H. H. ANDERSEN
J. C. JANTZEN
WOLFGANG SOERGEL

Representations of quantum groups at A p-th root of unity and of semisimple groups in characteristic p : independence of p

Astérisque, tome 220 (1994)
<http://www.numdam.org/item?id=AST_1994__220__1_0>

220 ASTÉRISQUE

1994

REPRESENTATIONS OF QUANTUM GROUPS AT A p-TH ROOT OF UNITY AND OF SEMISIMPLE GROUPS IN CHARACTERISTIC p: INDEPENDENCE OF p

H.H. ANDERSEN, J.C. JANTZEN, W. SOERGEL

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

A.M.S. Subjects Classification (1994) :

20G05, 17B35, 17B37

Table of Contents

Introduction

Let R be a finite root system with Weyl group W. For any prime p and any algebraically closed field k of characteristic p consider the connected, simply connected semisimple algebraic group G_k over k with root system R. Denote the Lie algebra of G_k by $\mathfrak{g}_k$. This is a p-Lie algebra, i.e., it has an additional structure, the p-th power map $X \mapsto X^{[p]}$. In this case it is the ordinary p-th power, if we think of elements of $\mathfrak{g}_k$ as derivations. We shall consider representations of $\mathfrak{g}_k$ as a p–Lie algebra. This means that the action of any $X^{[p]}$ on the module is the p-th power of the action of X. The corresponding module is then called a restricted $\mathfrak{g}_k$–module. It is a module for the restricted enveloping algebra $U^{[p]}(\mathfrak{g}_k)$, which is the quotient of the universal enveloping algebra of $\mathfrak{g}_k$ by the ideal generated by all $X^p - X^{[p]}$ with $X \in \mathfrak{g}_k$. The algebra $U^{[p]}(\mathfrak{g}_k)$ has finite dimension equal to p^m where $m = \dim \mathfrak{g}_k$.

The representation theory of the $U^{[p]}(\mathfrak{g}_k)$ turns out to have many features that are (conjecturally) independent of p. Let us mention first the one most easily described. Since $U^{[p]}(\mathfrak{g}_k)$ has finite dimension, it is the direct product of indecomposable algebras, the blocks of $U^{[p]}(\mathfrak{g}_k)$. Each indecomposable restricted $\mathfrak{g}_k$–module M belongs to exactly one of these blocks; it is the unique block not annihilating M. Denote by $\mathcal{B}_k$ the block of the trivial one dimensional $\mathfrak{g}_k$–module. Work ([Hu2]) by Humphreys from 1971 showed: If p is greater than the Coxeter number h of R, then the simple modules belonging to $\mathcal{B}_k$ are indexed by the Weyl group W. The Cartan matrix of $\mathcal{B}_k$ is therefore a $(W \times W)$–matrix. In the cases known at that time (and in the cases known today) this matrix is independent of p (as long as $p > h$). So one might conjecture that this independence should hold in general. (This conjecture is implicitly contained in Verma's last conjecture in [Ver] to be discussed below.) We shall prove:

Theorem 1: *There is a $\mathbf{Z}$–algebra $\mathcal{B}$ (finitely generated as a $\mathbf{Z}$–module) such that for all k with* $\mathrm{char}(k) > h$ *the block $\mathcal{B}_k$ is Morita equivalent to $\mathcal{B} \otimes_{\mathbf{Z}} k$.*

(More precisely, we construct a $\mathcal{B}$ such that $\mathcal{B} \otimes_{\mathbf{Z}} \mathbf{Z}[((h-1)!)^{-1}]$ is free of finite rank over $\mathbf{Z}[((h-1)!)^{-1}]$.) The theorem implies that for $p \gg 0$ the Cartan matrix above is indeed independent of p. Our methods do not yield reasonable bounds. These bounds arise from conditions that certain algebraic numbers should not have p in their denominators.

