TOPICS IN ALGEBRA
BANACH CENTER PUBLICATIONS, VOLUME 26, PART 1
PWN POLISH SCIENTIFIC PUBLISHERS
WARSAW 1990

HALL ALGEBRAS

CLAUS MICHAEL RINGEL

Fakultät für Mathematik, Universität Bielefeld
Bielefeld, F.R.G.

The free abelian group with basis indexed by the isomorphism classes of finite p-groups may be endowed with a product by counting filtrations of finite p-groups: we obtain what is called the Hall algebra $\mathscr{H}(\mathbf{Z}_p)$ of the ring $\mathbf{Z}_p$ of p-adic integers. It is a commutative and associative ring with identity element and plays an important role in algebra and combinatorics. It was first studied by Steinitz [S], and later by Ph. Hall [H]; a good account is the book by I. G. Macdonald [M].

The basic concept may be generalized to fairly arbitrary rings. Under a mild finiteness condition on the ring R, one may define a similar product on the free abelian group with basis indexed by the set $\mathscr{B}$ of isomorphism classes of finite R-modules (where finite means to have finitely many elements, not just finite length), and one obtains an associative ring $\mathscr{H}(R)$ with identity element, the integral Hall algebra of R. In contrast to the case $R = \mathbf{Z}_p$, the Hall algebras in general need not be commutative; in fact, our main concern will be the corresponding Lie algebras.

The investigations presented here will deal with the special case of R a representation-directed algebra over a finite field k. As in the classical case $\mathscr{H}(\mathbf{Z}_p)$, the structure constants turn out to be evaluations of integral polynomials which we call Hall polynomials. In order to obtain a generic Hall algebra $\mathscr{H}(R, \mathbf{Z}[T])$, we take the free $\mathbf{Z}[T]$-module with basis indexed by $\mathscr{B}$, and use the Hall polynomials as structure constants. Of particular interest seems to be the specialization $\mathscr{H}(R)_1$ of $\mathscr{H}(R, \mathbf{Z}[T])$ for $T = 1$. Note that the additive group of $\mathscr{H}(R)_1$ is again the free abelian group on $\mathscr{B}$, but the product is defined by evaluating the Hall polynomials at 1. We denote by $K(R\text{-mod})$ the free abelian group with basis indexed by the set of isomorphism classes of indecomposable finite modules [Gr]. By definition, $K(R\text{-mod})$ is a subgroup of

This paper is in final form and no version of it will be submitted for publication elsewhere.

$\mathscr{H}(R)_1$, and it turns out that $K(R\text{-mod})$ is even a Lie subalgebra. Actually, $\mathscr{H}(R)_1 \otimes \mathbf{Q}$ is just the universal enveloping algebra of $K(R\text{-mod}) \otimes \mathbf{Q}$, and the $\mathbf{Z}$-form $\mathscr{H}(R)_1$ of $\mathscr{H}(R)_1 \otimes \mathbf{Q}$ is quite analoguous to the Kostant $\mathbf{Z}$-form for a semisimple complex Lie algebra.

The stimulus for these investigations was the following: Let A be a finite-dimensional hereditary algebra over some base field k. In case k is algebraically closed, Gabriel [Ga] showed that the isomorphism classes of indecomposable A-modules correspond bijectively to the positive roots of the corresponding semisimple complex Lie algebra $\mathbf{g}$, and this result was extended to arbitrary base fields in a joint paper [DR] with Dlab. In particular, the $\mathbf{C}$-dimension of $K(A\text{-mod}) \otimes_{\mathbf{Z}} \mathbf{C}$ coincides with the $\mathbf{C}$-dimension of $\mathbf{n}_+$, where $\mathbf{g} = \mathbf{n}_- \oplus \mathbf{h} \oplus \mathbf{n}_+$ is a triangular decomposition of $\mathbf{g}$. It is natural to ask whether it is possible to use the representation theory for A in order to define a Lie product on $K(A\text{-mod})$ so that $K(A\text{-mod}) \otimes_{\mathbf{Z}} \mathbf{C}$ and $\mathbf{n}_+$ are isomorphic Lie algebras. A partial answer to this question is given in this paper: we show that $K(A\text{-mod})$, or, more generally, $K(R\text{-mod})$ for any representation-directed algebra R, carries in a natural way the structure of a Lie algebra. In a subsequent publication [R2], it will be shown that this Lie structure is the one we want to have: we will show that $K(A\text{-mod})$ is the Chevalley $\mathbf{Z}$-form of $\mathbf{n}_+$.

The results of this paper and an outline of the calculations of [R2] have been presented at the Antwerp conference and the Ottawa–Moosonee workshop in 1987, and at the Banach Center in Warsaw in 1988. The author is grateful to these institutions for providing the possibility of discussing these investigations; in particular, he has learnt from R. Dipper, B. Pareigis and L. Scott that there is a strong relationship to recent advances on Hopf algebras and quantum groups [D]; a detailed account on this relationship will be given in [R3], see also [R4].

For unexplained notions concerning the representation theory of algebras we refer to [R1], for those concerning Lie theory, we refer to [Hu].

1. The integral Hall algebra of a finitary ring

Given a finite set M, we denote its cardinality by $|M|$.

Rings will always be assumed to be associative. We will not insist on a ring R to have an identity element; however, we will assume that there exists a set of idempotents $e_i \in R$ $(i \in I)$ such that $R = \bigoplus_{i,j \in I} e_i R e_j$. For a (left) R-module M, we will assume that $RM = M$, or, equivalently, that $M = \bigoplus_{i \in I} e_i M$. Of course, in case R has an identity element 1, we may take as such a set of idempotents the one-element set $\{1\}$, so in this case R-modules are just unital left R-modules. (There are several reasons for dealing with the more general case of rings which do not necessarily have an identity element: First of all, we incorporate the so-called "rings with several objects": any small additive category $\mathscr{C}$ gives rise to a ring $R_{\mathscr{C}} = \bigoplus_{a,b} \mathscr{C}(a, b)$, where a, b run through all objects of $\mathscr{C}$, with multiplication given by the composition in $\mathscr{C}$ and extended by zero; the $R_{\mathscr{C}}$-modules just correspond to the additive functors from $\mathscr{C}$ into the category of abelian groups. Even if we are only interested in rings with identity it may be necessary to invoke other rings which lack an identity element; typical examples are given in the covering theory for finite-dimensional algebras. Finally, given a family R_i $(i \in I)$ of rings, we may form the direct sum $\bigoplus R_i$ with componentwise operations and this again will be a ring even if I is infinite.)

Let R be a ring. The category of all R-modules will be denoted by R-Mod, and R-mod is the category of R-modules of finite length. If the R-modules M, M' are isomorphic, we write $M \cong M'$, and we denote the isomorphism class of M by $[M]$. We are mainly interested in modules with only finitely many elements and call them *finite* R-modules. The full subcategory of R-Mod given by the finite R-modules will be denoted by R-fin. Thus, if R is finite, R-fin $= R$-mod.

