alpha}_{\rho\rho'} g^{\beta}_{\sigma\sigma'} \cdot a_\rho a_\sigma a_{\rho'} a_{\sigma'} \frac{1}{a_{\alpha'} a_{\beta'}} \cdot (u_\alpha \otimes u_\beta) ,$$

where

(2.2c) $$D = \langle \rho, \sigma \rangle + \langle \rho', \sigma' \rangle + \langle \rho, \rho' \rangle + \langle \sigma, \sigma' \rangle + \sigma \cdot \rho' .$$

The sums above are taken over all values in $\mathscr{P}$ of the variables indicated. However from the definition of $g^{\lambda}_{\alpha\beta}$ it follows that $g^{\lambda}_{\alpha\beta} \neq 0$ implies $\mathbf{dim}\, U_\lambda = \mathbf{dim}\, U_\alpha + \mathbf{dim}\, U_\beta$, for any $\alpha, \beta, \lambda \in \mathscr{P}$. So we may, and shall, assume in (2.2a) that

(2.2d) $$\mathbf{dim}\, U_\alpha + \mathbf{dim}\, U_\beta = \mathbf{dim}\, U_\lambda = \mathbf{dim}\, U_{\alpha'} + \mathbf{dim}\, U_{\beta'} ,$$

and in (2.2b) that

(2.2e) $$\mathbf{dim}\, U_\rho + \mathbf{dim}\, U_\sigma = \mathbf{dim}\, U_{\alpha'}, \quad \mathbf{dim}\, U_{\rho'} + \mathbf{dim}\, U_{\sigma'} = \mathbf{dim}\, U_{\beta'} ,$$

$$\mathbf{dim}\, U_\rho + \mathbf{dim}\, U_{\rho'} = \mathbf{dim}\, U_\alpha \quad \text{and} \quad \mathbf{dim}\, U_\sigma + \mathbf{dim}\, U_{\sigma'} = \mathbf{dim}\, U_\beta .$$

From (2.2e) we have $\langle \alpha', \beta' \rangle = \langle \rho, \rho' \rangle + \langle \rho, \sigma' \rangle + \langle \sigma, \rho' \rangle + \langle \sigma, \sigma' \rangle$ and $\langle \alpha, \beta \rangle = \langle \rho, \sigma \rangle + \langle \rho, \sigma' \rangle + \langle \rho', \sigma \rangle + \langle \rho', \sigma' \rangle$, and hence

$$D = \langle \alpha, \beta \rangle + \langle \alpha', \beta' \rangle - 2\langle \rho, \sigma' \rangle .$$

Now multiply both (2.2a) and (2.2b) by $a_{\alpha'} a_{\beta'} \cdot v^{-\langle \alpha,\beta \rangle - \langle \alpha',\beta' \rangle}$. The coefficients of $u_\alpha \otimes u_\beta$ in the resulting sums are

$$N_1 = N_1(\alpha, \beta, \alpha', \beta') = \sum_\lambda g^{\lambda}_{\alpha\beta} g^{\lambda}_{\alpha'\beta'} a_\alpha a_\beta a_{\alpha'} a_{\beta'} \cdot \frac{1}{a_\lambda} \quad \text{and}$$
$$N_2 = N_2(\alpha, \beta, \alpha', \beta') = \sum_{\rho,\sigma,\rho',\sigma'} |k|^{-\langle \rho, \sigma' \rangle} g^{\alpha}_{\rho\rho'} g^{\beta}_{\sigma\sigma'} g^{\alpha'}_{\rho\sigma} g^{\beta'}_{\rho'\sigma'} a_\rho a_\sigma a_{\rho'} a_{\sigma'} ,$$

respectively, bearing in mind that $v^2 = |k|$. Thus to prove Theorem 1, it is enough to prove $N_1 = N_2$, for all $\alpha, \beta, \alpha', \beta' \in \mathscr{P}$. We may state this equality as the following theorem.

Theorem 2. *Let $\mathscr{P}$ be the set of all isomorphism classes of finite R-modules, where R is a finitary, hereditary algebra over the finite field k. Let $\alpha, \beta, \alpha', \beta'$ be fixed elements of $\mathscr{P}$. Then there holds*

$$a_\alpha a_\beta a_{\alpha'} a_{\beta'} \sum_\lambda g^{\lambda}_{\alpha\beta} g^{\lambda}_{\alpha'\beta'} \frac{1}{a_\lambda} = \sum_{\rho,\sigma,\rho',\sigma'} \frac{|\mathrm{Ext}^1_R(U_\rho, U_{\sigma'})|}{|\mathrm{Hom}_R(U_\rho, U_{\sigma'})|} g^{\alpha}_{\rho\rho'} g^{\beta}_{\sigma\sigma'} g^{\alpha'}_{\rho\sigma} g^{\beta'}_{\rho'\sigma'} a_\rho a_\sigma a_{\rho'} a_{\sigma'} .$$

From now on $\alpha, \beta, \alpha', \beta'$ are fixed elements of $\mathscr{P}$. Since (2.2d), (2.2e) may be assumed to hold in the sums defining N_1 and N_2, we assume that

$\dim_k U_\lambda = n$ for all terms in the sum defining N_1, where $n = \dim_k U_\alpha + \dim_k U_\beta = \dim_k U_{\alpha'} + \dim_k U_{\beta'}$.

2.3. *The set $\mathscr{Q}$*

We define a set $\mathscr{Q}$, whose cardinal determines the number $N_1 = N_1(\alpha, \beta, \alpha', \beta')$.

(2.3a) Lemma. *Let U_ξ, U_η, U_θ be R-modules in the classes $\xi, \eta, \theta \in \mathscr{P}$, respectively. Then the number of short exact sequences $0 \to U_\eta \xrightarrow{p} U_\theta \xrightarrow{s} U_\xi \to 0$ in R-fin is $g^\theta_{\xi\eta} a_\xi a_\eta$.*

Proof. The submodule $W = \operatorname{Im} p = \operatorname{Ker} s$ of U_θ can be chosen in $g^\theta_{\xi\eta}$ ways. With W given, there are a_ξ ways of choosing s, and a_η ways of choosing p. □

Now let E be a fixed k-space of dimension n. Let $\operatorname{Rep}(R,E)$ be the set of all representations τ of R on E, i.e. of all k-algebra homomorphisms $\tau : R \to \operatorname{End}_k(E)$. Each such τ determines an R-module (E, τ), by making R act on E by the rule $xe = \tau(x)(e)$, for $x \in R$, $e \in E$. The general linear group $G_n = GL(E)$ acts on $\operatorname{Rep}(R,E)$ in a well known way: $(g, \tau) \mapsto g\tau g^{-1}$. Then elements τ, τ' of $\operatorname{Rep}(R,E)$ are in the same G_n-orbit if and only if $(E,\tau) \cong (E,\tau')$ in R-fin. From this we have the next lemma.

(2.3b) Lemma. *The number of elements $\tau \in \operatorname{Rep}(R,E)$, such that (E,τ) belongs to a given class $\lambda \in \mathscr{P}$, is $|G_n|/a_\lambda$.*

Definition. *$\mathscr{Q} = \mathscr{Q}(\alpha, \beta, \alpha', \beta')$ is the set of all quintets $q = (\tau, p, s, p', s')$ such that $\tau \in \operatorname{Rep}(R,E)$, and p, s, p', s' are R-maps such that*

$$(2.3c) \qquad 0 \to U_\beta \xrightarrow{p} (E,\tau) \xrightarrow{s} U_\alpha \to 0, \quad 0 \to U_{\beta'} \xrightarrow{p'} (E,\tau) \xrightarrow{s'} U_{\alpha'} \to 0$$

are both exact sequences.