The algebra $\mathcal{B}$ has also an interpretation in characteristic 0. Take an odd integer $p > 1$ (prime to 3 if R has a G_2 component) and consider the quantized enveloping algebra U_p at a p–th root of unity. Here we take Lusztig's version constructed via divided powers. It contains a finite dimensional analogue $\mathbf{u}_p$ of the restricted enveloping algebra. (This was discovered by Lusztig, cf. [Lu6] and [Lu7].) Then:

Theorem 2: *If $p > h$, then $\mathcal{B} \otimes_{\mathbf{Z}} \mathbf{Q}(\sqrt[p]{1})$ is Morita equivalent to the block of $\mathbf{u}_p$ containing the trivial one dimensional module.*

Let us return to the characteristic $p > 0$ situation. One of the main tools of Humphreys in [Hu2] was the use of the analogues of the Verma modules: Consider the Lie algebra $\mathfrak{b}_k$ of a Borel subgroup of G_k, take a one dimensional $U^{[p]}(\mathfrak{b}_k)$–module and induce to $U^{[p]}(\mathfrak{g}_k)$. Suppose that $p > h$. Then there are $|W|$ induced modules $(Z_w)_{w \in W}$ of this type belonging to $\mathcal{B}_k$. Each Z_w has a unique simple homomorphic image L_w; the L_w with $w \in W$ are exactly the simple modules belonging to $\mathcal{B}_k$ mentioned above. One of the main results in [Hu2] is the following: The projective cover Q_w of L_w has a filtration with factors of the form $Z_{w'}$ with $w' \in W$; any $Z_{w'}$ occurs exactly $d_k(w', w)$ times where $d_k(w', w)$ is the multiplicity of the simple module L_w as a composition factor of $Z_{w'}$. This implies especially that the Cartan matrix of $\mathcal{B}_k$ is determined by the decomposition matrix, i.e., the matrix of all $d_k(w', w)$, and we can now replace the previous conjecture on the Cartan matrix by one on the decomposition matrix (for $p > h$). And that is indeed part of Verma's Conjecture V in [Ver]. We can show:

Theorem 3: *Let $w, w' \in W$. There is an integer $d(w', w) \geq 0$ such that $d_k(w', w) = d(w', w)$ for all k with $char(k) \gg 0$.*

Again, there is an interpretation in characteristic 0. The $\mathbf{u}_p$ have analogous modules Z_w and L_w, and then $d(w', w)$ is equal to the multiplicity of L_w in $Z_{w'}$ whenever $p > h$.

The remaining part of Verma's Conjecture V is concerned with multiplicities for the algebraic group G_k. (Both parts are in fact closely related, since Verma's (proven) Conjecture IV tells us how to express the $d(w', w)$ in terms of multiplicities for G_k.) At this point we need more notations. Let X be the group of weights of the root system R. Let W_a be the affine Weyl group of R, i.e., the semidirect product of W and the group of translations by elements in $\mathbf{Z}R$. Set ρ equal to the sum of the fundamental weights.

Let T_k be a maximal torus in G_k and set $\mathfrak{h}_k$ equal to the Lie algebra of T_k. We assume that T_k is contained in the Borel subgroup with Lie algebra $\mathfrak{b}_k$ so that $\mathfrak{h}_k \subset \mathfrak{b}_k$. We identify the group of characters of T_k with X. To each dominant weight $\lambda \in X$ there correspond a simple module and a Weyl module with highest weight λ. Denote by $b_k(\mu, \lambda)$ the multiplicity of the simple module with highest weight λ as a composition factor of the Weyl module with highest weight μ. The linkage principle (first conjectured by Verma) states that $b_k(\mu, \lambda) \neq 0$ implies $\lambda \in W_a \bullet \mu$ where any $w \in W$ acts via

$w{\bullet}\mu = w(\mu+\rho)-\rho$ and any translation by some $\nu \in \mathbf{Z}R$ as translation by $p\nu$. (Perhaps we should write $w{\bullet_p}\lambda$ for $w \in W_a$ and $\lambda \in X$ to denote this action. But it should always be clear what we mean.) The linkage principle together with the translation principle implies that we know (for $p \geq h$) all $b_k(\mu,\lambda)$ if we know all $b_k(w',w) = b_k(w'{\bullet}0, w{\bullet}0)$ with $w, w' \in W_a$ such that $w{\bullet}0$ and $w'{\bullet}0$ are dominant.