Of course, finite modules are of finite length, thus we can apply the theorems of Krull–Schmidt and Jordan–Hölder. Given any R-module M of finite length, and any simple R-module S, we denote by $(\mathbf{dim}\, M)_S$ the Jordan–Hölder multiplicity of S in M (i.e. the number of composition factors in a composition series of M which are isomorphic to S), and we call the function $\mathbf{dim}\, M$ the *dimension vector* of M. We denote by $K(R)$ the set of functions from the set of isomorphism classes of simple R-modules to $\mathbf{Z}$ which have finite support. With respect to componentwise addition, $K(R)$ is an abelian group, and for any R-module M of finite length, $\mathbf{dim}\, M$ may be considered as an element of $K(R)$.

LEMMA 1. *Let R be a ring. The following properties are equivalent:*

(i) $\mathrm{Ext}^1_R(M_1, M_2)$ *is finite for all finite R-modules M_1, M_2.*

(ii) $\mathrm{Ext}^1_R(S_1, S_2)$ *is finite for all simple finite R-modules S_1, S_2.*

(iii) *The number of isomorphism classes of finite R-modules with fixed dimension vector is finite.*

(iv) *The number of isomorphism classes of finite R-modules of length* 2 *with fixed dimension vector is finite.*

Proof. (i)$\Rightarrow$(iii). By induction, we assume that the number of isomorphism classes of finite R-modules of length n with fixed dimension vector is finite. Let M be a finite R-module of length $n+1$, with dimension vector $d = \mathbf{dim}\, M$. Let S be simple with $d_S \neq 0$, and let $d' = d - \mathbf{dim}\, S$. Let M' be a module with dimension vector d'. Clearly, both S and M' are finite R-modules, thus $\mathrm{Ext}^1_R(M', S)$ is finite. Thus, the number of isomorphism classes of modules M with a submodule $U \cong S$ such that $M/U \cong M'$ is finite. Since there are only finitely many choices for the isomorphism classes of S and M', it follows that there are only finitely many isomorphism classes of such modules M.

(iv)$\Rightarrow$(ii). Let S_1, S_2 be simple finite R-modules, and let $0 \to S_2 \xrightarrow{f} M \xrightarrow{g} S_1 \to 0$ be an exact sequence. There are only finitely many isomorphism classes of modules M with $\mathbf{dim}\, M = \mathbf{dim}\, S_1 + \mathbf{dim}\, S_2$, say $[M_1], \ldots, [M_t]$, and up to equivalence in $\mathrm{Ext}_R^1(S_1, S_2)$, we may assume $M = M_i$ for some $1 \leqslant i \leqslant t$. Since $\mathrm{Hom}_R(S_2, M_i)$ and $\mathrm{Hom}_R(M_i, S_1)$ are finite for all i, there are only finitely many elements in $\mathrm{Ext}_R^1(S_1, S_2)$.

(ii)$\Rightarrow$(i). We use induction on the length of M_1 and M_2 and the long exact Hom sequences.

In case the equivalent conditions (i)–(iv) are satisfied, R will be said to be *finitary*. The rings considered throughout this paper will be assumed to be finitary.

EXAMPLES. (a) *Any finitely generated ring is finitary.* (In particular, all finite rings are finitary.) For, assume the ring R is generated by $r_1, \ldots, r_n$. An R-module is an abelian group with prescribed endomorphisms given by scalar multiplication by $r_1, \ldots, r_n$. But the number of isomorphism classes of abelian groups of fixed finite order is finite, and given such an abelian group, the number of endomorphisms is finite, thus the number of isomorphism classes of R-modules with a fixed number of elements is finite. [On the other hand, the polynomial ring $R = k[X_1, X_2, \ldots]$ in countably many variables over a finite field k is not finitary: let S be the one-dimensional R-module annihilated by all X_i. Clearly, $\mathrm{Ext}_R^1(S, S)$ is infinite-dimensional over k, thus S is finite, whereas $\mathrm{Ext}_R^1(S, S)$ is not finite.]

(b) *If R is finitary, and $R \to R'$ is an epimorphism of rings, then R' is finitary.* For, the canonical functor ι: R'-Mod $\to$ R-Mod is fully faithful. Given finite R'-modules M_1, M_2, then $\iota(M_1), \iota(M_2)$ are finite R-modules, and ι yields an injective map from the set of isomorphism classes of R'-modules with dimension vector $\mathbf{dim}\, M_1 + \mathbf{dim}\, M_2$ into the set of isomorphism classes of R-modules with dimension vector $\mathbf{dim}\, \iota(M_1) + \mathbf{dim}\, \iota(M_2)$.

(c) A ring R may be called a *discrete valuation domain* provided it has no nonzero zero divisors, and there exists a nonzero maximal ideal I such that the only nonzero one-sided ideals are the powers of I. If R is a discrete valuation domain with maximal ideal I, then up to isomorphism, R/I^t is the only indecomposable R-module of length t, for $t \in \mathbb{N}_1$. It follows that the isomorphism classes of the R-modules of finite length n correspond bijectively to the partitions of n (cf. [M], Section II.1). It follows that R is always finitary. Of course, the only interesting case for considering finite R-modules is the case where R/I is finite, since otherwise the only finite R-module is the zero module.

Let R be any ring, and $N_1, \ldots, N_t$ and M finite R-modules. Let $F^M_{N_1, \ldots, N_t}$ be the number of filtrations

$$M = U_0 \supseteq U_1 \supseteq \ldots \supseteq U_t = 0$$

of M such that $U_{i-1}/U_i \cong N_i$, for $1 \leqslant i \leqslant t$. (Note that in case $N_1, \ldots, N_t$ are in addition simple, we just count the number of composition series with prescribed composition factors.)

Assume that R is a finitary ring. Let $\mathscr{H}(R)$ be the free abelian group with basis $(u_{[M]})_{[M]}$, indexed by the set of isomorphism classes of finite R-modules. Instead of $u_{[M]}$ we will also write u_M. We define on $\mathscr{H}(R)$ a multiplication by the following rule:

$$u_{[N_1]}u_{[N_2]} = \sum_{[M]} F^M_{N_1N_2}u_{[M]};$$

note that on the right, we deal with a finite sum, since $F^M_{N_1N_2} \neq 0$ only for those modules M which satisfy $\mathbf{dim}\, M = \mathbf{dim}\, N_1 + \mathbf{dim}\, N_2$, and R is assumed to be finitary.

PROPOSITION 1. *$\mathscr{H}(R)$ is an associative ring with* 1.

Proof. The identity element is $u_{[0]}$, the associativity of this multiplication follows from the fact that the coefficient of $u_{[M]}$ in either $u_{N_1}(u_{N_2}u_{N_3})$ or $(u_{N_1}u_{N_2})u_{N_3}$ is just $F^M_{N_1N_2N_3}$.

