The Hall algebra of the category of coherent sheaves on the projective line

Pierre Baumann and Christian Kassel

Abstract

To an abelian category $\mathcal{A}$ of homological dimension one satisfying certain finiteness conditions, one can associate an algebra, called the Hall algebra. Kapranov studied this algebra when $\mathcal{A}$ is the category of coherent sheaves over a smooth projective curve defined over a finite field, and observed analogies with quantum affine algebras. We recover here in an elementary way his results in the case when the curve is the projective line.

Résumé

A toute catégorie abélienne $\mathcal{A}$ de dimension homologique égale à un vérifiant certaines conditions de finitude, on peut associer une algèbre appelée l'algèbre de Hall. Kapranov a étudié cette algèbre lorsque $\mathcal{A}$ est la catégorie des faisceaux cohérents sur une courbe projective lisse définie sur un corps fini et a observé des analogies entre l'algèbre de Hall et les algèbres affines quantiques. Nous redémontrons de manière élémentaire ses résultats dans le cas où la courbe est la droite projective.

Introduction

The combinatorial lattice structure of objects in an abelian category $\mathcal{A}$ of homological dimension one satisfying certain finiteness conditions may be encoded in an algebraic structure, called the Hall algebra of $\mathcal{A}$. Hall's original results, as described in Chapters II and III of Macdonald's book [14], concern the category of modules of finite length over a discrete valuation ring with finite residue field.

A decade ago Ringel studied the Hall algebra of the category of finite-dimensional representations over a finite field $\mathbf{F}_q$ of a quiver whose underlying graph Γ is a Dynkin diagram of type A, D, or E. He showed that a suitable modification of this Hall algebra yields an algebra isomorphic to the "positive part" of Drinfeld and Jimbo's quantized enveloping algebra associated to Γ and specialized at the value q of the parameter (see [9] or Section 2 of [17] for an introduction to Ringel's results).

More recently, Kapranov investigated the case when $\mathcal{A}$ is the category of coherent sheaves over a smooth projective curve X defined over $\mathbf{F}_q$. In a remarkable paper [13], he used

1991 Mathematics Subject Classification: Primary 16S99; Secondary 14H60, 16E60, 17B37, 81R50.
Keywords: Hall algebra, vector bundle on a curve, quantum affine algebra.

unramified automorphic forms, Eisenstein series, and L-functions to carry the geometrical properties of X into the algebraic structure of the Hall algebra of $\mathcal{A}$. This allowed him to observe some striking similarities between such a Hall algebra and Drinfeld's loop realization of the quantum affine algebras [7]. In the case when X is the projective line $\mathbf{P}^1(\mathbf{F}_q)$, Kapranov deduced from his general constructions an isomorphism between a certain subalgebra of the Hall algebra and a certain "positive part" of the (untwisted) quantum affine algebra $U_q(\widehat{\mathfrak{sl}_2})$.

The main objective of this article is to recover Kapranov's isomorphism for the projective line in a more elementary way. Avoiding any use of adelic theory or of automorphic forms, we compute directly the structure constants of the Hall algebra of the category of coherent sheaves over $\mathbf{P}^1(\mathbf{F}_q)$. As is well known (see the references given in Remark 5.2.7 of [13]), this category has the same derived category as the category of modules over a tame hereditary algebra; this may be the reason why our computations are feasible. Our approach moves us away from the analogy that motivated Kapranov, but hopefully makes his results more accessible and concrete. We also observe that Kapranov's isomorphism yields a natural definition for the vectors of the Poincaré-Birkhoff-Witt basis of $U_q(\widehat{\mathfrak{sl}_2})$ that Beck, Chari, and Pressley introduced in [2].

The paper is organized as follows. In Section 1 we give the definitions of the Hall algebra and of its Ringel variant associated to an abelian category satisfying adequate conditions. In Section 2 we recall basic facts on the category $\mathcal{A}$ of coherent sheaves on the projective line $\mathbf{P}^1(k)$ over an arbitrary field k and we carefully analyse the extensions between certain "elementary" objects. This leads in Section 3.1 to Theorem 10, which provides many structure constants of the Hall algebra of $\mathcal{A}$ when $k = \mathbf{F}_q$. Now every coherent sheaf can be written as the direct sum of its torsion subsheaf and of a locally free subsheaf. The existence of such decompositions gives rise to a factorization of the Hall algebra as a semidirect product of two subalgebras, denoted below by B_1 and $H(\mathcal{A}_{\mathrm{tor}})$, and related to locally free coherent sheaves and torsion sheaves, respectively. By an averaging process which takes into account all closed points of $\mathbf{P}^1(\mathbf{F}_q)$, we define in Sections 3.2 and 3.3 a subalgebra B_0 of $H(\mathcal{A}_{\mathrm{tor}})$. In the final Section 4, we recall the definition of the quantum affine algebra $U_q(\widehat{\mathfrak{sl}_2})$ and we relate it to the subalgebra of the Hall algebra generated by B_0 and B_1.

Our interest in this subject grew out of a seminar held in Strasbourg in 1996–97 and aimed at understanding Kapranov's paper [13]. We are grateful to Henri Carayol, Florence Lecomte, Louise Nyssen, Georges Papadopoulo, and Marc Rosso for their enlightening lectures. The first author acknowledges the financial support of the French Ministère de l'Education Nationale, de la Recherche et de la Technologie and of the CNRS.

1 Hall algebras

1.1 Initial data

Let k be a field. Recall that an abelian category $\mathcal{A}$ is said to be k-linear if the homomorphism groups in $\mathcal{A}$ are endowed with the structure of k-vector spaces, the composition of morphisms being a k-bilinear operation. The extension groups in $\mathcal{A}$, which can be defined even if $\mathcal{A}$ does not have enough injectives or projectives (see [3], § 7, n° 5), are then automatically k-vector spaces. In the sequel, we will consider abelian k-linear categories $\mathcal{A}$ satisfying the following finiteness conditions (H1)–(H3):

(H1) The isomorphism classes of objects in $\mathcal{A}$ form a set $\mathrm{Iso}(\mathcal{A})$.

(H2) For all objects V, W in $\mathcal{A}$, the k-vector spaces $\mathrm{Hom}_{\mathcal{A}}(V,W)$ and $\mathrm{Ext}^1_{\mathcal{A}}(V,W)$ are finite-dimensional.

(H3) The second extension group $\mathrm{Ext}^2_{\mathcal{A}}(V,W)$ vanishes for all objects V, W in $\mathcal{A}$.

The isomorphism class of an object V in $\mathcal{A}$ will be denoted by $[V] \in \mathrm{Iso}(\mathcal{A})$, and the isomorphism class of the zero object by $[0]$. It will be convenient to choose a preferred object $M(\alpha)$ in each isomorphism class $\alpha \in \mathrm{Iso}(\mathcal{A})$. Condition (H2) implies that $\mathcal{A}$ satisfies the Krull-Schmidt property: each object V in $\mathcal{A}$ can be written as a direct sum $W_1 \oplus \cdots \oplus W_\ell$ of indecomposable objects, the isomorphism classes of the objects W_i and their multiplicities in the decomposition being uniquely determined. Condition (H3) ensures that short exact sequences in $\mathcal{A}$ give rise to 6-term exact sequences of k-vector spaces involving the bifunctors $\mathrm{Hom}_{\mathcal{A}}(-,-)$ and $\mathrm{Ext}^1_{\mathcal{A}}(-,-)$.