(2.3d) Proposition. $|\mathscr{Q}| = |G_n| \cdot N_1$.

Proof. With $\tau \in \operatorname{Rep}(R,E)$ fixed, the number of quintets $(\tau, p, s, p', s') \in \mathscr{Q}$ is the number of pairs (2.3c) of exact sequences. By lemma (2.3a), this number is $g^\lambda_{\alpha\beta} g^\lambda_{\alpha'\beta'} a_\alpha a_\beta a_{\alpha'} a_{\beta'}$, where λ is the class of (E,τ). Now sum over all $\tau \in \operatorname{Rep}(R,E)$, and use lemma (2.3b). □

2.4. *The set $\mathscr{O}$*

We next define a set $\mathscr{O}$, whose cardinal is closely connected with the number $N_2 = N_2(\alpha, \beta, \alpha', \beta')$.

Definition. *Let $\mathscr{O} = \mathscr{O}(\alpha, \beta, \alpha', \beta')$ be the set of all octets $\Delta = (A, A', B, B', \pi_1, \pi_2, \pi_3, \pi_4)$ such that A, A', B, B' are R-submodules of $U_\alpha, U_{\alpha'}, U_\beta, U_{\beta'}$, respec-*

tively, and $\pi_1, \pi_2, \pi_3, \pi_4$ *are R-isomorphisms as follows:* $\pi_1 : U_\alpha/A \to U_{\alpha'}/A'$, $\pi_2 : U_\beta/B \to A'$, $\pi_3 : U_{\beta'}/B' \to A$, $\pi_4 : B \to B'$.

Definition. *Let* $\Delta \in \mathscr{O}$ *be as above. Then the* **type** *of* Δ *is* $(\rho, \sigma, \rho', \sigma')$, *where these are the isomorphism classes of the R-modules* $U_\alpha/A, A', A, B$, *respectively.*

(2.4a) Lemma. *The number of octets* $\Delta \in \mathscr{O}$ *of given type* $(\rho, \sigma, \rho', \sigma')$ *is* $g^\alpha_{\rho\rho'} g^\beta_{\sigma\sigma'} g^{\alpha'}_{\rho\sigma} g^{\beta'}_{\rho'\sigma'} a_\rho a_\sigma a_{\rho'} a_{\sigma'}$.

Proof. There are $g^\alpha_{\rho\rho'}$ ways of choosing the submodule A of U_α, since U_α/A and A must be in classes ρ and ρ', respectively. Similarly there are $g^\beta_{\sigma\sigma'}, g^{\alpha'}_{\rho\sigma}, g^{\beta'}_{\rho'\sigma'}$ ways of choosing A', B, B', respectively. With A, A', B, B' all chosen, the number of quartets of isomorphisms $(\pi_1, \pi_2, \pi_3, \pi_4)$ is $a_\rho a_\sigma a_{\rho'} a_{\sigma'}$. □

2.5. *The map* $f: \mathscr{Q} \to \mathscr{O}$

This map provides the connection between the sets $\mathscr{Q}$ and $\mathscr{O}$, by which we shall later prove that $N_1 = N_2$. Suppose that $q = (\tau, p, s, p', s') \in \mathscr{Q}$. Then we define the octet $f(q) = (A, A', B, B', \pi_1, \pi_2, \pi_3, \pi_4)$ as follows.

Define $A = \operatorname{Im} sp'$, $A' = \operatorname{Im} s'p$, $B = \operatorname{Ker} s'p$, $B' = \operatorname{Ker} sp'$; these are submodules of $U_\alpha, U_{\alpha'}, U_\beta, U_{\beta'}$, respectively. Next define isomorphisms $\pi_1 : U_\alpha/A \to U_{\alpha'}/A'$, $\pi_2 : U_\beta/B \to A'$, $\pi_3 : U_{\beta'}/B' \to A$, $\pi_4 : B \to B'$ by the following prescriptions. (Here $x_\alpha, x_{\alpha'}, \ldots$ denote elements of $U_\alpha, U_{\alpha'}, \ldots$.)

$\pi_1(x_\alpha + A) = x_{\alpha'} + A'$ if and only if there is some $e \in E$ such that $s(e) = x_\alpha$, $s'(e) = x_{\alpha'}$.

$\pi_2(x_\beta + B) = x_{\alpha'}$ if and only if $s'p(x_\beta) = x_{\alpha'}$.

$\pi_3(x_{\beta'} + B') = x_\alpha$ if and only if $sp'(x_{\beta'}) = x_\alpha$.

$\pi_4(x_\beta) = x_{\beta'}$ if and only if $p(x_\beta) = p'(x_{\beta'})$.

It is easy to verify that these rules do indeed define isomorphisms as required. We give the verification for π_1, as an example. Let Π_1 be the submodule of $U_\alpha \oplus U_{\alpha'}$ consisting of all $(x_\alpha, x_{\alpha'})$ such that there is some $e \in E$ such that $s(e) = x_\alpha$, $s'(e) = x_{\alpha'}$. Since s and s' are both surjective, every element $x_\alpha \in U_\alpha$, and every element $x_{\alpha'} \in U_{\alpha'}$, appears in some $(x_\alpha, x_{\alpha'}) \in \Pi_1$. Also $(x_\alpha, 0) \in \Pi_1$ if and only if $e \in \operatorname{Ker} s' = \operatorname{Im} p'$, i.e. if and only if $x_\alpha \in s(\operatorname{Im} p') = \operatorname{Im} sp' = A$. Similarly $(0, x_{\alpha'}) \in \Pi_1$ if and only if $x_{\alpha'} \in A'$. This proves that the rule above defines an R-isomorphism $\pi_1 : U_\alpha/A \to U_{\alpha'}/A'$.

It is our intention to prove the following fact about the fibres of the map $f : \mathscr{Q} \to \mathscr{O}$.

(2.5a) Proposition. *Let* $\Delta \in \mathscr{O}$ *have type* $(\rho, \sigma, \rho', \sigma')$. *Then* $|f^{-1}(\Delta)| = |G_n| \cdot |k|^{-\langle \rho, \sigma' \rangle}$.

This will give a proof of Theorem 1. For from (2.4a) and (2.5a) we deduce

$$\begin{aligned}
|\mathcal{Q}| &= \textstyle\sum_{\Delta\in\mathcal{O}} |f^{-1}(\Delta)| \\
&= \sum_{\rho,\sigma,\rho',\sigma'} |G_n| \cdot |k|^{-\langle\rho,\sigma'\rangle} g^{\alpha}_{\rho\rho'} g^{\beta}_{\sigma\sigma'} g^{\alpha'}_{\rho\sigma} g^{\beta'}_{\rho'\sigma'} a_\rho a_\sigma a_{\rho'} a_{\sigma'} \\
&= |G_n| \cdot N_2 .
\end{aligned}$$

But by (2.3d), $|\mathcal{Q}| = |G_n| \cdot N_1$. Hence $N_1 = N_2$, and this proves part (iii) of Theorem 1 (see 2.2).