We call $\mathscr{H}(R)$ the *integral Hall algebra* of R. The special case of $R = \mathbf{Z}$ (or of a discrete valuation domain with finite residue field) was considered by Hall [H] in 1959 when he introduced his "algebra of partition". The denomination Hall algebra, in this special case, seems to be due to I. G. Macdonald [M] and is widely accepted. However, the reader should be aware that already in 1900, Steinitz [S] considered the Hall algebra $\mathscr{H}(\mathbf{Z})$.

In contrast to $R = \mathbf{Z}$, or R a discrete valuation domain, the Hall algebras in general are not commutative. For example, let $R = \left[\begin{smallmatrix} k & k \\ 0 & k \end{smallmatrix}\right]$, the ring of upper-triangular 2×2 matrices over the finite field k. Then there are two nonisomorphic simple R-modules S_1, S_2, and a nonsplit exact sequence $0 \to S_2 \to P \to S_1 \to 0$, whereas $\operatorname{Ext}^1_R(S_2, S_1) = 0$. It follows that in $\mathscr{H}(R)$, we have

$$u_{S_1}u_{S_2} = u_{S_1\oplus S_2} + u_P,$$

but

$$u_{S_2}u_{S_1} = u_{S_1\oplus S_2}.$$

PROPOSITION 2. *The rings $\mathscr{H}(R^{\mathrm{op}})$ and $\mathscr{H}(R)^{\mathrm{op}}$ are isomorphic.*

Proof. The functor $D := \operatorname{Hom}_{\mathbf{Z}}(-, \mathbf{Q}/\mathbf{Z})$ is a duality from R-fin to R^{op}-fin. It follows that $F^{DM}_{DN_2,DN_1} = F^M_{N_1,N_2}$, for arbitrary finite R-modules, thus we obtain an isomorphism of rings $\mathscr{H}(R)^{\mathrm{op}} \to \mathscr{H}(R^{\mathrm{op}})$ by sending $u_{[M]}$ to $u_{[DM]}$.

PROPOSITION 3. *If R_i $(i \in I)$ is a family of rings, $\mathscr{H}(\bigoplus_{i\in I} R_i)$ and $\bigotimes_{i\in I}\mathscr{H}(R_i)$ are isomorphic. For any ring R, let $R_p = R\otimes_{\mathbf{Z}}\mathbf{Z}_p$, where $\mathbf{Z}_p$ are the p-adic numbers. Then $\mathscr{H}(R)$ and $\mathscr{H}(\bigoplus_{p\in P} R_p)$, with P the set of prime numbers, are isomorphic.*

Proof. Clearly,

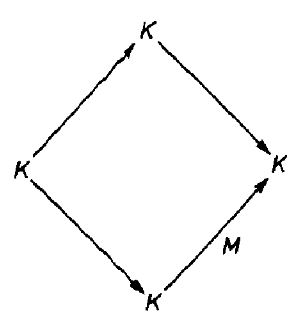
$$\Big(\bigoplus_{i\in I} R_i\Big)\text{-fin} = \coprod_{i\in I} R_i\text{-fin} \quad \text{and} \quad R\text{-fin} = \coprod_{p\in P} R_p\text{-fin}.$$

2. The Hall polynomials for a representation-directed algebra

Let k be a field, and R a finite-dimensional k-algebra. We denote by Γ_R the Auslander–Reiten quiver of R, it is a proper valued translation quiver. Recall that a valued translation quiver $\Gamma = (\Gamma_0, \Gamma_1, \tau, d, d')$ is given by a translation quiver $(\Gamma_0, \Gamma_1, \tau)$ (without loops or multiple arrows) and functions d, d': $\Gamma_1 \to \mathbf{N}_1$ such that for any arrow $y \to z$ with z nonprojective, we have $d_{\tau z,y} = d'_{y,z}$ and $d'_{\tau z,y} = d_{y,z}$ (here, $d_{y,z} = d(y \to z)$ and $d'_{y,z} = d'(y \to z)$). Let Γ be a proper valued translation quiver. A function e: $\Gamma_0 \to \mathbf{N}_1$ with $e(x)d'_{xy} = d_{xy}e(y)$ for any arrow $x \to y$ is called a *symmetrization.* In case Γ is connected, all symmetrizations of Γ are rational multiples of each other (but there may not exist any), so if there are symmetrizations for Γ, then we denote by e_Γ the unique minimal one.

Assume that R is connected and representation-finite. The vertices $x \in (\Gamma_R)_0$ are the isomorphism classes of indecomposable R-modules, and we choose for any vertex x a representative $M(x) = M(R, x)$ in x. Note that for $x, y \in (\Gamma_R)_0$, the numbers d_{xy}, d'_{xy} are defined as the length of $\operatorname{rad}(M(x), M(y))/\operatorname{rad}^2(M(x), M(y))$ as an $\operatorname{End} M(y)$-module and as an $\operatorname{End} M(x)$-module, respectively. It follows that the function $\dim_k \operatorname{End} M(-)$: $(\Gamma_R)_0 \to \mathbf{N}_1$ is a symmetrization for Γ_R. The integer r with $re_\Gamma = \dim_k \operatorname{End} M(-)$ will be called the *symmetrization index* of the k-algebra R.

Remark. Observe that the symmetrization index of R depends on the base field k. Of course, in case the center of R is a field k', we may assume $k = k'$. On the other hand, we note the following. Even if we assume that there exists a field K with $\operatorname{End} X = K$ for any indecomposable R-module X, we may have $k' \subset K$. A typical example is obtained as follows: Consider the tensor algebra of the species



where all arrows but one are endowed with the canonical bimodule ${}_K K_K$, and where the remaining one is endowed with $M = K$, with canonical operation of K on the left, but with the action on the right being twisted by an automorphism ϱ of K. Let R be the factor algebra of this tensor algebra modulo the square of the radical. Then R is representation-finite, even representation-directed, we have $\operatorname{End} X = K$ for any indecomposable R-module and the center of R is the field of invariants of ϱ. (In R-mod, we recover the K-K-bimodule $K \oplus M$ as follows: Let Q be the unique indecomposable injective R-module of length 3, and P the unique indecomposable projective R-module of length 3. Then $\operatorname{Hom}(Q, P) = K \oplus M$.)

A finite valued translation quiver Γ will be said to be an *Auslander–Reiten quiver* provided there exists a field k and a k-algebra R such that $\Gamma = \Gamma_R$. In this case, given a function a: $\Gamma_0 \to \mathbf{N}_0$, we denote by $M(a) = M(R, a)$ the R-module $\bigoplus_{x \in \Gamma_0} a(x) M(x)$. Let us denote by $\mathscr{B}$ the set of all functions a: $\Gamma_R \to \mathbf{N}_0$. We may consider $\mathscr{B}$ as the set of isomorphism classes of R-modules of finite length, for any k-algebra R with $\Gamma_R = \Gamma$.