The *Grothendieck group* of the category $\mathcal{A}$ is, by definition, the abelian group $K(\mathcal{A})$ presented by the generators $d(\alpha)$, where $\alpha \in \mathrm{Iso}(\mathcal{A})$, together with the relations $d(\beta) = d(\alpha) + d(\gamma)$ whenever there is a short exact sequence

$$0 \longrightarrow M(\gamma) \longrightarrow M(\beta) \longrightarrow M(\alpha) \longrightarrow 0.$$

If V is an object in $\mathcal{A}$, we will write $d(V)$ instead of $d([V])$ to denote the image of its class in the Grothendieck group. There exists a unique biadditive form $\langle \cdot, \cdot \rangle$ on $K(\mathcal{A})$, called the *Euler form*, such that for all objects V, W of $\mathcal{A}$,

$$\langle d(V), d(W) \rangle = \dim \mathrm{Hom}_{\mathcal{A}}(V,W) - \dim \mathrm{Ext}^1_{\mathcal{A}}(V,W).$$

Among the categories $\mathcal{A}$ that we will consider, certain enjoy an additional finiteness condition (H4), namely:

(H4) Each object in $\mathcal{A}$ has a finite filtration with simple quotients (Jordan-Hölder series).

If $\mathcal{A}$ satisfies Condition (H4), then $K(\mathcal{A})$ is the free abelian group on the symbols $d(\alpha)$, for all isomorphism classes $\alpha \in \mathrm{Iso}(\mathcal{A})$ of simple objects.

1.2 Hall numbers

In the remainder of Section 1, the field k will be the finite field $\mathbf{F}_q$ with q elements.

Given an isomorphism class $\alpha \in \mathrm{Iso}(\mathcal{A})$, we denote the order of the automorphism group $\mathrm{Aut}_{\mathcal{A}}(M(\alpha))$ by g_α.

Given three isomorphism classes $\alpha, \beta, \gamma \in \mathrm{Iso}(\mathcal{A})$, we denote by $\phi^\beta_{\alpha\gamma}$ the number of subobjects $X \subseteq M(\beta)$ such that $X \in \gamma$ and $M(\beta)/X \in \alpha$. To be more precise, let $S(\alpha,\beta,\gamma)$ be the set of pairs

$$(f,g) \in \mathrm{Hom}_{\mathcal{A}}(M(\gamma), M(\beta)) \times \mathrm{Hom}_{\mathcal{A}}(M(\beta), M(\alpha))$$

such that the sequence

$$0 \longrightarrow M(\gamma) \xrightarrow{f} M(\beta) \xrightarrow{g} M(\alpha) \longrightarrow 0$$

is exact. The group $\mathrm{Aut}_{\mathcal{A}}(M(\alpha)) \times \mathrm{Aut}_{\mathcal{A}}(M(\gamma))$ acts freely on $S(\alpha,\beta,\gamma)$, and $\phi^{\beta}_{\alpha\gamma}$ is by definition the cardinality of the quotient space $S(\alpha,\beta,\gamma)/(\mathrm{Aut}_{\mathcal{A}}(M(\alpha)) \times \mathrm{Aut}_{\mathcal{A}}(M(\gamma)))$.

The integer $\phi^{\beta}_{\alpha\gamma}$ is called a *Hall number*. It is zero if $d(\beta) \neq d(\alpha) + d(\gamma)$. Hall numbers have the following properties.

Proposition 1 *If $\alpha, \beta, \gamma, \delta \in \mathrm{Iso}(\mathcal{A})$ are isomorphism classes, then*

(i) there are only finitely many isomorphism classes λ such that $\phi^{\lambda}_{\alpha\gamma} \neq 0$;

(ii) if (H4) holds, there are only finitely many pairs $(\rho, \sigma) \in \mathrm{Iso}(\mathcal{A})^2$ such that $\phi^{\beta}_{\rho\sigma} \neq 0$;

(iii) $\phi^{\beta}_{\alpha[0]} = \delta_{\alpha\beta}$ and $\phi^{\beta}_{[0]\gamma} = \delta_{\beta\gamma}$ (Kronecker symbols);

(iv) $\displaystyle\sum_{\lambda \in \mathrm{Iso}(\mathcal{A})} \phi^{\lambda}_{\alpha\beta}\phi^{\delta}_{\lambda\gamma} = \sum_{\lambda \in \mathrm{Iso}(\mathcal{A})} \phi^{\delta}_{\alpha\lambda}\phi^{\lambda}_{\beta\gamma}$;

(v) the number $q^{\dim \mathrm{Hom}_{\mathcal{A}}(M(\alpha), M(\gamma))}\, \phi^{\beta}_{\alpha\gamma}\, g_\alpha g_\gamma / g_\beta$ is an integer;

(vi) $\displaystyle\sum_{\lambda \in \mathrm{Iso}(\mathcal{A})} \phi^{\lambda}_{\alpha\gamma}\, g_\alpha g_\gamma / g_\lambda = q^{-\langle d(\alpha), d(\gamma)\rangle}$;

(vii) if $M(\alpha)$ and $M(\gamma)$ are indecomposable objects and $M(\beta)$ is a decomposable object, then $q-1$ divides $\phi^{\beta}_{\alpha\gamma} - \phi^{\beta}_{\gamma\alpha}$;

(viii) the following formula holds:

$$g_\alpha g_\beta g_\gamma g_\delta \sum_{\lambda \in \mathrm{Iso}(\mathcal{A})} \phi^{\lambda}_{\alpha\beta}\, \phi^{\lambda}_{\gamma\delta} / g_\lambda = \sum_{\rho,\sigma,\tau,\upsilon \in \mathrm{Iso}(\mathcal{A})} q^{-\langle d(\rho), d(\upsilon)\rangle}\, \phi^{\alpha}_{\rho\sigma}\, \phi^{\beta}_{\tau\upsilon}\, \phi^{\gamma}_{\rho\tau}\, \phi^{\delta}_{\sigma\upsilon}\, g_\rho g_\sigma g_\tau g_\upsilon.$$

In the above statement, the sums in Items (iv), (vi), and (viii) involve a finite number of non-zero terms.