The second part of Verma's Conjecture V says that the $b_k(w',w)$ should be independent of k for all $w, w' \in W_a$ with $w{\bullet}0$ and $w'{\bullet}0$ dominant. (This condition is independent of k if $p \geq h$.) Steinberg's tensor product theorem shows easily that this conjecture will not work if $w'{\bullet}0$ is "large" with respect to p^2. So one should modify the conjecture and impose an upper bound on w'. In [Lu1] Lusztig has made a conjecture on the $b_k(w',w)$ (or rather for the inverse matrix) that would imply Verma's (modified) Conjecture V. Set W_a^+ equal to the set of all $w \in W_a$ with $w{\bullet}0$ dominant whenever $p \geq h$. Our results imply:

Theorem 4: *For all $w, w' \in W_a^+$ there is an integer $b(w',w)$ such that $b(w',w) = b_k(w',w)$ for all k with $char(k) \gg 0$.*

In characteristic 0 consider an odd integer p and the algebra U_p as above. We have simple modules and Weyl modules for U_p indexed by the dominant weights, and we have analogous multiplicities $b_p(\mu,\lambda)$. There is again a linkage principle involving the action of W_a where again the translation by a weight $\nu \in \mathbf{Z}R$ acts as translation by $p\nu$. We get now:

Theorem 5: *If $p \geq h$, then $b(w',w) = b_p(w'{\bullet}0, w{\bullet}0)$ for all $w, w' \in W_a^+$.*

These two results imply that one gets for $\mathrm{char}(k) = p \gg 0$ each irreducible G_k–module with "restricted" highest weight by reduction modulo p from a simple U_p–module as conjectured by Lusztig. It also implies that his conjecture in [Lu1] follows for $\mathrm{char}(k) \gg 0$ from its quantum analogue in [Lu4], 8.2.

Kazhdan and Lusztig have recently shown that there is an equivalence of categories between certain U_p–modules and certain representations of affine Kac–Moody Lie algebras. This result was announced in [KL1], proved in the simply laced case in [KL2] – [KL5], and in general in [Lu11]. (Recall that our p is always prime to the entries in the Cartan matrix.) This equivalence implies that Lusztig's conjecture in the quantum case is equivalent to a similar conjecture in the Kac–Moody case. In the latter case Kashiwara and Tanisaki have recently announced ([KT]) a proof of the conjecture; an earlier manuscript by Casian ([Cas]) has not convinced all of its readers.

In order to get our results we work mainly not in the categories of restricted $\mathfrak{g}_k$–modules or of G_k–modules (or their analogues in characteristic 0), but in the category of $\mathfrak{g}_k$-T_k–modules and a characteristic 0 analogue. A $\mathfrak{g}_k$-T_k–module is a restricted $\mathfrak{g}_k$–module M that is also a T_k–module such that (obvious) compatibility conditions hold. Giving a representation of T_k on M is the same as giving a grading $M = \bigoplus_{\nu \in X} M_\nu$ of M by X. The compatibility conditions say that every root vector E_α in $\mathfrak{g}_k$ maps each M_ν to $M_{\nu+\alpha}$ and that every $H \in \mathfrak{h}_k$ acts on each M_ν as multiplication by $\nu(H)$. (We write

$\nu(H)$ by abuse of notation. We really mean the differential of $\nu : T_k \to k$ on the Lie algebra $\mathfrak{h}_k$ of T_k.) Note that $\mathfrak{g}_k$-T_k–modules were called $\mathbf{u}_1$–T-modules in [Ja3] and that they are usually called $(G_k)_1T_k$–modules nowadays.

One can define $\mathfrak{b}_k$-T_k–modules similarly. One associates to each $\lambda \in X$ a one dimensional $\mathfrak{b}_k$-T_k–module, then an induced $\mathfrak{g}_k$-T_k–module $Z_k(\lambda)$. It has a simple head $L_k(\lambda)$. Denote the multiplicity of $L_k(\lambda)$ as a composition factor of $Z_k(\mu)$ by $d'_k(\mu, \lambda)$. If $\operatorname{char}(k) \geq h$, then all these multiplicities are known as soon as we know all $d'_k(w', w) = d'_k(w'{\bullet}0, w{\bullet}0)$ with $w, w' \in W_a$.