Recall that the k-algebra R is said to be *representation-directed* provided R is representation-finite, and the indecomposable R-modules $X_1, \ldots, X_n$ can be ordered in such a way that $\operatorname{Hom}(X_i, X_j) = 0$ for $i > j$. Of course, R is representation-directed if and only if R is representation-finite and Γ_R is directed. Note that for any directed Auslander–Reiten quiver Γ and any finite field k, there exists a k-algebra R with $\Gamma_R = \Gamma$ and arbitrary symmetrization index (construct R inductively using appropriate one-point extensions).

THEOREM 1. *Let Γ be a directed Auslander–Reiten quiver, and $a, b, c \in \mathscr{B}$. There exists a polynomial $\varphi^b_{ca} \in \mathbf{Z}[T]$ with the following property: if k is a field, and R a k-algebra with $\Gamma_R = \Gamma$ and symmetrization index r, then*

$$F^{M(R,b)}_{M(R,c)\,M(R,a)} = \varphi^b_{ca}(|k|^r).$$

The polynomials φ^b_{ca} will be called the *Hall polynomials* for Γ (or for R).

The proof will be done in several steps. The first assertions which we need are well-known. For the convenience of the reader, we include the proofs.

(1) Let $x, z \in \Gamma_0$. There is $h(x, z) \in \mathbf{N}_0$ with $\dim_k \operatorname{Hom}_R(M(x), M(z)) = rh(x, z)$.

Proof. For $x = z$, let $h(x, x) = e_\Gamma(x)$. In general, we use induction on the number of predecessors of z. Note that the sink map for z is of the form $\bigoplus_{y \in z^-} d'_{yz} M(y) \to M(z)$. Let $x \neq z$. If z is projective, then the induced map for $\operatorname{Hom}_R(M(x), -)$ is bijective, therefore let $h(x, z) = \sum_{y \in z^-} d'_{yz} h(x, y)$. If z is not projective, we apply $\operatorname{Hom}_R(M(x), -)$ to the Auslander–Reiten sequence ending with $M(z)$, thus, take $h(x, z) = -h(x, \tau z) + \sum_{y \in z^-} d'_{yz} h(x, y)$.

(1′) Let $a, b \in \mathscr{B}$. There is $h(a, b) \in \mathbf{N}_0$ with $\dim_k \operatorname{Hom}_R(M(a), M(b)) = rh(a, b)$.

Proof.

$$\operatorname{Hom}_R(M(a), M(b)) \cong \bigoplus_{x,y} a(x) b(y) \operatorname{Hom}_R(M(x), M(y)).$$

For $a, b \in \mathscr{B}$, define $\gamma_{ab} = T^{h(a,b)} \in \mathbf{Z}[T]$; thus we can reformulate (1') as follows:

(1'') $|\mathrm{Hom}_R(M(a), M(b))| = \gamma_{ab}(|k|^r)$.

Recall that $K(R)$ denotes the Grothendieck group of R. The set of projective vertices of Γ will be denoted by $\mathscr{P}$. The simple R-modules will be indexed by the elements of $\mathscr{P}$, say, let $S(p)$ be the top of $M(p)$, for $p \in \mathscr{P}$. In this way, we identify $K(R)$ with the set $\mathbf{Z}^{\mathscr{P}}$ of integer-valued functions on $\mathscr{P}$. Given an R-module M, its dimension vector $\mathbf{dim}\, M$ is an element in $K(R) = \mathbf{Z}^{\mathscr{P}}$.

(2) For $a \in \mathscr{B}$ the element $\mathbf{dim}\, M(R, a)$ in $\mathbf{Z}^{\mathscr{P}}$ is independent of R.

Proof. Let $p \in \mathscr{P}$. Then

$$(\mathbf{dim}\, M(R, a))_p = \frac{1}{\dim_k \mathrm{End}_R(M(p))} \dim_k \mathrm{Hom}_R(M(p), M(a))$$

$$= \frac{1}{re_\Gamma(p)} rh(p, a).$$

We consider $\mathbf{Z}^{\mathscr{P}}$ as a partially ordered set, using the componentwise ordering. Given $a: \Gamma_0 \to \mathbf{N}_0$, let $\mathscr{S}(a)$ be the set of all $c: \Gamma_0 \to \mathbf{N}_0$ with $\mathbf{dim}\, M(c) < \mathbf{dim}\, M(a)$. Note that $\mathscr{S}(a)$ is a finite set.

For $x \in \Gamma_0$, and $n \in \mathbf{N}_0$, define $\alpha_{nx} \in \mathbf{Z}[T]$ as follows:

$$\alpha_{nx} = \prod_{i=1}^{n} (\gamma_{xx}^{n} - \gamma_{xx}^{i-1});$$

for $a: \Gamma_0 \to \mathbf{N}_0$, let $\alpha_a \in \mathbf{Z}[T]$ be given by the formula

$$\alpha_a = \prod_{x \in \Gamma_0} \alpha_{a(x)x} \cdot \prod_{\substack{x, y \in \Gamma_0 \\ x \neq y}} \gamma_{xy}^{a(x)a(y)}.$$

Note that α_a is a monic polynomial.

(3) $|\mathrm{Aut}_R M(a)| = \alpha_a(|k|^r)$.

Proof. Since $M(a) = \bigoplus_{x \in \Gamma_0} a(x) M(x)$, the automorphisms can be written as matrices indexed by $\Gamma_0 \times \Gamma_0$, with entries f_{xy}, where f_{xy} is an arbitrary element of $\mathrm{Hom}_R(a(x)M(x), a(y)M(y))$, for $x \neq y$, and an invertible element of $\mathrm{End}_R(a(x)M(x))$, for $x = y$. By (1), we have $|\mathrm{Hom}_R(M(x), M(y))| = \gamma_{xy}(|k|^r)$, thus $|\mathrm{Hom}_R(a(x)M(x), a(y)M(y))| = \gamma_{xy}^{a(x)a(y)}(|k|^r)$. On the other hand, $\mathrm{End}_R(M(x))$ is a division ring, since R is representation-directed. But finite division rings are fields, and the number of elements of $\mathrm{Aut}_R(a(x)M(x)) = \mathrm{Gl}(a(x), \mathrm{End}_R(M(x)))$ is well known to be

$$\prod_{i=1}^{n} (d^n - d^i),$$

with $d = |\mathrm{End}_R(M(x))| = \gamma_{xx}(|k|^r)$, thus $|\mathrm{Aut}_R(a(x)M(x))| = \alpha_{nx}(|k|^r)$.

(4) Given $a, b \in \mathscr{B}$, there are polynomials $\sigma_a^b, \eta_a^b \in \mathbf{Z}[T]$ such that $\sigma_a^b(|k|^r)$ is the number of submodules of $M(b)$ isomorphic to $M(a)$, and $\eta_a^b(|k|^r)$ is the number of submodules U of $M(b)$ with $M(b)/U$ isomorphic to $M(a)$.