Proof. Assertion (i) holds because the extension group $\mathrm{Ext}^1_{\mathcal{A}}(M(\alpha), M(\gamma))$ is a finite set. Conditions (H2) and (H4) imply that the map $d : \mathrm{Iso}(\mathcal{A}) \to K(\mathcal{A})$ has finite fibers; Assertion (ii) follows from this fact. Assertion (iii) is trivial. Assertion (iv) is Proposition 1 in [16]. Items (v) and (vi) are consequences of the proposition in Section II.4 of [19] (see also [14], p. 221). To prove (vii), it suffices to follow the proof of Proposition 1 in [17]. Finally, to prove (viii), one can adapt the proof of Theorem 2 in [8] to the present framework. □

1.3 The Hall algebra and the Ringel-Green bialgebra

We will use $\widetilde{\mathbf{Z}} = \mathbf{Z}[v, v^{-1}]/(v^2 - q)$ as the ground ring. Let $H(\mathcal{A})$ be the free $\widetilde{\mathbf{Z}}$-module on the symbols α, where α runs over $\operatorname{Iso}(\mathcal{A})$. Items (i), (iii), and (iv) of Proposition 1 show that the multiplication

$$\alpha \cdot \gamma = \sum_{\beta \in \operatorname{Iso}(\mathcal{A})} \phi^{\beta}_{\alpha\gamma}\, \beta$$

endows $H(\mathcal{A})$ with the structure of an associative $\widetilde{\mathbf{Z}}$-algebra with unit given by [0]. This algebra is called the *Hall algebra* of the category $\mathcal{A}$; it is graded by the group $K(\mathcal{A})$, the symbol α being homogeneous of degree $d(\alpha)$.

Using the Euler form on $K(\mathcal{A})$ and following [15], one can twist this product and get a new multiplication $*$ on $H(\mathcal{A})$, by setting on the basis vectors

$$\alpha * \gamma = v^{\langle d(\alpha), d(\gamma)\rangle}\, \alpha \cdot \gamma.$$

The associative $\widetilde{\mathbf{Z}}$-algebra with unit that one obtains in this way is called the *Ringel algebra.*

If Condition (H4) holds, then one can define a coproduct $\Delta : H(\mathcal{A}) \to H(\mathcal{A}) \otimes_{\widetilde{\mathbf{Z}}} H(\mathcal{A})$ and a coünit $\varepsilon : H(\mathcal{A}) \to \widetilde{\mathbf{Z}}$ by

$$\Delta(\beta) = \sum_{\alpha,\gamma \in \operatorname{Iso}(\mathcal{A})} v^{\langle d(\alpha), d(\gamma)\rangle}\, \frac{g_\alpha g_\gamma}{g_\beta}\, \phi^{\beta}_{\alpha\gamma}\, (\alpha \otimes \gamma) \qquad \text{and} \qquad \varepsilon(\beta) = \delta_{\beta[0]},$$

for all $\beta \in \operatorname{Iso}(\mathcal{A})$. In this way, $H(\mathcal{A})$ becomes a $\widetilde{\mathbf{Z}}$-coalgebra in view of Properties (ii)–(v) of Proposition 1. Property (viii) of Proposition 1 implies that Δ is an homomorphism of algebras when one equips $H(\mathcal{A}) \otimes_{\widetilde{\mathbf{Z}}} H(\mathcal{A})$ with the following twisted product:

$$(\alpha \otimes \beta) * (\gamma \otimes \delta) = v^{\langle d(\beta), d(\gamma)\rangle + \langle d(\gamma), d(\beta)\rangle}\, (\alpha * \gamma) \otimes (\beta * \delta),$$

where $\alpha, \beta, \gamma, \delta \in \operatorname{Iso}(\mathcal{A})$. Endowed with the Ringel product $*$, the coproduct Δ, and the coünit ε, the $\widetilde{\mathbf{Z}}$-module $H(\mathcal{A})$ is called the *twisted Ringel-Green bialgebra.*

2 Coherent sheaves over the projective line

Let k be a field. In this section, we investigate the category $\mathcal{A}$ of coherent sheaves over the projective line $\mathbf{P}^1(k)$. We recall what the indecomposable objects of $\mathcal{A}$ are and study certain extensions between them. This information will be used in Section 3 to determine structure constants of the Hall algebra $H(\mathcal{A})$ when k is a finite field.

2.1 Generalities on coherent sheaves on $\mathbf{P}^1(k)$

We put homogeneous coordinates $(t : u)$ on $\mathbf{P}^1(k)$. The two affine open subsets

$$U' = \{(t : u) \mid t \neq 0\} \quad \text{and} \quad U'' = \{(t : u) \mid u \neq 0\}$$

cover $\mathbf{P}^1(k)$, and the formulae $z = u/t$ and $z^{-1} = t/u$ define coordinates on U' and U'' respectively. The rings $k[z]$ and $k[z^{-1}]$ are the respective rings of regular functions on U' and U''.

We will use the following convention: if A is a commutative ring, M an A-module and z an element of A, then M_z denotes the localized A-module obtained from M by inverting z. An analogous notation will be used for morphisms.

An object of the category $\mathcal{A}$ of *coherent sheaves* on $\mathbf{P}^1(k)$ is a triple (M', M'', φ), where M' is a finitely generated $k[z]$-module, M'' is a finitely generated $k[z^{-1}]$-module, and $\varphi : M'_z \to M''_{z^{-1}}$ is an isomorphism of $k[z, z^{-1}]$-modules. A morphism in $\mathcal{A}$ from the coherent sheaf (M', M'', φ) to the coherent sheaf (N', N'', ψ) is a pair of maps (f', f''), where $f' : M' \to N'$ is a $k[z]$-linear map and $f'' : M'' \to N''$ is a $k[z^{-1}]$-linear map such that $\psi \circ f'_z = f''_{z^{-1}} \circ \varphi$. One also defines in an obvious way the notions of direct sums and exact sequences in $\mathcal{A}$, so that $\mathcal{A}$ becomes an abelian k-linear category. This definition of $\mathcal{A}$ is equivalent to the standard geometric definition that can be found, for instance, in Section II.5 of [11].

The study of coherent sheaves over a curve splits into the study of locally free sheaves and the study of torsion coherent sheaves. In our case, a coherent sheaf $\mathcal{F} = (M', M'', \varphi)$ is said to be *locally free* if M' and M'' are free modules over $k[z]$ and $k[z^{-1}]$ respectively; the sheaf $\mathcal{F}$ is said to be a *torsion sheaf* if M' is a torsion $k[z]$-module, which is equivalent to a similar requirement for M'_z, $M''_{z^{-1}}$, or M''. The full subcategory of $\mathcal{A}$ consisting of all locally free sheaves will be denoted by $\mathcal{A}_{\mathrm{lf}}$. The full subcategory of $\mathcal{A}$ consisting of all torsion sheaves will be denoted by $\mathcal{A}_{\mathrm{tor}}$.

The study of coherent torsion sheaves splits further into the study of torsion sheaves whose support is a point. Let us first recall the notion of closed point.

A *closed point* x of $\mathbf{P}^1(k)$ is the zero locus of an irreducible homogeneous polynomial $P \in k[T, U]$. If P is proportional to the polynomial T (respectively, U), then the closed point is the point at infinity $\infty \in U''$ (respectively, is the origin $0 \in U'$). Otherwise, x can be viewed as the zero locus in U' of the irreducible polynomial $P(1, z) \in k[z]$ and as the zero locus in U'' of the irreducible polynomial $P(z^{-1}, 1) \in k[z^{-1}]$. In any case, x determines P up to a non-zero scalar, and the degree $\deg x$ of x is defined as the degree of P.