2.6. *A diagram for* $f^{-1}(\Delta)$

For the rest of section 2, let $\Delta = (A, A', B, B', \pi_1, \pi_2, \pi_3, \pi_4)$ be a fixed element of $\mathcal{O} = \mathcal{O}(\alpha, \beta, \alpha', \beta')$, of type $(\rho, \sigma, \rho', \sigma')$. Construct the following short exact sequences from Δ:

(2.6a) $$0 \to A \oplus A' \xrightarrow{h} X \xrightarrow{h'} U_\alpha/A \to 0 \quad \text{and}$$

(2.6b) $$0 \to B \xrightarrow{j'} Y \xrightarrow{j} A \oplus A' \to 0 ,$$

where $X = \{(x_\alpha, x_{\alpha'}) \in U_\alpha \oplus U_{\alpha'} : \pi_1(x_\alpha + A) = x_{\alpha'} + A'\}$, h is the inclusion map, $h'(x_\alpha, x_{\alpha'}) = x_\alpha + A$ in sequence (2.6a), and $Y = (U_{\beta'} \oplus U_\beta)/M$ where $M = \{(-\pi_4(b), b) : b \in B\}$, $j'(b) = [0, b] = [\pi_4(b), 0]$, $j[x_{\beta'}, x_\beta] = (\pi_3(x_{\beta'} + B'), \pi_2(x_\beta + B))$ in sequence (2.6b). (We use the notation $[x_{\beta'}, x_\beta] = (x_{\beta'}, x_\beta) + M$ for a typical element of the pushout Y.)

It is routine to verify that the maps in (2.6a) and (2.6b) are well defined, and that both sequences are exact. We now place (2.6a) as the upper horizontal sequence, and (2.6b) as the left-hand vertical sequence in the diagram (2.6c) below. Keeping these fixed, we shall show that the elements of $f^{-1}(\Delta)$ correspond bijectively with the ways of "filling out" (2.6c), i.e. with the triples (τ, c, d) such that (2.6c) is exact and commutative (notice that $d' = h'c$ and $c' = dj'$ are automatically determined by c and d).

(2.6c) $$\begin{tikzcd}
 & 0 & 0 & & \\
0 \arrow[r] & A \oplus A' \arrow[u] \arrow[r, "h"] & X \arrow[u] \arrow[r, "h'"] & U_\alpha/A \arrow[r] & 0 \\
0 \arrow[r] & Y \arrow[u, "j"] \arrow[r, "d"] & (E, \tau) \arrow[u, "c"'] \arrow[r, "d'"] & U_\alpha/A \arrow[u, equal] \arrow[r] & 0 \\
 & B \arrow[u, "j'"] \arrow[r, equal] & B \arrow[u, "c'"'] & & \\
 & 0 \arrow[u] & 0 \arrow[u] & &
\end{tikzcd}$$

(2.6d) Proposition. (i) *Suppose that* $q = (\tau, p, s, p', s')$ *lies in* $f^{-1}(\Delta)$ *Define maps* $c : (E,\tau) \to X$ *and* $d : Y \to (E,\tau)$ *by*

(*) $c(e) = (s(e), s'(e))$, *for all* $e \in E$, *and*

(**) $d[x_{\beta'},x_\beta] = p'(x_{\beta'}) + p(x_\beta)$, *for all* $[x_{\beta'},x_\beta] \in Y$.

Define also $d' = h'c$, $c' = dj'$. *Then* (2.6c) *is exact and commutative.*

(ii) *Suppose conversely that* τ, c, d *are given* ($\tau \in \mathrm{Rep}(R, E)$), *so that, taking* $d' = h'c$, $c' = dj'$, (2.6c) *is exact and commutative. Then there are unique R-maps* $s : (E,\tau) \to U_\alpha$, $s' : (E,\tau) \to U_{\alpha'}$ *such that* $(*)$ *holds, and unique R-maps* $p : U_\beta \to (E,\tau)$, $p' : U_{\beta'} \to (E,\tau)$ *such that* $(**)$ *holds. Moreover the sequences* $0 \to U_\beta \xrightarrow{p} (E,\tau) \xrightarrow{s} U_\alpha \to 0$ *and* $0 \to U_{\beta'} \xrightarrow{p'} (E,\tau) \xrightarrow{s'} U_{\alpha'} \to 0$ *are both exact, and* $f(q) = \Delta$, *where* $q = (\tau, p, s, p', s')$.

The proof of this proposition is by a series of routine verifications. Most of these are left to the reader, but we give three of them, as examples.

Example 1. Verify, in (i), that $cd = hj$. We have $hj[x_{\beta'},x_\beta] = (\pi_3(x_{\beta'} + B'), \pi_2(x_\beta+B))$ by our definitions. On the other hand $cd[x_{\beta'},x_\beta] = c(p'(x_{\beta'})+ p(x_\beta)) = (sp'(x_{\beta'}), s'p(x_\beta))$, using (*) and (**) and $s'p' = 0$, $sp = 0$. But $sp'(x_{\beta'}) = \pi_3(x_{\beta'}+B')$ and $s'p(x_\beta) = \pi_2(x_\beta+B)$, because $f(q) = \Delta$ (see 2.5).

Example 2. Verify, in (ii), that $\mathrm{Ker}\, s = \mathrm{Im}\, p$. Since (**) must hold, the maps p, p' are given by $p(x_\beta) = d[0,x_\beta]$, $p'(x_{\beta'}) = d[x_{\beta'},0]$. Since (*) must hold, the maps s,s' are given by $s(e) = p_1c(e)$, $s'(e) = p_2c(e)$, where p_1, p_2 are the projections of $U_\alpha \oplus U_{\alpha'}$ onto $U_\alpha, U_{\alpha'}$, respectively. So $sp(x_\beta) = sd[0,x_\beta] = p_1cd[0,x_\beta] = p_1hj[0,x_\beta]$ (we are given that $cd = hj$). We know from Example 1 that $hj[0,x_\beta] = (0, \pi_2(x_\beta + B))$. Hence $sp(x_\beta) = 0$ for all $x_\beta \in U_\beta$. Therefore $\mathrm{Ker}\, s \geqslant \mathrm{Im}\, p$. It remains to prove that $\mathrm{Ker}\, s \leqslant \mathrm{Im}\, p$. Let $e \in \mathrm{Ker}\, s$, so that $c(e) = (0,x_{\alpha'})$ for some $x_{\alpha'} \in U_{\alpha'}$. Therefore $h'c(e) = 0$, i.e. $e \in \mathrm{Ker}\, d' = \mathrm{Im}\, d$. Thus $e = d[x_{\beta'},x_\beta]$, for some $[x_{\beta'},x_\beta] \in Y$. This shows that $0 = s(e) = p_1cd[x_{\beta'},x_\beta] = p_1hj[x_{\beta'},x_\beta] = \pi_3(x_{\beta'}+B')$, which implies $x_{\beta'} \in B'$, hence $x_{\beta'} = \pi_4(b)$ for some $b \in B$ (we have an isomorphism $\pi_4 : B \to B'$). So $e = d[x_{\beta'},x_\beta] = d[0, b + x_\beta] = p(b + x_\beta)$ lies in $\mathrm{Im}\, p$.

Example 3. In proving (ii) we must show that $f(q) = \Delta$, where $q = (\tau, p,s, p',s')$. Let us prove that $A' = \mathrm{Im}\, s'p$. From the descriptions of p, s' given in the last example, $s'p(x_\beta) = s'd[0,x_\beta] = p_2cd[0,x_\beta] = p_2hj[0,x_\beta] = \pi_2(x_\beta+B)$, for all $x_\beta \in U_\beta$. Therefore $\mathrm{Im}\, s'p = \mathrm{Im}\, \pi_2 = A'$. The same calculation shows that π_2 satisfies the prescription given in 2.5, namely a pair $(x_\beta,x_{\alpha'})$ in $U_\beta \oplus U_{\alpha'}$ satisfies $\pi_2(x_\beta + B) = x_{\alpha'}$ if and only if $s'p(x_\beta) = x_{\alpha'}$.