Proof. If $\mathbf{dim}\, M(a) \nleq \mathbf{dim}\, M(b)$, let $\sigma_a^b = \eta_a^b = 0$. Now, let $\mathbf{dim}\, M(a) \leqslant \mathbf{dim}\, M(b)$, and use induction on $\mathbf{dim}\, M(b)$. Of course, for $\mathbf{dim}\, M(b) = 0$, thus $a = b = 0$, let $\sigma_a^b = \eta_a^b = 1$. Assume now that $b \neq 0$, and use induction on $\mathbf{dim}\, M(a)$. Define μ_a^b, ε_a^b as follows:

$$\mu_a^b = \gamma_{ab} - \sum_{c \in \mathscr{S}(a)} \eta_c^a \alpha_c \sigma_c^b, \qquad \varepsilon_a^b = \gamma_{ba} - \sum_{c \in \mathscr{S}(a)} \eta_c^b \alpha_c \sigma_c^a.$$

Note that the right-hand sides only involve terms which are already defined. We claim that $\eta_c^a \alpha_c \sigma_c^b(|k|^r)$ is the number of maps $M(a) \to M(b)$ with image isomorphic to $M(c)$. Given a submodule U of $M(a)$, with $M(a)/U$ isomorphic to $M(c)$, we choose a fixed epimorphism g_U: $M(a) \to M(c)$ with kernel U. Similarly, if V is a submodule of $M(b)$ isomorphic to $M(c)$, we fix some monomorphism h_V: $M(c) \to M(b)$ with image V. The maps $M(a) \to M(b)$ with kernel U and image V correspond bijectively to the automorphisms of $M(c)$, where a bijection is given as follows: given an automorphism f of $M(c)$, associate to it the composition

$$M(a) \xrightarrow{g_U} M(c) \xrightarrow{f} M(c) \xrightarrow{h_V} M(b).$$

Clearly, a map $M(a) \to M(b)$ is a monomorphism if and only if its image is not isomorphic to any $M(c)$, with $\mathbf{dim}\, M(c) < \mathbf{dim}\, M(b)$. Thus, $\mu_a^b(|k|^r)$ is the number of monomorphisms $M(a) \to M(b)$. Similarly, $\varepsilon_a^b(|k|^r)$ is the number of epimorphisms $M(b) \to M(a)$.

We claim that both polynomials μ_a^b, ε_a^b are divisible by α_a. We need the following lemma.

LEMMA. *Let $\varphi, \psi \in \mathbf{Z}[T]$, and assume ψ is monic. Then ψ divides φ if and only if the integer $\psi(q)$ divides the integer $\varphi(q)$ for infinitely many $q \in \mathbf{Z}$.*

Proof. Since ψ is monic, we divide φ by ψ with remainder, say $\varphi = \eta\psi + \varrho$, with $\eta, \varrho \in \mathbf{Z}[T]$, and the degree of ϱ smaller than the degree of ψ. The inequality of degrees shows that $|\varrho(x)| < |\psi(x)|$ for all large x. Choose $q \in \mathbf{Z}$ large, with $\psi(q) | \varphi(q)$. Then $\varrho(q)\psi(q)^{-1} = \varphi(q)\psi(q)^{-1} - \eta(q)$ is an integer, and $|\varrho(q)\psi(q)^{-1}| < 1$, thus $\varrho(q) = 0$. But there are infinitely many such q, therefore $\varrho = 0$.

We return to the proof of (4). As above, given a submodule V of $M(b)$ isomorphic to $M(a)$, we fix a monomorphism h_V: $M(b) \to M(a)$ with image V. Then any monomorphism $M(a) \to M(b)$ can be written uniquely as the composition of an automorphism of $M(a)$ followed by some h_V. Thus $\alpha_a(|k|^r)^{-1} \mu_a^b(|k|^r)$ is equal to the number of submodules of $M(b)$ isomorphic to $M(a)$, in particular, it is an integer. Since there is a realization $\Gamma = \Gamma_R$ with an arbitrary finite field k and arbitrary r, we see that $\alpha_a(q)$ divides $\mu_a^b(q)$ for any prime power q, thus α_a divides μ_a^b. Let $\alpha_a^{-1}\mu_a^b = \sigma_a^b$; then $\sigma_a^b(|k|^r)$ is the number of submodules of $M(b)$ isomorphic to $M(a)$.

Similarly, we see that α_a divides ε_a^b, and that $\eta_a^b = \alpha_a^{-1}\varepsilon_a^b$ counts the number of submodules of $M(b)$ with factor module isomorphic to $M(a)$.

With these preparations we are going to give the proof of the theorem. Of course, if $\mathbf{dim}\, M(b) \neq \mathbf{dim}\, M(a) + \mathbf{dim}\, M(c)$, let $\varphi_{ca}^b = 0$. Thus it remains to consider the case when $\mathbf{dim}\, M(b) = \mathbf{dim}\, M(a) + \mathbf{dim}\, M(c)$.

A map $a \in \mathscr{B}$ will be called *homogeneous* provided $a(x) \neq 0$ for at most one $x \in \Gamma_0$. We are going to define φ_{ca}^b by induction on $\mathbf{dim}\, M(c)$. For $\mathbf{dim}\, M(c) = 0$, thus $c = 0$, let $\varphi_{ca}^a = 1$, and $\varphi_{ca}^b = 0$ for $a \neq b$. Now assume $c \neq 0$.

First, consider the case where c is not homogenous. Choose x minimal in Γ_0 with $c(x) \neq 0$. Here, we consider Γ_0 as a partially ordered set, with $x \preccurlyeq y$ if and only if there is a path from x to y. Let $c', c'' \in \mathscr{B}$ be defined by $c'(x) = c(x)$, $c'(y) = 0$, for $y \neq x$, and $c'' = c - c'$. We define

$$\varphi_{ca}^b = \sum_d \varphi_{c'd}^b \varphi_{c''a}^d,$$

where the sum is taken over all $d \in \mathscr{B}$ such that $\mathbf{dim}\, M(d) = \mathbf{dim}\, M(c'') + \mathbf{dim}\, M(a)$; of course, this is a finite sum. Observe that the terms on the right are all already defined, since $M(c) = M(c') \oplus M(c'')$, with both $M(c')$, $M(c'')$ nonzero, thus $\mathbf{dim}\, M(c') < \mathbf{dim}\, M(c)$, and $\mathbf{dim}\, M(c'') < \mathbf{dim}\, M(c)$. Let us evaluate φ_{ca}^b at $|k|^r$:

$$\varphi_{ca}^b(|k|^r) = \sum_d \varphi_{c'd}^b(|k|^r)\varphi_{c''a}^d(|k|^r) = \sum_d F_{M(c')M(d)}^{M(b)} F_{M(c'')M(a)}^{M(d)}$$

$$= F_{M(c')M(c'')M(a)}^{M(b)} = \sum_e F_{M(c')M(c'')}^{M(e)} F_{M(e)M(a)}^{M(b)},$$

where e runs through all maps with $\mathbf{dim}\, M(e) = \mathbf{dim}\, M(c') + \mathbf{dim}\, M(c'')$. Note that $\operatorname{Ext}^1(M(c'), M(c'')) = 0$ by the choice of x, therefore $F_{M(c')M(c'')}^{M(e)} \neq 0$ only for $e = c' + c''$ $(= c)$, and $F_{M(c')M(c'')}^{M(c)} = 1$ since $\operatorname{Hom}(M(c''), M(c')) = 0$. It follows that there is only one nontrivial summand in $\sum_e$, and this summand is $F_{M(c)M(a)}^{M(b)}$.