If x belongs to the affine open set U' (respectively, to U''), one defines the local ring $\mathcal{O}_{\mathbf{P}^1(k),x}$ of rational functions regular near x as the localization of $k[z]$ at the prime ideal generated by $P(1, z)$ (respectively, as the localization of $k[z^{-1}]$ at the prime ideal generated by $P(z^{-1}, 1)$). If x belongs to U' and to U'', then both definitions of $\mathcal{O}_{\mathbf{P}^1(k),x}$ yield isomorphic rings. We choose a generator π_x of the maximal ideal of $\mathcal{O}_{\mathbf{P}^1(k),x}$ ("uniformizer"), and denote by $\mathcal{O}_{\mathbf{P}^1(k),x}$-$\underline{\mathrm{modf}}$ the category of $\mathcal{O}_{\mathbf{P}^1(k),x}$-modules of finite length, that is, of modules that are finitely generated and annihilated by some power of π_x.

Let $\mathcal{F} = (M', M'', \varphi)$ be a coherent sheaf and x be a closed point, determined by the irreducible homogeneous polynomial P, and belonging to U' (respectively, U''). The *stalk* $\mathcal{F}_x$ of the sheaf $\mathcal{F}$ at x is the $\mathcal{O}_{\mathbf{P}^1(k),x}$-module obtained by localizing the $k[z]$-module M' at the prime ideal generated by $P(1, z)$ (respectively, the $k[z^{-1}]$-module M'' at the prime ideal generated by $P(z^{-1}, 1)$). If x belongs to U' and U'', then both definitions are equivalent. One says that the point x belongs to the *support* of $\mathcal{F}$ if the stalk $\mathcal{F}_x$ does not vanish. The support of a torsion coherent sheaf if always a finite set of points. Given a closed point x, we denote by $\mathcal{A}_{\{x\}}$ the full subcategory of $\mathcal{A}$ consisting of all torsion sheaves with support included in $\{x\}$.

Proposition 2 *(i) The category $\mathcal{A}$ is k-linear, abelian, and satisfies Conditions (H1)–(H3) of Section 1.1. The subcategories $\mathcal{A}_{\mathrm{lf}}$, $\mathcal{A}_{\mathrm{tor}}$, and $\mathcal{A}_{\{x\}}$ of $\mathcal{A}$ are closed under extensions. The categories $\mathcal{A}_{\mathrm{tor}}$ and $\mathcal{A}_{\{x\}}$ are k-linear, abelian, and satisfy Conditions (H1)–(H4) of Section 1.1.*

(ii) If $\mathcal{F}$ is a locally free sheaf and $\mathcal{G}$ is a torsion sheaf, then $\mathrm{Hom}_{\mathcal{A}}(\mathcal{G},\mathcal{F}) = \mathrm{Ext}^1_{\mathcal{A}}(\mathcal{F},\mathcal{G}) = 0$.

(iii) If $\mathcal{F}$ and $\mathcal{G}$ are torsion sheaves with disjoint supports, then $\mathrm{Hom}_{\mathcal{A}}(\mathcal{F},\mathcal{G}) = \mathrm{Ext}^1_{\mathcal{A}}(\mathcal{F},\mathcal{G}) = 0$.

(iv) Every coherent sheaf $\mathcal{F}$ can be written as a direct sum of a torsion sheaf and a locally free sheaf. Every torsion sheaf can be written as a finite direct sum of sheaves whose supports are closed points.

(v) The category $\mathcal{A}_{\mathrm{tor}}$ is the direct sum of the subcategories $\mathcal{A}_{\{x\}}$, where x runs over the set of all closed points of $\mathbf{P}^1(k)$.

(vi) Going from a sheaf to its stalk at a closed point x gives an isomorphism of categories from $\mathcal{A}_{\{x\}}$ to $\mathcal{O}_{\mathbf{P}^1(k),x}$-$\underline{\mathrm{modf}}$.

Proof. (i) The assertion about $\mathcal{A}$ is a standard result of algebraic geometry. It is immediate from the definitions that $\mathcal{A}_{\mathrm{lf}}$, $\mathcal{A}_{\mathrm{tor}}$, and $\mathcal{A}_{\{x\}}$ are closed under extensions in $\mathcal{A}$. Since subobjects and quotients of torsion sheaves are torsion sheaves, $\mathcal{A}_{\mathrm{tor}}$ is an abelian subcategory of $\mathcal{A}$, and the Ext spaces between two objects in $\mathcal{A}_{\mathrm{tor}}$ are the same when computed in $\mathcal{A}$ or in $\mathcal{A}_{\mathrm{tor}}$. Therefore $\mathcal{A}_{\mathrm{tor}}$ satisfies Conditions (H1)–(H3). Finally, the simple fact that finitely generated torsion modules over principal ideal domains have Jordan-Hölder series implies that $\mathcal{A}_{\mathrm{tor}}$ satisfies Condition (H4). A similar argument shows that $\mathcal{A}_{\{x\}}$ is an abelian subcategory of $\mathcal{A}$ which satisfies Conditions (H1)–(H4).

(ii) Given a locally free sheaf $\mathcal{F}$ and a torsion sheaf $\mathcal{G}$, the vanishing of $\mathrm{Hom}_{\mathcal{A}}(\mathcal{G},\mathcal{F})$ is a direct consequence of the definitions, while that of $\mathrm{Ext}^1_{\mathcal{A}}(\mathcal{F},\mathcal{G})$ follows from Serre's vanishing theorem (Theorem III.5.2 (b) in [11]).
(iii) and (vi) These assertions follow from standard properties of finitely generated torsion modules over the principal ideal domains $k[z]$ and $k[z^{-1}]$.

(iv) Let $\mathcal{F}$ be a coherent sheaf. One can define in an obvious way the torsion subsheaf $\mathrm{tor}(\mathcal{F})$ of $\mathcal{F}$, and the quotient sheaf $\mathcal{F}/\mathrm{tor}(\mathcal{F})$ is locally free. By Assertion (ii), the group $\mathrm{Ext}^1_{\mathcal{A}}(\mathcal{F}/\mathrm{tor}(\mathcal{F}),\mathrm{tor}(\mathcal{F}))$ vanishes. Thus the short exact sequence

$$0 \longrightarrow \mathrm{tor}(\mathcal{F}) \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}/\mathrm{tor}(\mathcal{F}) \longrightarrow 0$$

splits and one gets the decomposition $\mathcal{F} \simeq \mathrm{tor}(\mathcal{F}) \oplus (\mathcal{F}/\mathrm{tor}(\mathcal{F}))$, as desired in the first assertion. The second assertion follows from the primary decomposition of finitely generated torsion modules over the principal ideal domains $k[z]$ and $k[z^{-1}]$.

(v) This follows from Assertions (iii) and (iv).
□

2.2 Indecomposable coherent sheaves over $\mathbf{P}^1(k)$

By Assertion (iv) of Proposition 2, indecomposable objects of $\mathcal{A}$ are either locally free or have support in some closed point $\{x\}$.

For any $n \in \mathbf{Z}$, we construct a locally free coherent sheaf (M', M'', φ) by letting $M' = k[z]$, $M'' = k[z^{-1}]$, and $\varphi : k[z, z^{-1}] \to k[z, z^{-1}]$ be the multiplication by z^{-n}. As usual, this sheaf will be denoted by $\mathcal{O}(n)$. A theorem of Grothendieck [10] asserts that any locally free coherent sheaf is isomorphic to a direct sum $\mathcal{O}(n_1) \oplus \cdots \oplus \mathcal{O}(n_r)$ for some sequence $n_1 \leq \cdots \leq n_r$ of uniquely determined integers. Thus the sheaves $\mathcal{O}(n)$ are the indecomposable locally free coherent sheaves.