2.7. *A Lemma on extensions in R-fin*

The following will be needed in the next paragraph.

(2.7a) Lemma. *Let* $\tau \in \mathrm{Rep}(R,E)$, *and suppose that* $\mathbf{E} : 0 \to U \xrightarrow{a} (E,\tau) \xrightarrow{b} V \to 0$ *is an exact sequence in R-fin belonging to the extension class* $\xi \in$

$\mathrm{Ext}^1_R(V,U)$. *Then the set* $\mathscr{E}$ *of all exact sequences* $\mathbf{E}' : 0 \to U \xrightarrow{a'} (E,\tau') \xrightarrow{b'} V \to 0$ *belonging to* ξ (τ' *can be any element of* $\mathrm{Rep}(R,E)$), *has cardinal* $|G_n|/|\mathrm{Hom}_R(V,U)|$.

Proof. $\mathbf{E},\mathbf{E}'$ are in the same extension class if and only if there is some $g \in G_n = \mathrm{Aut}_k(E)$ such that $\mathbf{E}' = g\mathbf{E}$, where $g\mathbf{E} : 0 \to U \xrightarrow{ga} (E,\, g\tau g^{-1}) \xrightarrow{bg^{-1}} V \to 0$. So G_n acts transitively on $\mathscr{E}$, and $|\mathscr{E}| = |G_n|/|G_{\mathbf{E}}|$, where $G_{\mathbf{E}} = \{g \in G_n : g\mathbf{E} = \mathbf{E}\}$. We must prove that $|G_{\mathbf{E}}| = |\mathrm{Hom}_R(V,U)|$. Let $W = \mathrm{Im}\ a$. $G_{\mathbf{E}}$ consists of all $g \in G_n$ such that $ga = a, bg^{-1} = b$ and $g\tau g^{-1} = \tau$. The first two conditions say that g acts identically on W and on E/W, respectively. It follows that $g = id_E + ahb$, for some $h \in \mathrm{Hom}_k(V,U)$. The condition $g\tau g^{-1} = \tau$ is equivalent to the condition that $h \in \mathrm{Hom}_R(V,U)$. The correspondence $g \mapsto h$ sets up a bijection (in fact a group isomorphism) $G_{\mathbf{E}} \to \mathrm{Hom}_R(V,U)$. Therefore $|G_{\mathbf{E}}| = |\mathrm{Hom}_R(V,U)|$, are required.

2.8. *Proof of proposition* (2.5*a*)

Proposition (2.6d) shows that the set $f^{-1}(\Delta)$ is in bijective correspondence with the set T of all trios (τ,c,d) such that the diagram (2.6c) is exact and commutative. Thus to prove Proposition (2.5a), it will be enough to prove

(2.8a)
$$|T| = |G_n| \cdot |k|^{-\langle \rho,\sigma' \rangle}\ .$$

Because Δ has type $(\rho,\sigma,\rho',\sigma')$ we may take $U_\alpha/A = U_\rho$ (see 2.4). Then $(\tau,c,d) \in T$ if and only if the diagram

(2.8b)
$$\begin{array}{ccccccccc} 0 & \to & A \oplus A' & \xrightarrow{h} & X & \xrightarrow{h'} & U_\rho & \to & 0 \\ & & \uparrow j & & \uparrow c & & \| & & \\ 0 & \to & Y & \xrightarrow[d]{} & (E,\tau) & \xrightarrow[d']{} & U_\rho & \to & 0 \end{array}$$

is exact and commutative. Let η be the element of $\mathrm{Ext}^1_R(U_\rho, A \oplus A')$ corresponding to the top row of (2.8b), i.e. to the exact sequence (2.6a). Given an exact sequence $0 \to Y \xrightarrow{d} (E,\tau) \xrightarrow{d'} U_\rho \to 0$, a necessary and sufficient condition that there exist a map $c : (E,\tau) \to X$ such that (2.8b) is commutative, is that the corresponding element $\zeta \in \mathrm{Ext}^1_R(U_\rho, Y)$ should satisfy

(2.8c)
$$j^*(\zeta) = \eta,$$

where $j^* = \mathrm{Ext}^1_R(j)$ (see, for example, [3, p.66]).

Apply the functor $\mathrm{Hom}_R(U_\rho, -)$ to (2.6b), and replace B by $U_{\sigma'}$ (which is permissible because B is in class σ', see 2.4). We get the following exact "Ext" sequence, in which we abbreviate Hom_R to H, and Ext^1_R to E:

(2.8d)
$$\begin{aligned} 0 \to H(U_\rho, Y_{\sigma'}) \to H(U_\rho, Y) \to H(U_\rho, A \oplus A') \to E(U_\rho, U_{\sigma'}) \\ \to E(U_\rho, Y) \xrightarrow[j^*]{} E(U_\rho, A \oplus A') \to 0\ . \end{aligned}$$

Notice that $\mathrm{Ext}^2(U_\rho, -) = 0$, because R is hereditary.

(2.8d) shows that j^* is surjective, consequently (2.8c) has solutions ζ. The set of all such solutions is a coset of the k-subspace $S = \mathrm{Ker}\ j^*$ of $H(U_\rho, Y)$. Hence the number of all solutions ζ of (2.8c) is $|S| = |k|^{\dim S}$ ($\dim S = \dim_k S$).

We may construct from (2.8d) another exact sequence (2.8d′), by replacing the three final terms $E(U_\rho, Y)$, $E(U_\rho, A \oplus A'), 0$ of (2.8d) by $S(= \mathrm{Ker}\ j^*), 0, 0$, respectively. The alternating sum of the dimensions (as k-spaces) of the terms in (2.8d′) is zero. This gives a formula for $\dim S$, from which follows a formula for $|S| = |k|^{\dim S}$, namely

$$|S| = |E(U_\rho, U_{\sigma'})||H(U_\rho, Y)| \,/\, |H(U_\rho, A \oplus A')||H(U_\rho, U_{\sigma'})\,. \tag{2.8e}$$

We may now count the elements (τ, c, d) of T, as follows. First choose a solution ζ of (2.8c), which can be done in $|S|$ ways. By lemma (2.7a), there are $|G_n|/|H(U_\rho, Y)|$ exact sequences

$$0 \to Y \xrightarrow{d} (E, \tau) \xrightarrow{d'} U_\rho \to 0 \tag{2.8f}$$

in the extension class ζ. Fix (2.8f). We know that there is at least one R-map $c : (E, \tau) \to X$ such that (2.8b) commutes. An easy "diagram chase" shows that the condition for any R-map $c' : (E, \tau) \to X$ to have the same property, is that $z = c - c'$ should satisfy

$$\mathrm{Im}\ z \subseteq \mathrm{Im}\ h \quad \text{and} \quad \mathrm{Ker}\ z \supseteq \mathrm{Im}\ d\,. \tag{2.8g}$$

But the set of all such z, is a k-subspace of $\mathrm{Hom}_R((E, \tau), X)$ which is clearly isomorphic to $H(U_\rho, \mathscr{A} \oplus A')$. So with (2.8f) given the number of ways of choosing c is $|H(U_\rho, A\oplus, A')|$. Putting all this together we have

$$|T| = |S| \cdot \big(|G_n|/|H(U_\rho, Y)|\big) \cdot |H(U_\rho, A \oplus A')|\,,$$

and then, using (2.8e), $|T| = |G_n||\mathrm{Ext}^1_R(U_\rho, U_{\sigma'})|/|\mathrm{Hom}_R(U_\rho, U_{\sigma'})|$. But the definition of the Ringel form (see section 1) tells us that $\langle \rho, \sigma' \rangle = \dim \mathrm{Hom}_R (U_\rho, U_{\sigma'}) - \dim \mathrm{Ext}^1_R(U_\rho, U_{\sigma'})$. Therefore $|T| = |G_n||k|^{-\langle \rho, \sigma' \rangle}$, which proves Proposition (2.5a), and with it Theorem 1.