Second, consider the case of c being homogeneous. Note that if also $d \in \mathscr{B}$ is homogeneous, and $\mathbf{dim}\, M(c) = \mathbf{dim}\, M(d)$, then $c = d$. For, let $x \neq y \in \Gamma_0$; then it is well known that $\mathbf{dim}\, M(x)$ and $\mathbf{dim}\, M(y)$ are not proportional. It follows that the polynomials φ_{da}^b with $d \neq c$ are already defined, and we define

$$\varphi_{ca}^b = \sigma_a^b - \sum_{d \neq c} \varphi_{da}^b.$$

Clearly, the right side evaluated at $|k|^r$ gives the number of submodules U of $M(b)$ which are isomorphic to $M(a)$ such that $M(b)/U$ is not isomorphic to any $M(d)$ with $d \neq c$. But this means that we count the number of submodules U of $M(b)$ isomorphic to $M(a)$ such that $M(b)/U$ is isomorphic to $M(c)$.

3. Hall polynomials evaluated at 1

By abuse of language, we denote the characteristic function for $x \in \Gamma_0$ just by x. Thus, we consider Γ_0 as a subset of $\mathscr{B}$ and the elements in $\mathscr{B} \setminus \Gamma_0$ will be said to be *decomposable*. As usual, δ_{ab} is the Kronecker symbol (with $\delta_{ab} = 1$ in case $a = b$, and $\delta_{ab} = 0$ otherwise).

THEOREM 2. *Let Γ be a directed Auslander–Reiten quiver. Let $x, y \in \Gamma_0$ and let $a \in \mathscr{B}$ be decomposable. Then $\varphi^a_{zx}(1) = \delta_{a,x+z}(1 + \delta_{xz})$. Consequently,*

$$\varphi^a_{zx}(1) = \varphi^a_{xz}(1).$$

Proof. Let us first observe that $(T-1)^n$ divides α_a if and only if $n \leqslant \sum_{y \in \Gamma_0} a(y)$. In particular, $(T-1)^2$ does not divide α_x.

We can assume $a \neq 0$, and we write $a = a_1 + a_2$ with nonzero functions a_i: $\Gamma_0 \to \mathbb{N}_0$. Let R be a k-algebra with $\Gamma_R = \Gamma$ and symmetrization index r. Let $\mathscr{M}_R$ be the set of R-module monomorphisms $f = [f_1, f_2]$: $M(x) \to M(a_1) \oplus M(a_2)$, where both f_i: $M(x) \to M(a_i)$ are nonzero and $\operatorname{Cok} f \cong M(z)$.

$$(1) \qquad |\mathscr{M}_R| = \alpha_x(|k|^r) \cdot \left(F^{M(R,a)}_{M(R,z)M(R,x)} - \delta_{a,x+z}(1 + \delta_{xz})\right).$$

For the proof of (1), let $\mathscr{M}'_R$ denote the set of R-module monomorphisms f: $M(x) \to M(a_1) \oplus M(a_2)$ with cokernel isomorphic to $M(z)$; thus, clearly

$$|\mathscr{M}'_R| = \alpha_x(|k|^r) \cdot F^{M(R,a)}_{M(R,z)M(R,x)}.$$

We have $\mathscr{M}_R \subseteq \mathscr{M}'_R$, so consider an element $f \in \mathscr{M}'_R \setminus \mathscr{M}_R$. Write $f = [f_1, f_2]$ with f_i: $M(x) \to M(a_i)$, thus $f_1 = 0$ or $f_2 = 0$. Assume $f_2 = 0$. Then $\operatorname{Cok} f \cong (\operatorname{Cok} f_1) \oplus M(a_2)$, but $\operatorname{Cok} f \cong M(z)$ is indecomposable, and $M(a_2) \neq 0$, thus $\operatorname{Cok} f_1 = 0$ and $M(a_2) \cong M(z)$. It follows that f_1 is an isomorphism, thus $x = a_1$, and $z = a_2$. Similarly, if $f_1 = 0$, then $x = a_2$, and $z = a_1$. In particular, if $a \neq x + z$, then $\mathscr{M}_R = \mathscr{M}'_R$, and we obtain (1).

Thus, consider now the case $a = x + z$, say $x = a_1$, $z = a_2$. If $x \neq z$, then $\mathscr{M}'_R \setminus \mathscr{M}_R$ is the set of maps $[f_1, 0]$, where f_1 is an automorphism of $M(x)$, thus $|\mathscr{M}'_R \setminus \mathscr{M}_R| = \alpha_x(|k|^r)$. If $x = z$, then any automorphism g of $M(x)$ gives rise to the two elements $[g, 0]$ and $[0, g]$ in $\mathscr{M}'_R \setminus \mathscr{M}_R$, thus $|\mathscr{M}'_R \setminus \mathscr{M}_R| = 2\alpha_x(|k|^r)$. This finishes the proof of (1).

$$(2) \qquad (|k|^r - 1)^2 \quad \text{divides} \quad |\mathscr{M}_R|.$$

Let K be the field with $|k|^r$ elements. Let $y \in \Gamma_0$. Since $r \leqslant \dim_k \operatorname{End} M(y)$, and $\operatorname{End} M(y)$ is a field, we see that K embeds into $\operatorname{End} M(y)$. Consequently, we can embed K into $\operatorname{End} M(a_i)$, for $i = 1, 2$. Let $K^* = K \setminus \{0\}$. We claim that $K^* \times K^*$ operates on $\mathscr{M}_R$ from the right, via $[f_1, f_2] \cdot [g_1, g_2] = [f_1 g_1, f_2 g_2]$, where f_i: $M(x) \to M(a_i)$, and $g_i \in K \subseteq \operatorname{End} M(a_i)$. Of course $f_i \neq 0$ implies $g_i \neq 0$, thus we only have to verify that $[f_1 g_1, f_2 g_2]$ is a monomorphism with cokernel isomorphic to $M(z)$. But this is clear due to the following commutative diagram:

$$\begin{array}{ccccccccc} 0 \to & M(x) & \xrightarrow{A} & M(a_1)\oplus M(a_2) & \xrightarrow{C} & M(z) & \to 0 \\ & \| & & \downarrow E & & \| & \\ 0 \to & M(x) & \xrightarrow{B} & M(a_1)\oplus M(a_2) & \xrightarrow{D} & M(z) & \to 0 \end{array}$$

where

$$A = [f_1, f_2], \quad B = [f_1 g_1, f_2 g_2],$$

$$C = \begin{bmatrix} h_1 \\ h_2 \end{bmatrix}, \quad D = \begin{bmatrix} g_1^{-1} h_1 \\ g_2^{-1} h_2 \end{bmatrix}, \quad E = \begin{bmatrix} g_1 & 0 \\ 0 & g_2 \end{bmatrix}.$$