For any $m, n \in \mathbf{Z}$, the space of homogeneous polynomials $F \in k[T, U]$ of degree $n - m$ is naturally isomorphic to the homomorphism space $\operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))$: one associates to F the pair of maps (f', f''), where $f' : k[z] \to k[z]$ is the multiplication by $F(1, z)$ and $f'' : k[z^{-1}] \to k[z^{-1}]$ is the multiplication by $F(z^{-1}, 1)$.

In particular, given an irreducible homogeneous polynomial $P \in k[T, U]$ of degree d and an integer $r \geq 1$, the r-th power polynomial P^r defines a morphism from $\mathcal{O}(-rd)$ to $\mathcal{O}(0)$. The cokernel is the torsion sheaf (M', M'', φ), where $M' = k[z]/(P(1, z)^r)$, $M'' = k[z^{-1}]/(P(z^{-1}, 1)^r)$ and φ is induced by the identity of $k[z, z^{-1}]$. Calling x the closed point defined by P, we denote this torsion sheaf by $\mathcal{O}_{r[x]}$; its support is $\{x\}$. Through the isomorphism of categories of Proposition 2 (vi), this sheaf corresponds to the $\mathcal{O}_{\mathbf{P}^1(k),x}$-module $\mathcal{O}_{\mathbf{P}^1(k),x}/(\pi_x^r)$. Consequently, these sheaves $\mathcal{O}_{r[x]}$ are the indecomposable objects of the category $\mathcal{A}_{\{x\}}$.

To deal with torsion sheaves more conveniently in the sequel, we introduce some further notation. According to standard terminology, a partition is a non-increasing sequence of non-negative integers with only finitely many non-zero terms: $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$ with $\lambda_i = 0$ for i big enough. The length of λ is the smallest integer $\ell \geq 0$ such that $\lambda_{\ell+1} = 0$, and the weight $|\lambda|$ of λ is the sum of the non-zero integers λ_i. We also put $n(\lambda) = \sum_{i \geq 1}(i-1)\lambda_i$, as in [14]. The empty partition is the partition with no non-zero part; the partition with r non-zero parts, all equal to 1, is denoted by (1^r); the partition with one non-zero part, equal to r, is denoted by (r). Finally, given a closed point x and a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$ of length ℓ, we define the torsion sheaf

$$\mathcal{O}_{\lambda[x]} = \mathcal{O}_{\lambda_1[x]} \oplus \cdots \oplus \mathcal{O}_{\lambda_\ell[x]}.$$

For instance, $\mathcal{O}_{(1^r)[x]} = \left(\mathcal{O}_{[x]}\right)^{\oplus r}$ and $\mathcal{O}_{(r)[x]} = \mathcal{O}_{r[x]}$.

2.3 The Grothendieck group and the Euler form

We define the rank and the degree of an indecomposable sheaf by

$$\operatorname{rk} \mathcal{O}(n) = 1, \quad \deg \mathcal{O}(n) = n, \quad \operatorname{rk} \mathcal{O}_{r[x]} = 0, \quad \text{and} \quad \deg \mathcal{O}_{r[x]} = r \deg x.$$

Since every coherent sheaf can be written in an essentially unique way as a sum of indecomposable sheaves, we may extend additively the notions of rank and degree to arbitrary coherent sheaves. It is well-known from algebraic geometry that the rank and degree maps factor through the Grothendieck group $K(\mathcal{A})$, defining a isomorphism of abelian groups $K(\mathcal{A}) \to \mathbf{Z}^2$ by

$$d(\mathcal{F}) \mapsto (\operatorname{rk}\mathcal{F}, \deg\mathcal{F}).$$

Proposition 3 *The Euler form on $K(\mathcal{A})$ is given for all coherent sheaves $\mathcal{F}$ and $\mathcal{G}$ by*

$$\langle d(\mathcal{F}), d(\mathcal{G})\rangle = \operatorname{rk}\mathcal{F}\ \operatorname{rk}\mathcal{G} + \operatorname{rk}\mathcal{F}\ \deg\mathcal{G} - \deg\mathcal{F}\ \operatorname{rk}\mathcal{G}. \tag{1}$$

Proof. Using the Riemann-Roch formula (Theorem IV.1.3 in [11]) and standard results of sheaf cohomology (Propositions II.5.12, III.6.3 (c), and III.6.7 in [11]), we obtain

$$\begin{aligned}
\langle d(\mathcal{O}(m)), d(\mathcal{O}(n))\rangle &= \dim \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n)) - \dim \operatorname{Ext}^1_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n)) \\
&= \dim \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}_{\mathbf{P}^1(k)}, \mathcal{O}(n-m)) - \dim \operatorname{Ext}^1_{\mathcal{A}}(\mathcal{O}_{\mathbf{P}^1(k)}, \mathcal{O}(n-m)) \\
&= \dim H^0(\mathbf{P}^1(k), \mathcal{O}(n-m)) - \dim H^1(\mathbf{P}^1(k), \mathcal{O}(n-m)) \\
&= 1 + \deg(\mathcal{O}(n-m)) \\
&= 1 + n - m \\
&= \operatorname{rk}\mathcal{O}(m)\ \operatorname{rk}\mathcal{O}(n)\ +\ \operatorname{rk}\mathcal{O}(m)\ \deg\mathcal{O}(n)\ -\ \deg\mathcal{O}(m)\ \operatorname{rk}\mathcal{O}(n)
\end{aligned}$$

for all $m, n \in \mathbf{Z}$. This proves (1) when $\mathcal{F}$ and $\mathcal{G}$ are locally free sheaves of rank 1. Since the classes of such sheaves generate $K(\mathcal{A})$, the general case follows by the biadditivity of both sides of (1). □

2.4 Some extensions of sheaves

In this section, we study in detail certain extensions in the category $\mathcal{A}$. Beforehand, let us record the following lemma, whose proof is immediate from the definitions in Section 2.2.

Lemma 4 *For all $m, n \in \mathbf{Z}$,*

(i) any non-zero element in $\operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))$ is a monomorphism;

(ii) as a k-algebra, $\operatorname{End}_{\mathcal{A}}(\mathcal{O}(n)) \simeq k$;

(iii) the k-vector space $\operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))$ has dimension $\max(0, n-m+1)$;

(iv) for any closed point x and any partition λ, the k-vector space $\operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(n), \mathcal{O}_{\lambda[x]})$ has dimension $|\lambda| \deg x$.

Our first result describes the extensions between the indecomposable locally free sheaves. In a short exact sequence of the form

$$0 \longrightarrow \mathcal{O}(m) \xrightarrow{f} \mathcal{F} \xrightarrow{g} \mathcal{O}(n) \longrightarrow 0,$$

the coherent sheaf $\mathcal{F}$ is necessarily locally free of rank 2, and so there are integers p and $q \in \mathbf{Z}$ such that $\mathcal{F}$ is isomorphic to the sheaf $\mathcal{O}(p) \oplus \mathcal{O}(q)$.