Theorem 6: *For all $w, w' \in W_a$ there is an integer $d'(w', w)$ such that $d'(w', w) = d'_k(w', w)$ for all k with $\operatorname{char}(k) \gg 0$.*

The $d'(w', w)$ have again an interpretation in characteristic 0. One defines a suitable category of $\mathbf{u}_p$–modules with an X–grading satisfying similar compatibility conditions. Then the $d'(w', w)$ are the corresponding multiplicities in this category whenever $p \geq h$.

* * *

We want to give an idea of how these results are reached. For the sake of simplicity let us concentrate on the prime characteristic case and just say that there are analogous results or constructions in the quantum case. Let us also assume that $\operatorname{char}(k) = p \geq h$.

In the category of $\mathfrak{g}_k$-T_k–modules each simple module $L_k(\lambda)$ has a projective cover $Q_k(\lambda)$. It has a filtration with factors of the form $Z_k(\mu)$ and each $Z_k(\mu)$ occurs exactly $d'_k(\mu, \lambda)$ times. One can therefore translate Theorem 6 into a statement about the characters of the $Q_k(w{\bullet}0)$. In one case this character is well understood: Take the unique element $w_0 \in W$ that maps all positive roots into negative roots. One knows that $Q_k = Q_k(w_0{\bullet}0)$ has a filtration with factors $Z_k(w{\bullet}0)$, $w \in W$ each w occurring once. We have now for our category the so–called wall crossing functors. If we apply a sequence I of these wall crossing functors to Q_k, we get a projective module $Q_{k,I}$. If one knows for all I and $w \in W_a$ the multiplicity of $Q_k(w{\bullet}0)$ as a direct summand of $Q_{k,I}$, then one knows all $d'_k(w', w'')$. In fact, one can find a finite family $\mathfrak{J}$ of these sequences such that the decomposition of the $Q_{k,I}$ with $I \in \mathfrak{J}$ alone determines all multiplicities.

Theorem 7: *There is an algebra $\mathcal{E}$ over $\mathbf{Z}$ (finitely generated as a $\mathbf{Z}$–module) such that $\mathcal{E} \otimes_{\mathbf{Z}} k$ is isomorphic to the endomorphism ring of the $\mathfrak{g}_k$-T_k–module $\bigoplus_{I \in \mathfrak{J}} Q_{k,I}$ for all k. Moreover, we have a decomposition $\mathcal{E} = \bigoplus_{I,J \in \mathfrak{J}} \mathcal{E}_{I,J}$ such that the isomorphism takes each $\mathcal{E}_{I,J} \otimes_{\mathbf{Z}} k$ to $\operatorname{Hom}_{\mathfrak{g}_k, T_k}(Q_{k,I}, Q_{k,J})$.*

This theorem (together with some alcove geometry and elementary facts on idempotents) yields Theorem 6. From that Theorems 3 and 4 follow by known results. Considered as a $U^{[p]}(\mathfrak{g}_k)$–module $\bigoplus_{I \in \mathfrak{J}} Q_{k,I}$ is a projective generator for the block $\mathcal{B}_k$. A small modification of the construction of $\mathcal{E}$ from Theorem 7 yields an algebra $\mathcal{B}$ over $\mathbf{Z}$ such that $\mathcal{B} \otimes_{\mathbf{Z}} k$ is (for $\operatorname{char}(k) \gg 0$) isomorphic to the algebra of all endomorphisms of $\bigoplus_{I \in \mathfrak{J}} Q_{k,I}$ as a $\mathfrak{g}_k$–module. Then $\mathcal{B}$ satisfies the claim of Theorem 1.

These indications should convince you that Theorem 7 and its quantum analogue are really the crucial results. So we should now answer the question: How does one get a characteristic free approach to these endomorphism algebras? Well, one essential step is not to work just with these $\mathfrak{g}_k$-T_k–modules, but also to lift them to suitable local rings. This approach was inspired by the success of a similar method in [So2] and [So3].