This is a free operation: Namely, assume $f_1 = f_1 g_1$ with $f_1 \neq 0$ and $g_1 \in K^*$. Then $f_1(1-g_1) = 0$. But for $g_1 \neq 1$ also $1-g_1$ belongs to K^*, and therefore is invertible, thus $f_1 = 0$, a contradiction. Similarly, $f_2 = f_2 g_2$ with $f_2 \neq 0$ and $g_2 \in K^*$ implies $g_2 = 1$. It follows that all orbits of the operation of $K^* \times K^*$ on $\mathcal{M}_R$ consist of $(|k|^r - 1)^2$ elements; this completes the proof of (2).

(3) $\qquad (T-1)^2$ divides $\alpha_x(\varphi^a_{zx} - \delta_{a,x+z}(1+\delta_{xz}))$.

According to the general lemma in the previous section, this is an immediate consequence of (1) and (2), using various k-algebras R with $\Gamma_R = \Gamma$.

Since $(T-1)^2$ does not divide α_x, it follows that $T-1$ divides $\varphi^a_{zx} - \delta_{a,x+z}(1+\delta_{xz})$. This means that the evaluation of φ^a_{zx} at 1 yields $\delta_{a,x+z}(1+\delta_{xz})$, and therefore $\varphi^a_{zx}(1) = \varphi^a_{xz}(1)$.

We recall the following: given a directed quiver, we denote by $\preccurlyeq$ the partial ordering of its vertices: we have $x \preccurlyeq y$ if and only if there exists a path from x to y.

THEOREM 3. *Let Γ be a directed Auslander–Reiten quiver. Let $a \in \mathscr{B}$. Let $z \in \Gamma_0$ and assume $a(y) = 0$ for all $y \prec z$. Then $\varphi^b_{za} = 0$ for all $b \neq a+z$. Also, $\varphi^{a+z}_{za}(1) = a(z)+1$, therefore $\varphi^a_{a(z)z,a-a(z)z} = a(z)!$.*

Proof. Let R be a k-algebra with $\Gamma_R = \Gamma$ and symmetrization index r. Since $\mathrm{Ext}^1_R(M(z), M(a)) = 0$, we see that $F^{M(b)}_{M(z)M(a)} \neq 0$ only for $b = a+z$, and that $F^{M(a+z)}_{M(z)M(a)}$ is the number of direct summands of $M(a+z)$ which are isomorphic to $M(a)$. Write $M(a+z) = M' \oplus (a(z)+1)M(z)$, with $M' = M(a-a(z)z)$. Any epimorphism $f\colon M(a+z) \to M(z)$ vanishes on M', since $a(y) = 0$ for $y \prec z$, thus the kernel of f is a direct summand of $M(a+z)$ and isomorphic to $M(a)$. It follows that

$$\varphi^{a+z}_{za} = \eta^{a+z}_z = \alpha_z^{-1}\varepsilon^{a+z}_z = \alpha_z^{-1}(\gamma^{a(z)+1}_{zz} - 1) = \sum_{i=1}^{a(z)} \gamma^i_{zz},$$

where we use the notations from the proof of Theorem 1. In particular, $\gamma_{zz}(1) = 1$ implies that $\varphi^{a+z}_{za}(1) = a(z)+1$. By induction, we conclude that $\varphi^a_{a(z)z,a-a(z)z}(1) = a(z)!$. This completes the proof.

4. The generic Hall algebra and its degeneration

Let R be a representation-directed algebra with Auslander–Reiten quiver $\Gamma = \Gamma_R$. The existence of the Hall polynomials allows us to define a generic Hall algebra $\mathscr{H}(R, \mathbf{Z}[T])$ as follows. Let $\mathscr{H}(R, \mathbf{Z}[T])$ be the free $\mathbf{Z}[T]$-module with basis $(u_a)_{a\in\mathscr{A}}$, and we define a multiplication

$$u_c u_a = \sum_b \varphi_{ca}^b u_b;$$

the sum on the right is finite, since $\varphi_{ca}^b = 0$ unless $\mathbf{dim}\, M(b) \neq \mathbf{dim}\, M(a) + \mathbf{dim}\, M(c)$, and there are only finitely many b with a given $\mathbf{dim}\, M(b)$.

PROPOSITION 4. *$\mathscr{H}(R, \mathbf{Z}[T])$ is an associative ring with* 1; *it only depends on the valued translation quiver Γ_R.*

Proof. The index set of our free $\mathbf{Z}[T]$-basis as well as the multiplication constants φ_{ca}^b only depend on Γ, thus $\mathscr{H}(R, \mathbf{Z}[T])$ only depends on Γ. For the associativity, we have to see that

$$\sum_v \varphi_{cb}^v \varphi_{va}^w = \sum_u \varphi_{cu}^w \varphi_{ba}^u \quad \text{for all } a, b, c, u, v, w;$$

this follows from the corresponding equalities which we obtain as evaluations at numbers of the form $|k|^s$, where S is a k-algebra with $\Gamma_S = \Gamma$ and symmetrization index s. The element u_0 is the identity of $\mathscr{H}(R, \mathbf{Z}[T])$, since $\varphi_{0a}^a = 1 = \varphi_{a0}^a$.

The ring $\mathscr{H}(R, \mathbf{Z}[T])$ will be called the *generic* Hall algebra for R, or for Γ_R.

Finally, we will consider the degeneration which we obtain from $\mathscr{H}(R, \mathbf{Z}[T])$ by specializing T to 1. Thus, we consider the free $\mathbf{Z}$-module $\mathscr{H}(R)_1$ with basis $(u_a)_{a\in\mathscr{A}}$ with multiplication

$$u_c u_a = \sum_b \varphi_{ca}^b(1) u_b.$$

The free $\mathbf{Z}$-module with basis $(u_x)_{x\in\Gamma_0}$ will be denoted by $K(R\text{-mod})$. By our convention, $K(R\text{-mod})$ is a subgroup of $\mathscr{H}(R)_1$.