Proposition 5 *Let m, n, p, q be integers, and consider a sequence of the form*

$$0 \longrightarrow \mathcal{O}(m) \xrightarrow{f} \mathcal{O}(p) \oplus \mathcal{O}(q) \xrightarrow{g} \mathcal{O}(n) \longrightarrow 0.$$

Let

$$\begin{aligned} h &\in \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(p)), & j &\in \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(p), \mathcal{O}(n)), \\ i &\in \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(q)), & \ell &\in \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(q), \mathcal{O}(n)), \end{aligned}$$

be defined by $f = h \oplus i$ and $g = j \oplus \ell$, and call H, I, J, L the homogeneous polynomials in $k[T, U]$ representing h, i, j, ℓ, respectively. Then the sequence is a non-split short exact sequence if and only if the following three conditions are satisfied:

(a) $m < \min(p, q)$, $\max(p, q) < n$, and $p + q = m + n$.

(b) J and L are coprime polynomials.

(c) There is a non-zero scalar E such that $H = EL$ and $I = -EJ$.

Proof. We first prove that Conditions (a), (b), and (c) are necessary. Suppose that the sequence is exact and non-split. If one of the homomorphism h or i was the zero arrow, then the other one would be an isomorphism since the cokernel of f is indecomposable, and the sequence would split. Similarly, neither j nor ℓ can vanish. The four maps h, i, j, and ℓ are thus non-zero. The fact that the sequence does not split also implies that none of these maps is an isomorphism. In view of Lemma 4 (ii) and (iii), it follows that $m < \min(p, q)$ and $\max(p, q) < n$. For degree reasons we also have $m + n = p + q$. Therefore Condition (a) holds.

Let us turn to Condition (b). In the unique factorization domain $k[T, U]$, one may consider a g.c.d. D of the polynomials J and L. Since every irreducible factor of a homogeneous polynomial is itself homogeneous (by uniqueness of the factorization), the polynomial D is homogeneous and defines a homomorphism $d \in \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(n - \deg D), \mathcal{O}(n))$. We get a factorization

$$\begin{tikzcd} \mathcal{O}(p) \oplus \mathcal{O}(q) \arrow[rr, "g"] \arrow[dr] & & \mathcal{O}(n) \\ & \mathcal{O}(n - \deg D) \arrow[ur, "d"'] & \end{tikzcd} .$$

Since g is surjective, so must be d. The non-zero morphism d being injective by Lemma 4 (i), it is an isomorphism, which implies that $\deg D = 0$. Thus J and L are coprime, and Condition (b) holds.

Finally, the equality $g \circ f = 0$ implies that $HJ + IL = 0$. Condition (b) and Gauss's lemma then imply the existence of a non-zero homogeneous polynomial $E \in k[T, U]$ such that $H = EL$ and $I = -EJ$. Since

$$2 \deg E = \deg H + \deg I - \deg L - \deg J = (p - m) + (q - m) - (n - q) - (n - p) = 0,$$

E is a constant polynomial, which proves Condition (c).

In order to prove the converse statement, we now assume that Conditions (a), (b), and (c) are fulfilled. Over the affine subset U', our sequence of sheaves reads

$$\begin{array}{ccccccccc} 0 \longrightarrow & \mathcal{O}(m)(U') & \xrightarrow{f_{U'}=h_{U'}\oplus i_{U'}} & \mathcal{O}(p)(U') \oplus \mathcal{O}(q)(U') & \xrightarrow{g_{U'}=j_{U'}\oplus \ell_{U'}} & \mathcal{O}(n)(U') & \longrightarrow 0, \\ & \| & & \| & & \| & \\ & k[z] & & k[z] \oplus k[z] & & k[z] & \end{array}$$

where the maps $h_{U'}$, $i_{U'}, \ldots$ are the multiplications by $H(1, z)$, $I(1, z), \ldots$ respectively. Condition (b) implies that the polynomials $J(1, z)$ and $L(1, z)$ are coprime, which ensures by Bezout's lemma that the $k[z]$-linear map $g_{U'}$ is surjective. An analogous simple reasoning based on Gauss's lemma shows that Conditions (b) and (c) imply that $\ker g_{U'} = \operatorname{im} f_{U'}$. Thus our sequence of sheaves is exact over the open subset U'. A similar argument can be used over U'', and we conclude that our sequence of sheaves is exact. □

Corollary 6 *If $m, n \in \mathbf{Z}$ are integers satisfying $n \leq m + 1$, then the extension group $\operatorname{Ext}^1_{\mathcal{A}}(\mathcal{O}(n), \mathcal{O}(m))$ vanishes.*

We now investigate the extensions of certain torsion sheaves by indecomposable locally free sheaves. We begin with the following lemma.

Lemma 7 *Let x be a closed point of $\mathbf{P}^1(k)$, corresponding to an irreducible homogeneous polynomial $P \in k[T, U]$. Let $m, n \in \mathbf{Z}$, let $F \in k[T, U]$ be a non-zero homogeneous polynomial of degree $n - m$, and let $f \in \operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))$ be the morphism defined by F. If the support of the cokernel of f is included in $\{x\}$, then there exists an integer $r \geq 1$ such that $F = P^r$, up to a non-zero scalar, and one has* $\operatorname{coker} f \simeq \mathcal{O}_{r[x]}$.

Proof. The polynomial F defines a morphism $\widetilde{f} : \mathcal{O}(m-n) \to \mathcal{O}(0)$. By unique factorization, and up to a non-zero scalar, we can write $F = P_1^{r_1} \cdots P_t^{r_t}$, for some positive integers $r_1, \ldots, r_t$ and some pairwise non-proportional irreducible homogeneous polynomials $P_1, \ldots, P_t$. For each $1 \leq i \leq t$, let x_i be the closed point of $\mathbf{P}^1(k)$ corresponding to P_i. The homogeneous polynomial $P_i^{r_i}$ defines an element of $\operatorname{Hom}_{\mathcal{A}}(\mathcal{O}(-r_i \deg P_i), \mathcal{O}(0))$ whose cokernel is $\mathcal{O}_{r_i[x_i]}$, whence a canonical morphism $g_i : \mathcal{O}(0) \to \mathcal{O}_{r_i[x_i]}$. A direct application of the Chinese remainder theorem implies that the sequence

$$0 \longrightarrow \mathcal{O}(m-n) \xrightarrow{\widetilde{f}} \mathcal{O}(0) \xrightarrow{\oplus g_i} \oplus_{i=1}^t \mathcal{O}_{r_i[x_i]} \longrightarrow 0$$

is exact over the affine subsets U' and U'', hence is exact. Taking the tensor product with the locally free sheaf $\mathcal{O}(n)$, we get an exact sequence

$$0 \longrightarrow \mathcal{O}(m) \xrightarrow{f} \mathcal{O}(n) \longrightarrow \oplus_{i=1}^t \mathcal{O}_{r_i[x_i]} \longrightarrow 0.$$

Therefore, the cokernel of f is isomorphic to $\mathcal{O}_{r_1[x_1]} \oplus \cdots \oplus \mathcal{O}_{r_t[x_t]}$. If the support of $\operatorname{coker} f$ is included in $\{x\}$, then $t = 1$ and $P_1 = P$, up to a non-zero scalar, which entails the lemma. □

Proposition 8 *Given a closed point x and an integer $r \geq 1$, let*

$$0 \longrightarrow \mathcal{O}(m) \xrightarrow{f} \mathcal{F} \xrightarrow{g} \mathcal{O}_{(1^r)[x]} \longrightarrow 0$$

be a non-split short exact sequence of coherent sheaves. Then the middle term $\mathcal{F}$ is isomorphic to $\mathcal{O}_{(1^{r-1})[x]} \oplus \mathcal{O}(m + \deg x)$. If we write $f = h \oplus i$ in this decomposition, then $h = 0$ and $\operatorname{coker} i \simeq \mathcal{O}_{[x]}$.