3. Lusztig algebras

3.1. The class $\mathscr{L}(\mathscr{A}, v, I, \cdot)$

Our aim in this section is to describe a class of associative, graded algebras which includes Lusztig's algebra **f** and also Ringel's composition algebra $C_{\mathscr{A},v}(R)$ (for definitions see 3.3), and which may perhaps have some further interest.

A pair $(I, \cdot)$ consisting of a set I and a symmetric, bilinear, $\mathbb{Z}$-valued form $(i, j) \mapsto i \cdot j$ on $\mathbb{Z}I$ ($\mathbb{Z}I$ is the free Abelian group with I as basis) will be called a *datum* (we need not yet assume that $(I, \cdot)$ is a *Cartan datum* in Lusztig's sense, see 3.4).

Definition. *Let $(I, \cdot)$ be a datum, $\mathscr{A}$ an integral domain containing $\mathbb{Z}$, and v any invertible element of $\mathscr{A}$. Then an $\mathscr{A}$-algebra L is said to belong to the class $\mathscr{L}(\mathscr{A}, v, I, \cdot)$ if the following conditions* **L1**, **L2**, **L3** *are satisfied.*

L1 $L = \sum_{\nu}^{\oplus} L_{\nu}$ is an $\mathbb{N}I$-graded, associative $\mathscr{A}$-algebra generated by elements $u_i \in L_i (i \in I)$; also $L_0 = \mathscr{A}.1$, where 1 is the identity element of L. The elements $u_i (i \in I)$ will be called *the generators* of L.

L2 There is an $\mathscr{A}$-linear map $r : L \to L \otimes L$ ($\otimes$ means $\otimes_{\mathscr{A}}$) such that
(i) $r(u_i) = u_i \otimes 1 + 1 \otimes u_i$ for all $i \in I$, and
(ii) r is a map of $\mathscr{A}$-algebras, where the product in $L \otimes L$ is given by *Lusztig's rule*, viz.

$$(x \otimes y)(x' \otimes y') = v^{|y| \cdot |x'|}(xx') \otimes (yy') \tag{3.1a}$$

for all homogeneous x, y, x', y', $\in L$ (we write $|z| = \nu$ if $z \in L_{\nu}, \nu \in \mathbb{N}I$). The map r will be called the *co-multiplication* on L.

L3 There is a symmetric, $\mathscr{A}$-bilinear form $(-,-) : L \times L \to \mathscr{A}$ (possibly degenerate) such that
(i) $(L_{\mu}, L_{\nu}) = 0$ for all $\mu \neq \nu$ in $\mathbb{N}I$,
(ii) $(1, 1) = 1$, and $(u_i, u_i) \neq 0$ for all $i \in I$, and
(iii) $(x, yz) = (r(x), y \otimes z)$, for all $x, y, z \in L$.
This form $(-,-)$ will be called *the bilinear form* on L. (The form on $L \otimes L$ which features in (iii) is defined by $(x \otimes y, x' \otimes y') = (x, x')(y, y')$, for all x, $y, x', y' \in L$.)

Remark. If $L \in \mathscr{L}(\mathscr{A}, v, I, \cdot)$, it is clear that r is uniquely determined by **L2**. Proposition (3.2a) below will show that the form $(-,-)$ is uniquely determined by **L3**, as soon as the elements $(u_i, u_i) (i \in I)$ are given.

3.2. *The elements $M_{a,b}(t)$*

If $\nu = \sum_{i \in I} \nu_i i$ is an element of $\mathbb{N}I$, let tr $\nu = \sum_i \nu_i$ [2, p.2]. Now let $\nu \neq 0$, and write $p = \operatorname{tr} \nu$. Define $I(\nu)$ to be the set of all vectors $a = (a_1, \ldots, a_p) \in I^p$ which have *weight* ν, i.e. which satisfy

$$\nu_i = |\{\pi \in \mathbb{N} : 1 \leqq \pi \leqq p, a_{\pi} = i\}|, \text{ all } i \in I.$$

Define $I(0)$ to consist of a single element $\emptyset$. Let $I(\infty)$ denote the disjoint union $\bigcup_{\nu \in \mathbb{N}I} I(\nu)$.

If $u_i (i \in I)$ are the generators of an algebra $L \in \mathscr{L}(\mathscr{A}, v, I, \cdot)$, and if $\nu \in \mathbb{N}I$, then by **L1**, L_{ν} is the A-span of the monomials $u_a = u_{a_1} \ldots u_{a_p}, a \in I(\nu)$; in case $\nu = 0$, we define $u_{\emptyset} = 1$. If $a \in I(\mu), b \in I(\nu)$, for distinct elements $\mu, \nu \in \mathbb{N}I$, then $(u_a, u_b) = 0$ by **L3** (i).

(3.2a) Proposition. *Let $\nu \in \mathbb{N}I$, and let a, b be elements of $I(\nu)$. Then there exists an element $M_{a,b}(t) \in \mathbb{Z}[t, t^{-1}]$ (t indeterminate) such that for any $\mathscr{A}$, v, I,. as in 3.1, and for any $L \in \mathscr{L}(\mathscr{A}, v, I, .)$ with generators $u_i (i \in I)$, there holds*

$$(3.2b) \qquad (u_a, u_b) = M_{a,b}(v).B_\nu(L) \, ,$$

where $B_\nu(L) = \prod_{i \in I} (u_i, u_i)^{\nu_i}$.

The proof of this proposition is given in 3.6 , together with an explicit formula for $M_{a,b}(t)$. This explicit formula is not needed in the present paper. The following lemma contains our main application of $M_{a,b}(t)$.

(3.2c) Lemma. *Let $L \in \mathscr{L}(\mathscr{A}, v, I, \cdot)$ be as in* 3.1. *Then each element of L can be written in the form $x = \sum_{a \in I(\infty)} c_a u_a$, where the $c_a \in \mathscr{A}$, and $c_a = 0$ for all but a finite number of $a \in I(\infty)$. Then x lies in rad$(-,-)$ if and only if*

$$(3.2d) \qquad \sum_{a \in I(\nu)} c_a M_{a,b}(v) = 0 \; for \; all \; b \in I(\nu), and \; all \, \nu \in \mathbb{N}I \, .$$

Proof. The first statement follows from **L1**. It is clear that x lies in rad$(-,-)$ if and only if $(x, u_b) = 0$ for all $b \in I(\nu)$ and all $\nu \in \mathbb{N}I$. But this condition is equivalent to (3.2d) by **L3**, (3.2b) and the fact that $B_\nu(L) \neq 0$ for all $\nu \in \mathbb{N}I$.