PROPOSITION 5. *$\mathscr{H}(R)_1$ is an associative ring with* 1; *it only depends on Γ_R. The subgroup $K(R\text{-mod})$ is a Lie subalgebra of $\mathscr{H}(R)_1$, and $\mathscr{H}(R)_1 \otimes_{\mathbf{Z}} \mathbf{Q}$ is the universal enveloping algebra of $K(R\text{-mod}) \otimes_{\mathbf{Z}} \mathbf{Q}$.*

Proof. Since $\mathscr{H}(R)_1$ is obtained from $\mathscr{H}(R, \mathbf{Z}[T])$ by factoring out the ideal generated by $(T-1)u_0$, the first assertion is immediate. According to Theorem 2, the subgroup $K(R\text{-mod})$ is closed under the Lie product of $\mathscr{H}(R)_1$, thus it is a Lie subalgebra. The last assertion will follow from the next proposition and the theorem of Poincaré–Birkhoff–Witt.

PROPOSITION 6. *Let $x_1, \ldots, x_n$ be the vertices of Γ, ordered in such a way that $x_i \preccurlyeq x_j$ implies $i \leqslant j$. Let $a \in \mathscr{B}$. Then, in $\mathscr{H}(R)_1 \otimes \mathbf{Q}$, we have*

$$u_a = \frac{u_{x_1}^{a(x_1)}}{a(x_1)!} \cdots \frac{u_{x_n}^{a(x_n)}}{a(x_n)!}.$$

Proof. We have to show that

$$u_{x_1}^{a(x_1)} \ldots u_{x_n}^{a(x_n)} = a(x_1)! \ldots a(x_n)!\, u_a$$

in $\mathscr{H}(R)_1$. We use induction on i, where $a(x_{n-j}) = 0$ for all $j \leqslant i$. If $i = 0$, then $a = 0$, and we deal with the identity element. If $1 \leqslant i \leqslant n$, and $a(x_{n-j}) = 0$ for all $j \leqslant i$, let $b = a - a(x_{n-i})x_{n-i}$. Then

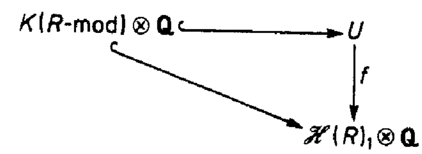
$$\begin{aligned} u_{x_1}^{a(x_1)} \ldots u_{x_n}^{a(x_n)} &= u_{x_{n-i}}^{a(x_{n-i})} u_{x_{n-i+1}}^{a(x_{n-i+1})} \ldots u_{x_n}^{a(x_n)} \\ &= u_{x_{n-i}}^{a(x_{n-i})} u_{x_1}^{b(x_1)} \ldots u_{x_n}^{b(x_n)} \\ &= b(x_1)! \ldots b(x_n)!\, u_{x_{n-i}}^{a(x_{n-i})} u_b \\ &= a(x_{n-i+1})! \ldots a(x_n)!\, u_{x_{n-i}}^{a(x_{n-i})} u_b. \end{aligned}$$

We apply Theorem 3 for $z = x_{n-i}$. Since $\varphi_{a(z)z,b}^{c} = 0$ for $c \neq b + a(z)z$, the product $u_z^{a(z)} u_b$ is a multiple of $u_{b+a(z)z} = u_a$, and the coefficient is $\varphi_{a(z)z,b}^{b+a(z)z} = a(z)!$. Thus we see that

$$u_{x_{n-i}}^{a(x_{n-i})} u_b = a(x_{n-i})!\, u_a.$$

This finishes the proof.

We return to the proof of Proposition 5. Since $\mathscr{H}(R)_1 \otimes \mathbf{Q}$ is an associative algebra with Lie subalgebra $K(R\text{-mod}) \otimes \mathbf{Q}$, there is a unique ring homomorphism f from the universal enveloping algebra U of $K(R\text{-mod}) \otimes \mathbf{Q}$ to $\mathscr{H}(R)_1 \otimes \mathbf{Q}$ such that the diagram



commutes. According to Proposition 6, the elements u_a are in the image of f, thus f is surjective. Also, the images under f of the PBW-basis of U (formed with respect to the ordering $u_{x_1}, \ldots, u_{x_n}$) are linearly independent over $\mathbf{Q}$, thus f is injective. This completes the proof of Proposition 5.

Remark. The reader will observe the similarity of our description of the elements u_a in Proposition 6 with some of the defining elements of the Kostant $\mathbf{Z}$-form of the universal enveloping algebra of a semisimple complex Lie algebra $\mathbf{g}$. In fact, let $\mathbf{h}$ be a Cartan subalgebra of $\mathbf{g}$, and $\mathbf{g} = \mathbf{n}_- \oplus \mathbf{h} \oplus \mathbf{n}_+$ the corresponding triangular decomposition. Let R be a finite-dimensional hereditary algebra of the same type as **g**. We will show in [R2] that the Lie algebra $K(R\text{-mod})$ can be identified with the Chevalley **Z**-form of $\mathbf{n}_+$ and that in this way $\mathscr{H}(R)_1$ becomes the Kostant **Z**-form of $U(\mathbf{n}_+)$.

References

[D] V. G. Drinfeld, *Quantum groups*, in: Proc. Internat. Congress Math. Berkeley 1986, Amer. Math. Soc., 1987, 798–820.

[DR] V. Dlab and C. M. Ringel, *On algebras of finite representation type*, J. Algebra 33 (1975), 306–394.

[Ga] P. Gabriel, *Unzerlegbare Darstellungen I*, Manuscripta Math. 6 (1972), 71–103.

[Gr] A. Grothendieck, *Groupes de classes des catégories abéliennes et triangulés. Complexes parfaits*, in: SGA 5, Lecture Notes in Math. 589, Springer, 1977, 351–371.

[H] P. Hall, *The algebra of partitions*, in: Proc. 4th Canad. Math. Congress, Banff 1957, Univ. of Toronto Press, 1959, 147–159.

[Hu] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Math. 9, Springer, 1972.

[HPR] D. Happel, U. Preiser and C. M. Ringel, *Vinberg's characterization of Dynkin diagrams using subadditive functions with application to D*Tr*-periodic modules*, in: Lecture Notes in Math. 832, Springer, 1980, 280–294.

[K] B. Kostant, *Groups over* **Z**, in: Algebraic Groups and Discontinuous Subgroups, Proc. Sympos. Pure Math. 9, Amer. Math. Soc., 1966, 90–98.

[M] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, 1979.

[R1] C. M. Ringel, *Tame Algebras and Integral Quadratic Forms*, Lecture Notes in Math. 1099, Springer, 1984.

[R2] —, *Hall polynomials for the representation-finite hereditary algebras*, Adv. in Math., to appear.

[R3] —, *Hall algebras and quantum groups*, Invent. Math., to appear.

[R4] —, *From representations of quivers via Hall and Loewy algebras to quantum groups*, in: Proc. Novosibirsk Algebra Conf. 1989, to appear.

[S] E. Steinitz, *Zur Theorie der Abel'schen Gruppen*, Jahresber. Deutsch. Math.-Verein. 9 (1901), 80–85.