Proof. We can write $\mathcal{F}$ as the direct sum of a torsion sheaf $\mathcal{F}_0$ and a locally free sheaf $\mathcal{F}_1$ of rank 1. Write the maps f and g as $h \oplus i$ and $j \oplus \ell$ in the decomposition $\mathcal{F} = \mathcal{F}_0 \oplus \mathcal{F}_1$. The morphism h cannot be injective, so i cannot be zero, so i is injective (Lemma 4 (i)), and it follows that j is injective. Thus $\mathcal{F}_0$ must be isomorphic to a subobject of $\mathcal{O}_{(1^r)[x]}$.

Under the isomorphism of categories described in Proposition 2 (vi), the sheaf $\mathcal{O}_{(1^r)[x]}$ corresponds to the elementary $\mathcal{O}_{\mathbf{P}^1(k),x}$-module $\left(\mathcal{O}_{\mathbf{P}^1(k),x}/(\pi_x)\right)^{\oplus r}$, hence to a vector space of dimension r over the residue field $\mathcal{O}_{\mathbf{P}^1(k),x}/(\pi_x)$. This shows that $\mathcal{F}_0$ is isomorphic to $\mathcal{O}_{(1^s)[x]}$ for some $s \leq r$. In the same way, and using Lemma 7, we see that the image of ℓ is either 0 or isomorphic to $\mathcal{O}_{[x]}$.

Now if the sequence is not split, then j is not an isomorphism, which rules out the case $s = r$. The surjectivity of g then requires that $s = r - 1$, that $\operatorname{im} \ell \simeq \mathcal{O}_{[x]}$, and that $\mathcal{O}_{(1^r)[x]} = \operatorname{im} j \oplus \operatorname{im} \ell$. The equality $g \circ f = 0$ then splits into the two equalities $j \circ h = 0$ and $\ell \circ i = 0$. Since j is injective, we get $h = 0$ and thus $\operatorname{coker} i \simeq \mathcal{O}_{[x]}$. Finally we compute

$$\deg \mathcal{F}_1 = \deg \mathcal{O}(m) + \deg \mathcal{O}_{(1^r)[x]} - \deg \mathcal{F}_0 = m + r \deg x - s \deg x = m + \deg x,$$

which shows that $\mathcal{F}_1 \simeq \mathcal{O}(m + \deg x)$. □

3 The Hall algebra of $\mathrm{Coh}(\mathbf{P}^1(\mathbf{F}_q))$

From now on, k is the finite field $\mathbf{F}_q$ with q elements, and $\mathcal{A}$ stands for the category of coherent sheaves over $\mathbf{P}^1(k)$. In this section, we describe the Ringel algebra $H(\mathcal{A})$. Relying on results of Section 2, we first compute some Hall numbers. Using results explained in Chapters II and III of [14], we next investigate more closely the Ringel algebras $H(\mathcal{A}_{\{x\}})$ and $H(\mathcal{A}_{\mathrm{tor}})$, which will be viewed as subalgebras of $H(\mathcal{A})$. This allows us eventually to define a certain subalgebra B of $H(\mathcal{A})$, which will turn out in Section 4 to be related to the quantum affine algebra $U_q(\widehat{\mathfrak{sl}_2})$.

3.1 Some Hall numbers for $\mathcal{A}$

We start with the following elementary combinatorial lemma.

Lemma 9 *The number $\varphi(a, b)$ of pairs (J, L) consisting of coprime homogeneous polynomials in $\mathbf{F}_q[T, U]$ of degrees a and b, respectively, is given by*

$$\varphi(a, b) = \begin{cases} (q-1)(q^{a+b+1} - 1) & \text{if } a = 0 \text{ or } b = 0, \\ (q-1)(q^2 - 1)q^{a+b-1} & \text{if } a \geq 1 \text{ and } b \geq 1. \end{cases}$$

Proof. Let S be the set of pairs $(J, L) \in \mathbf{F}_q[T, U]$ consisting of non-zero homogeneous polynomials of degree a and b respectively. The cardinality of S is $(q^{a+1} - 1)(q^{b+1} - 1)$. One can also count the number of elements in S by factoring out a g.c.d. D of J and L. For a fixed degree $d \leq \min(a, b)$, there are $(q^{d+1} - 1)/(q - 1)$ possibilities for D up to a non-zero scalar, and we thus get the relation

$$(q^{a+1} - 1)(q^{b+1} - 1) = \sum_{d=0}^{\min(a,b)} \frac{q^{d+1} - 1}{q - 1} \, \varphi(a - d, b - d).$$

The lemma then follows by induction on $\min(a, b)$. □

For any closed point x of $\mathbf{P}^1(\mathbf{F}_q)$, let $q_x = q^{\deg x}$ be the cardinal of the residue field of the local ring $\mathcal{O}_{\mathbf{P}^1(\mathbf{F}_q),x}$. We denote the greatest integer less than or equal to a real number a by $\lfloor a \rfloor$. The following theorem provides Hall numbers for the category $\mathcal{A}$.

Theorem 10 *In the Hall algebra $H(\mathcal{A})$, one has the following relations:*

(i) $[\mathcal{O}(m)^{\oplus a}][\mathcal{O}(m)^{\oplus b}] = \left(\prod_{c=1}^{a} \frac{q^{b+c}-1}{q^c-1}\right) [\mathcal{O}(m)^{\oplus(a+b)}]$ *for every* $m \in \mathbf{Z}$ *and* $a, b \in \mathbf{N}$.

(ii) If $\mathcal{F} = \mathcal{O}(n_1) \oplus \cdots \oplus \mathcal{O}(n_r)$ *is a locally free sheaf, if* $m \in \mathbf{Z}$ *is strictly greater than* $n_1, \ldots, n_r$*, and if* a *is a non-negative integer, then* $[\mathcal{F}][\mathcal{O}(m)^{\oplus a}] = [\mathcal{F} \oplus \mathcal{O}(m)^{\oplus a}]$.

(iii) If $m < n$*, then*

$$[\mathcal{O}(n)][\mathcal{O}(m)] = q^{n-m+1}[\mathcal{O}(m) \oplus \mathcal{O}(n)] + \sum_{a=1}^{\lfloor (n-m)/2 \rfloor} (q^2 - 1) \, q^{n-m-1} \, [\mathcal{O}(m + a) \oplus \mathcal{O}(n - a)].$$

(iv) If $\mathcal{F}$ *is a locally free sheaf and* $\mathcal{G}$ *is a torsion sheaf, then* $[\mathcal{F}][\mathcal{G}] = [\mathcal{F} \oplus \mathcal{G}]$.