3.3. Examples of algebras in $\mathscr{L}(\mathscr{A}, v, I,)$

The first two examples below are due to Lusztig, and show that for any $\mathscr{A}$, v, I, $\cdot$, the class $\mathscr{L}(\mathscr{A}, v, I, \cdot)$ is not empty, and it even contains a *non-degenerate* member L for which $(-,-)$ is a non-degenerate form on L.

(*3.3a*) *Example* (Lusztig). Let $'F$ be the free $\mathscr{A}$-algebra on free generators $'\theta_i (i \in I)$. $'F$ has a natural $\mathbb{N}I$-grading, such that for each $\nu \in \mathbb{N}I, 'F_\nu$ is the $\mathscr{A}$-span of the monomials $'\theta_a = {'\theta_{a_1}} \ldots {'\theta_{a_p}} (a \in I(\nu))$. The argument in [2, pp.2–4] extends trivially to our situation, to show that $'F$ has a co-multiplication r and symmetric bilinear form $(-,-)$ which make $'F$ a member of $\mathscr{L}(\mathscr{A}, v, I, \cdot)$. The construction of Lusztig in fact goes through with arbitrary non-zero elements of $\mathscr{A}$ for the $('\theta_i, '\theta_i)(i \in I)$. Lusztig's algebra $'\mathbf{f}$ [2, p.2] is the algebra $'F$ just described, for $\mathscr{A} = \mathbb{Q}(t)$ (t indeterminate, denoted v in [2]), $v = t, (I, \cdot)$ a Cartan datum, and with $('\theta_i, '\theta_i) = (1 - t^{-i.i})^{-1}$, $i \in I$.[1]

[1] (p.19) For our purpose, the bilinear form on $'\mathbf{f}$ could be defined with any non-zero values for $('\theta_i, '\theta_i)$. Lusztig's normalization $('\theta_i, '\theta_i) = (1 - t^{-i \cdot i})^{-1}$ is required for the definition of the canonical signed basis [2, Theorem 14.2.3].

(*3.3b*) *Example* (Lusztig). Given $L \in \mathscr{L}(\mathscr{A}, v, I, \cdot)$ with generators $u_i (i \in I)$ and bilinear form $(-,-)$, the argument on [2, p.5] shows that $J = \operatorname{rad}(-,-)$ is an ideal of L, and that (1) $J = \sum_{v \in \mathbb{N}I}(L_v \cap J)$, and (2) $r(J) \leqq J \otimes L + L \otimes J$. Therefore $L^0 = L/J$ is a member of $\mathscr{L}(\mathscr{A}, v, I, \cdot)$, with generators $u_i^0 = u_i + J (i \in I)$, co-multiplication r^0 and bilinear form $(-,-)^0$ inherited in obvious ways from L. It is clear that $(-,-)^0$ is non-degenerate, i.e. $\operatorname{rad}(-,-)^0$ is zero. In particular, Lusztig's algebra $\mathbf{f}$ [2, p.5] is the non-degenerate member $('\mathbf{f})^0$ of $\mathscr{L}(\mathbb{Q}(t), t, I, \cdot)$. We shall denote the generators $('\theta_i)^0$ of $\mathbf{f}$ by $\theta_i (i \in I)$.

(*3.3c*) *Ringel's composition algebra.* Suppose that we are in the situation of Theorem 1 (section 1). The finitary, hereditary k-algebra R provides us with a datum $(I, \cdot)$, where I is the set of simple isomorphism classes in R-fin, and $\cdot$ is Ringel's symmetric form ${}_{\dot{R}}$. The algebra $H_{\mathscr{A},v}(R)$ satisfies all the conditions **L1**, **L2**, **L3**, except that is not, in general, generated by the symbols $u_i (i \in I)$. However the $\mathscr{A}$-subalgebra $C = C_{\mathscr{A},v}(R)$ of $H_{\mathscr{A},v}(R)$ generated by the $u_i (i \in I)$, which clearly satisfies $r(C) \leqq C \otimes C$, is a member of $\mathscr{L}(\mathscr{A}, v, I, \cdot)$. $C_{\mathscr{A},v}(R)$ is called the *composition algebra* in Ringel's terminology [5, p.586], [6, p.396]. In some important cases, it coincides with $H_{\mathscr{A},v}(R)$ [8, Sect. 7].

3.4. *The generic composition algebra $C^*(I, \cdot)$*

In this sub-section and the next, we assume that $(I, \cdot)$ is a *Cartan datum* [2, p.2], i.e. that I is finite and that there hold

(a) $i \cdot i \in \{2, 4, 6, \dots\}$ for all $i \in I$, and

(b) $2\dfrac{i \cdot j}{i \cdot i} \in \{0, -1, -2, \dots\}$ for all $i \neq j$ in I.

Notice that $\Delta = (a_{ij})_{i,j \in I}$ is a symmetrizable (generalized) Cartan matrix, where $a_{ij} = 2(i \cdot j)/(i \cdot i)$, for all $i, j \in I$.

Given any finite field k, it is possible to find a finite dimensional, hereditary k-algebra R_k whose isomorphism classes of simple modules may be indexed by I, and in such a way that $i \cdot j = i_{\dot{R}_k} j = \langle i, j\rangle_{R_k} + \langle j, i\rangle_{R_k}$, for all $i, j \in I$ (see section 1). (C. Ringel, private communication. If the diagram Δ_0 associated to the Cartan matrix Δ is simply-laced, one may take R_k to be the path algebra kQ, where the quiver Q is made by orienting Δ_0 in any way which gives no oriented cycles. For the general case one may use the tensor ring constructed from a suitable modulation of Δ_0; see [1, p.5].)

Let $\mathscr{K}$ be a set of finite fields k, such that the set $\{|k| : k \in \mathscr{K}\}$ is infinite. Let $\mathscr{A}$ be an integral domain containing $\mathbb{Q}$, and also containing, for each $k \in \mathscr{K}$, an element v_k such that $v_k^2 = |k|$. For each $k \in \mathscr{K}$, the composition algebra $C_k = C_{\mathscr{A},v_k}(R_k)$ (see (3.3c)) is the $\mathscr{A}$-algebra generated by the elements $u_i^{(k)} (i \in I)$ of the Ringel–Hall algebra $H_{\mathscr{A},v_k}(R_k)$. Following Ringel [6, p.398], we consider the subring $C(I, \cdot)$ of the direct product $\prod_{k \in \mathscr{K}} C_k = \prod C_k$ which is generated by $\mathbb{Q}$ and the elements t, t^{-1} and $u_i (i \in I)$ of

$\prod C_k$ whose k-components are, respectively, v_k, v_k^{-1} and $u_i^{(k)}$. Since t is a central element of $C(I,\cdot)$, and satisfies no polynomial equation $p(t) = 0$, unless $p(T) \in \mathbb{Q}(T)$ is zero, we may regard $C(I,\cdot)$ as the $\mathscr{A}$-algebra generated by the $u_i (i \in I)$, where $\mathscr{A} = \mathbb{Q}[t,t^{-1}]$, t being treated as an indeterminate. Define the $\mathbb{Q}(t)$-algebra $C^*(I,\cdot) = \mathbb{Q}(t) \otimes_{\mathscr{A}} C(I,\cdot)$. This is a *generic composition algebra of type* $(I,\cdot)$. It is generated by the elements $u_i^* = 1 \otimes u_i (i \in I)$. From now on, we take $\mathscr{A} = \mathbb{Q}[t,t^{-1}]$.