For each commutative algebra A over the symmetric algebra $S(\mathfrak{h}_k)$ we define a category $\mathcal{C}_A$ generalizing the $\mathfrak{g}_k$-T_k–modules. An object in $\mathcal{C}_A$ is an A–module M with a structure as a $\mathfrak{g}_k$–module and with a grading $M = \bigoplus_{\nu \in X} M_\nu$ by X. Furthermore every root vector $E_\alpha \in \mathfrak{g}_k$ maps each M_ν to $M_{\nu+\alpha}$ and E_α^p annihilates M. Finally, every $H \in \mathfrak{h}_k$ acts on each M_ν as multiplication by $H + \nu(H)$, or rather by its image under the structural map $S(\mathfrak{h}_k) \to A$. If we take $A = k$ with the augmentation map $S(\mathfrak{h}_k) \to k$ where $H \mapsto 0$ for all $H \in \mathfrak{h}_k$, then $\mathcal{C}_k$ is just the category of all $\mathfrak{g}_k$-T_k–modules. (In our "real" definition in 2.3 we add a finiteness condition and assume additionally that A is Noetherian.)

The first seven sections of this paper contain the basic theory of the category $\mathcal{C}_A$ and its quantum analogue. We discuss topics such as induction, projective modules, Ext groups, base change, filtrations, the linkage principle, blocks, translation functors. All of this is quite parallel to the corresponding theories for algebraic groups (cf. [Ja6]) and quantum groups (cf. [APW1]). It should be noted that many of the special aspects of this type of theory over a ring were first dealt with in [GJ]. In the case where A is a field, we reprove some results from [VK], [FP1], [DCK1] and [DCK2].

The algebra $S(\mathfrak{h}_k)$ is a polynomial ring over k with generators H_α, α a simple root. Take for A especially the local ring at the maximal ideal generated by all H_α. (We should denote this algebra by A_k, but write A to avoid double indices.) It turns out that we can lift the $Q_{k,I}$ to projective objects $Q_{A,I}$ in $\mathcal{C}_A$ and that the homomorphisms behave well under base change:

$$\mathrm{Hom}_{\mathcal{C}_A}(Q_{A,I}, Q_{A,J}) \otimes_A k \simeq \mathrm{Hom}_{\mathcal{C}_k}(Q_{k,I}, Q_{k,J}).$$

There is a Lie algebra $\mathfrak{g}_{\mathbf{Z}}$ over $\mathbf{Z}$ with $\mathfrak{g}_{\mathbf{Z}} \otimes_{\mathbf{Z}} k \simeq \mathfrak{g}_k$ for all k. We can find a Cartan subalgebra $\mathfrak{h}_{\mathbf{Z}}$ of $\mathfrak{g}_{\mathbf{Z}}$ with $\mathfrak{h}_{\mathbf{Z}} \otimes_{\mathbf{Z}} k \simeq \mathfrak{h}_k$ for all k. Set $S = S(\mathfrak{h}_{\mathbf{Z}})$ equal to the symmetric algebra of $\mathfrak{h}_{\mathbf{Z}}$ over $\mathbf{Z}$. Then $S \otimes_{\mathbf{Z}} k \simeq S(\mathfrak{h}_k)$ for all k, and we can regard A as an S–algebra. Now Theorem 7 is an easy consequence of:

Theorem 7′: *There is an algebra $\widehat{\mathcal{E}}$ over S that is finitely generated as an S–module such that $\widehat{\mathcal{E}} \otimes_S A$ is isomorphic to the endomorphism ring of $\bigoplus_{I \in \mathfrak{J}} Q_{A,I}$ for all k. (Here $A = A_k$.) Moreover, we have a decomposition $\widehat{\mathcal{E}} = \bigoplus_{I,J \in \mathfrak{J}} \widehat{\mathcal{E}}_{I,J}$ such that the isomorphism takes each $\widehat{\mathcal{E}}_{I,J} \otimes_S A$ to $\mathrm{Hom}_{\mathcal{C}_A}(Q_{A,I}, Q_{A,J})$.*

Well, this just replaces the previous question by a modified one: How does one get a characteristic free approach to the homomorphisms of the