Let $'\mathbf{f}_{\mathscr{A}}$ be the $\mathscr{A}$-subalgebra of $'\mathbf{f}$ (see (3.3a)) which is generated by the $'\theta_i (i \in I)$; it is a free $\mathscr{A}$-algebra on these generators. $'\mathbf{f}_{\mathscr{A}}$ is a member of $\mathscr{L}(\mathscr{A},t,I,\cdot)$, with co-multiplication and bilinear form inherited from $'\mathbf{f} \in \mathscr{L}(\mathbb{Q}(t),t,I,\cdot)$. Denote the bilinear form on $'\mathbf{f}$ by $'(-,-)$, and let $J = \operatorname{rad} '(-,-)$. Then J is an ideal of $'\mathbf{f}$, and (by definition) $\mathbf{f} = {'\mathbf{f}}/J$.

(3.4a) Proposition. *Let $\mathscr{X} : {'\mathbf{f}_{\mathscr{A}}} \to C(I,\cdot)$ be the surjective $\mathscr{A}$-algebra map which takes $'\theta_i \mapsto u_i\ (i \in I)$. Then*

(i) *The kernel of $\mathscr{X}$ lies in $J = \operatorname{rad} '(-,-)$.*

(ii) *There is an $\mathscr{A}$-algebra map $\psi : C(I,\cdot) \to \mathbf{f}_{\mathscr{A}}$, where $\mathbf{f}_{\mathscr{A}} = {'\mathbf{f}_{\mathscr{A}}}/{'\mathbf{f}_{\mathscr{A}}} \cap J$; this map takes $u_i \mapsto {'\theta_i} + ({'\mathbf{f}_{\mathscr{A}}} \cap J)$, for all $i \in I$.*

Proof. (i) Let $x = \sum c_a(t)'\theta_a$ be an element of $'\mathbf{f}$, so that $c_a(t) \in \mathscr{A}$ for all $a \in I(\infty)$, and almost all $c_a(t) = 0$. Take any $k \in \mathscr{K}$. The k-th component of $\mathscr{X}(x)$ is $\mathscr{X}(x)^{(k)} = \sum c_a(v_k)u_a^{(k)} \in C_k$. If $\mathscr{X}(x) = 0$ then $\mathscr{X}(x)^{(k)}$ is zero, hence lies in $\operatorname{rad}(-,-)_{C_k}$. By lemma (3.2c)

$$\sum_{a \in I(v)} c_a(v_k)M_{a,b}(v_k) = 0 \text{ for all } b \in I(v) \text{ and all } v \in \mathbb{N}I.$$

Since this holds for all $k \in \mathscr{K}$, the element $\sum_{a \in I(v)} c_a(t)M_{a,b}(t)$ of $\mathscr{A}$ must be zero, for it has infinitely many zeros v_k in the integral domain $\mathscr{A}$. And this holds, for all $b \in I(v)$ and all $v \in \mathbb{N}I$. So by another application of (3.2c), we have $x \in J$. (ii) Let $\xi \in C(I,\cdot)$. Then there is some $x \in {'\mathbf{f}_{\mathscr{A}}}$ such that $\mathscr{X}(x) = \xi$. Define $\psi(\xi) = x + ({'\mathbf{f}_{\mathscr{A}}} \cap J)$. This is consistent by (i). Clearly ψ has the required properties. □

(3.4b) Corollary. *There is a $\mathbb{Q}(t)$-algebra map $\psi^* : C^*(I,\ \cdot\ ) \to \mathbf{f}$ which takes $u_i^* \mapsto \theta_i\ (= {'\theta_i} + J)$ for all $i \in I$.*

Proof. We get ψ^* by applying the functor $\mathbb{Q}(t) \otimes_{\mathscr{A}} -$ to the $\mathscr{A}$-algebra map $\psi : C(I,\ \cdot\ ) \to \mathbf{f}_{\mathscr{A}}$ of (3.4a) (ii). But we must prove that the natural $\mathbb{Q}(t)$-linear map $\mathbb{Q}(t) \otimes_{\mathscr{A}} \mathbf{f}_{\mathscr{A}} \to \mathbf{f}$ is an isomorphism. This will follow if we prove that $\mathbf{f}_{\mathscr{A}} = {'\mathbf{f}_{\mathscr{A}}}/J \cap {'\mathbf{f}_{\mathscr{A}}}$ is a free $\mathscr{A}$-module, because in that case the $\mathscr{A}$-module exact sequence $0 \to J \cap {'\mathbf{f}_{\mathscr{A}}} \to {'\mathbf{f}_{\mathscr{A}}} \to \mathbf{f}_{\mathscr{A}} \to 0$ splits, hence remains exact after applying $\mathbb{Q}(t) \otimes_{\mathscr{A}} -$, which gives us what we want. To prove that $\mathbf{f}_{\mathscr{A}}$ is free, it is enough to prove that $(\mathbf{f}_{\mathscr{A}})_v = ({'\mathbf{f}_{\mathscr{A}}})_v/J \cap ({'\mathbf{f}_{\mathscr{A}}})_v$ is free, for all $v \in \mathbb{N}I$. But this last module is finitely generated over the principal ideal domain $\mathscr{A}$. So it will be enough to prove that $({'\mathbf{f}_{\mathscr{A}}})_v/J \cap ({'\mathbf{f}_{\mathscr{A}}})_v$ is torsion-free, i.e. that

$J \cap ('\mathbf{f}_{\mathscr{A}})_v$ is a pure $\mathscr{A}$-submodule of $('\mathbf{f}_{\mathscr{A}})_v$. This is an immediate consequence of lemma (3.2c) (applied to $'\mathbf{f}_{\mathscr{A}} \in \mathscr{L}(\mathscr{A},t,I,\ \cdot\ ))$, which tells us that $x = \sum_{a\in I(v)} c_a(t)'\theta_a$ lies in $J \cap '\mathbf{f}_{\mathscr{A}}$ if and only if $\sum c_a(t)M_{a,b}(t) = 0$ for all $b \in I(v)$. □

3.5. *The quantum Serre relations*

Let $(I,\ \cdot\ )$ be a Cartan datum. We recall that the positive part U^+ of the Drinfeld–Jimbo quantization $U = U^- \otimes U^0 \otimes U^+$ of the enveloping algebra $\mathscr{U}(g)$, where g is any Kac–Moody Lie algebra associated to $(I,\ \cdot\ )$ or to Δ, is by definition the $\mathbb{Q}(t)$-algebra with generators $E_i (i \in I)$, and with the *quantum Serre relations* $F_{1-a_{ij}}(t^{i\cdot i/2}, E_i, E_j) = 0$ for all $i \neq j$ in I, as defining relations. Here, for any integer $m \geqq 1$, we define the polynomial over $\mathscr{A} = \mathbb{Q}[t,t^{-1}]$ in two non-commuting indeterminates X, Y

$$F_m(t,X,Y) = \sum_{p=0}^{m} (-1)^p \begin{bmatrix} m \\ p \end{bmatrix} X^p Y X^{m-p} ,$$

and $\begin{bmatrix} m \\ p \end{bmatrix}$ is the "quantum binomial coefficient" with t as parameter (see [2, p. 10], which gives the definition with v as parameter).

Ringel has proved [7, Proposition 2] that (for each $k \in \mathscr{K}$) *the generators $u_i^{(k)}$ of $C_k = C_{\mathscr{A},v_k}(R_k)$ satisfy the quantum Serre relations, with the parameter t replaced by v_k*. It follows that the u_i (hence also the $u_i^* = 1 \otimes u_i$) satisfy the quantum Serre relations. So by (3.4b) we have a new proof of a theorem of Lusztig, that the generators θ_i of $\mathbf{f}$ satisfy the quantum Serre relations[2] [2, Proposition 1.4.3]. Ringel's remarkable discovery also gives the following.

(3.5a) Proposition. (Ringel). *There is a $\mathbb{Q}(t)$-algebra map $\rho : U^+ \to C^*(I,\ \cdot\ )$ which takes $E_i \mapsto u_i^*$ for all $i \in I$.*

However Lusztig shows [2, Theorem 33.1.3][3] that there is a $\mathbb{Q}(t)$-algebra isomorphism $\lambda : \mathbf{f} \to U^+$ which takes $\theta_i \mapsto E_i$ for all $i \in I$. It is clear that $\rho\lambda\psi^*$ is the identity map on $C^*(I,\ \cdot\ )$. Therefore both ψ^* and ρ are isomorphisms, which proves the next theorem.

Theorem 3. *Let $(I,\ \cdot\ )$ be a Cartan datum, U^+ the positive part of a Drinfeld–Jimbo quantum group U of type $(I,\ \cdot\ )$, and $C^*(I,\ \cdot\ )$ a generic composition algebra as described in* 3.4. *Then there is a $\mathbb{Q}(t)$-algebra isomorphism $C^*(I,\ \cdot\ ) \to U^+$ taking $u_i^* \mapsto E_i$ for all $i \in I$.*

Remark. Theorem 3 is due to Ringel in case $(I,\ \cdot\ )$ is of finite (Dynkin) or affine (Euclidean) type ([8, Theorem 7], [6, p. 400]). Ringel's proof of (3.5a) is valid for all Cartan data $(I,\ \cdot\ )$.

[2] I am indebted to the referee for this observation.

[3] The proof of this theorem requires the representation theory of the (non-quantized) Kac-Moody algebras, but does not use perverse sheaves.

3.6. Proof of Proposition (3.2a)

This is by induction on $p = \operatorname{tr} \nu = \sum \nu_i$. If $p = 0$, then $a = b = \emptyset$, and $(u_a, u_b) = (1, 1) = 1$, by **L3**(ii). So (3.2b) is satisfied by taking $M_{\emptyset,\emptyset}(t) = 1$. Assume now that $p \geqq 1$ and that the proposition holds for $p-1$. Let $\nu \in \mathbb{N}I$ be such that $p = \operatorname{tr} \nu$. Notation: if $a \in I^p$ and S is a subset of $\underline{p} = \{1, \ldots, p\}$, we denote by $a(S)$ the vector of length $p - |S|$ obtained by removing from $a = (a_1, \ldots, a_p)$ all the terms $a_\sigma (\sigma \in S)$. In case $S = \{\pi\}$ for some $\pi \in p$, write $a[\pi]$ for $a(S)$.

Now let $a, b \in I(\nu)$. We have $u_b = u_{b[p]} u_{b_p}$, with the above notation. So by **L2** and **L3**, $(u_a, u_b) = (r(u_a), u_{b[p]} \otimes u_{b_p}) =$

$$(1) \qquad \left(\prod_{\pi \in \underline{p}} (u_{a_\pi} \otimes 1 + 1 \otimes u_{a_\pi}),\ u_{b[p]} \otimes u_{b_p} \right) .$$

Expand the product on the left side of (1) as $\sum_{P \subseteqq \underline{p}} z(P)$, where for each subset P of $\underline{p}, z(P) = z_1 \ldots z_p$, where $z_\pi = u_{a_\pi} \otimes 1$ if $\pi \in P$, and $z_{\pi'} = 1 \otimes u_{a'_\pi}$ if $\pi' \in P' = \underline{p} \backslash P$. Multiplying out this product with the aid of (3.1a) we get

$$(2) \qquad z(P) = v^{(a:P)} \cdot u_{a(P')} \otimes u_{a(P)} ,$$

where $(a : P)$ is the integer $\sum a_{\pi'} \cdot a_\pi$, summed over all (π', π) in $P' \times P$ such that $\pi' < \pi$. But by **L3**(i), $(z(P), u_{b[p]} \otimes u_{b_p})$ is zero unless $P' = \{\pi\}$ for some $\pi \in \underline{p}$, and in that case $(z(P), u_{b[p]} \otimes u_{b_p}) = v^{(a:P)} \cdot (u_{a[\pi]}, u_{b[p]})(u_{a_\pi}, u_{b_p})$, with $(a : P) = a_\pi \cdot (a_{\pi+1} + \ldots + a_p)$. So from (1) we find that, using the induction hypothesis,

$$(3) \qquad (u_a, u_b) = \sum_\pi v^{a_\pi \cdot (a_{\pi+1} + \ldots + a_p)} \cdot M_{a[\pi], b[p]}(v) \cdot B_\nu(L) ,$$

the sum being over those $\pi \in \underline{p}$ such that $a_\pi = b_p$. So we may take $M_{a,b}(t) = \sum t^{a_\pi \cdot (a_{\pi+1} + \ldots + a_p)} M_{a[\pi], b[p]}(t)$, and (3.2b) is satisfied. This proves the proposition. By some further calculation we may prove the formula

$$(4) \qquad M_{a,b}(t) = \sum_{as=b} t^{(s:a)} ,$$

where the sum is over all s in the symmetric group $\operatorname{Sym}(\underline{p})$ such that $as = b$ (i.e. $a_{s(\pi)} = b_\pi$, all $\pi \in \underline{p}$), and $(s : a) = \sum a_{\pi'} \cdot a_\pi$, summed over all $(\pi', \pi) \in \underline{p} \times \underline{p}$ such that $\pi' < \pi$ and $s^{-1}(\pi') > s^{-1}(\pi)$.

Acknowledgements. I should like to thank Professor Claus Ringel, and the referee, who have each made very useful comments, and whose suggestions have simplified the exposition in section 3. The main results in this paper were announced at meetings at the Technion, Haifa, Israel (Group Representation Theory Workshop, May 30–June 9, 1994) and at the University of Bielefeld, Germany (Quantum Groups and Related Topics, July 7–9, 1994). My thanks are due to the organizers of both these meetings for their kind hospitality.

References

1. Dlab, V., Ringel, C.M.: Indecomposable representations of graphs and algebras. Memoirs Am. Math. Soc. No. 173, 1976
2. Lusztig, G.: Introduction to Quantum Groups. Birkäuser, Boston, 1993
3. MacLane, S.: Homology, Springer, Berlin Göttingen Heidelberg, 1963
4. Ringel, C.M.: Hall algebras. In: Topics in Algebra, Banach Center Publ. **26**(1990) 433–447
5. Ringel, C.M.: Hall algebras and quantum groups. Invent. Math. **101**(1990) 583–592
6. Ringel, C.M.: From representations of quivers via Hall and Loewy algebras to quantum groups. Contemp. Math. **131**(1992) 381–401
7. Ringel, C.M.: Hall algebras revisited. In: Proceedings Israel Conference on Quantum deformations of algebras and their representations 1991/1992
8. Ringel, C.M.: The Hall algebra approach to quantum groups, Notas de Cursos, Escuela Latinoamericana de Matemáticas, Aportaciones Matemáticas, Sociedad Matemática Mexicana, 1993
9. Zelevinsky, A.V.: Representations of finite classical groups. Lecture Notes in Math. No. 869, Springer, Berlin Heidelberg New York 1981