(v) If $\mathcal{F}$ *and* $\mathcal{G}$ *are torsion sheaves with disjoint supports, then* $[\mathcal{F}][\mathcal{G}] = [\mathcal{F} \oplus \mathcal{G}]$.

(vi) If x *is a closed point,* r *is a positive integer, and* $n \in \mathbf{Z}$*, then*

$$[\mathcal{O}_{(1^r)[x]}][\mathcal{O}(n)] = [\mathcal{O}(n + \deg x) \oplus \mathcal{O}_{(1^{r-1})[x]}] + q_x^r \, [\mathcal{O}(n) \oplus \mathcal{O}_{(1^r)[x]}].$$

Proof. (i) Since the extension group $\mathrm{Ext}^1_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(m))$ vanishes by Corollary 6, any short exact sequence of the form

$$0 \longrightarrow \mathcal{O}(m)^{\oplus b} \longrightarrow \mathcal{F} \longrightarrow \mathcal{O}(m)^{\oplus a} \longrightarrow 0$$

necessarily splits, and the product $[\mathcal{O}(m)^{\oplus a}][\mathcal{O}(m)^{\oplus b}]$ in $H(\mathcal{A})$ is a scalar multiple of $[\mathcal{O}(m)^{\oplus(a+b)}]$. It remains to compute the corresponding Hall number. Since $\mathrm{End}_{\mathcal{A}}(\mathcal{O}(m)) \simeq \mathbf{F}_q$ by Lemma 4 (ii), this Hall number is equal to the number of vector subspaces of dimension b in a vector space of dimension $a + b$ over $\mathbf{F}_q$, namely to $\left(\prod_{c=1}^{a} \frac{q^{b+c}-1}{q^c-1}\right)$.

(ii) By Corollary 6, the extension groups $\mathrm{Ext}^1_{\mathcal{A}}(\mathcal{O}(n_i), \mathcal{O}(m))$ vanish. Thus any short exact sequence of the form

$$0 \longrightarrow \mathcal{O}(m)^{\oplus a} \xrightarrow{f} \mathcal{G} \longrightarrow \mathcal{F} \longrightarrow 0$$

splits, and the product $[\mathcal{F}][\mathcal{O}(m)^{\oplus a}]$ in $H(\mathcal{A})$ is a scalar multiple of $[\mathcal{F} \oplus \mathcal{O}(m)^{\oplus a}]$. Let us put $\mathcal{G} = \mathcal{F} \oplus \mathcal{O}(m)^{\oplus a}$ in the above short exact sequence, and write $f = h \oplus i$ according to this decomposition. Then $h = 0$, because all spaces $\mathrm{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n_i))$ vanish by Lemma 4 (iii). It follows that i is an automorphism. The number of suitable embeddings $f : \mathcal{O}(m)^{\oplus a} \to \mathcal{G}$ is therefore equal to $|\mathrm{Aut}_{\mathcal{A}}(\mathcal{O}(m)^{\oplus a})|$, and the Hall number we are looking for is equal to 1.

(iii) By Proposition 5, any short exact sequence of the form

$$0 \longrightarrow \mathcal{O}(m) \xrightarrow{f} \mathcal{F} \xrightarrow{g} \mathcal{O}(n) \longrightarrow 0$$

either splits, in which case $\mathcal{F} \simeq \mathcal{O}(m) \oplus \mathcal{O}(n)$, or there exists $1 \leq a \leq \lfloor (n-m)/2 \rfloor$ such that $\mathcal{F} \simeq \mathcal{O}(m+a) \oplus \mathcal{O}(n-a)$.

In the first case, we write $f = h \oplus i$ and $g = j \oplus \ell$, where $h \in \mathrm{End}_{\mathcal{A}}(\mathcal{O}(m))$, $i, j \in \mathrm{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))$, and $\ell \in \mathrm{End}_{\mathcal{A}}(\mathcal{O}(n))$. Since $\mathrm{Hom}_{\mathcal{A}}(\mathcal{O}(n), \mathcal{O}(m)) = 0$ by Lemma 4 (iii), the existence of a left inverse of f requires that h should be an automorphism. Similarly, ℓ is an automorphism. The map i may be arbitrarily chosen and then the map j should be equal to $-\ell \circ i \circ h^{-1}$. Thus the set of suitable pairs (f, g) is in one-to-one correspondence with $\mathrm{Aut}_{\mathcal{A}}(\mathcal{O}(m)) \times \mathrm{Aut}_{\mathcal{A}}(\mathcal{O}(n)) \times \mathrm{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))$, and the desired Hall number is $|\mathrm{Hom}_{\mathcal{A}}(\mathcal{O}(m), \mathcal{O}(n))| = q^{n-m+1}$. This yields the term $q^{n-m+1}[\mathcal{O}(m) \oplus \mathcal{O}(n)]$ in the Hall product.

In the second case, the number of epimorphisms $g : \mathcal{F} \to \mathcal{O}(n)$ such that $\ker g \simeq \mathcal{O}(m)$ is $(q-1)(q^2-1)q^{n-m-1}$ by Proposition 5 and Lemma 9. Since $|\mathrm{Aut}_{\mathcal{A}}(\mathcal{O}(n))| = q - 1$, the Hall number $\phi^{[\mathcal{F}]}_{[\mathcal{O}(n)],[\mathcal{O}(m)]}$ is $(q^2-1)q^{n-m-1}$, whence the term $(q^2-1)\, q^{n-m-1}\, [\mathcal{O}(m+a) \oplus \mathcal{O}(n-a)]$ in the Hall product.

(iv) and (v) These items follow from the vanishing of both $\mathrm{Ext}^1_{\mathcal{A}}(\mathcal{F}, \mathcal{G})$ and $\mathrm{Hom}_{\mathcal{A}}(\mathcal{G}, \mathcal{F})$ (see Proposition 2 (ii) and (iii)), as in the reasoning used to prove (ii).

(vi) This follows from Proposition 2 (ii), Lemma 4 (iv), Lemma 7, and Proposition 8, with the same reasoning as for (iii).
□

Application 11. Let x be a closed point of $\mathbf{P}^1(\mathbf{F}_q)$ and let $n \in \mathbf{Z}$. Using the relations in Theorem 10 and the associativity of the Hall product, one obtains after some calculations

$$\begin{aligned}
[\mathcal{O}_{[x]}][\mathcal{O}(n)^{\oplus 2}] = q_x[\mathcal{O}(n) \oplus \mathcal{O}(n + \deg x)] \\
+ q_x \left(1 - \frac{1}{q}\right) \sum_{a=1}^{\lfloor (\deg x)/2 \rfloor} [\mathcal{O}(n+a) \oplus \mathcal{O}(n + \deg x - a)] + q_x[\mathcal{O}(n)^{\oplus 2} \oplus \mathcal{O}_{[x]}].
\end{aligned}$$

In particular, if $\deg x \geq 2$, then the Hall number $\phi^{[\mathcal{O}(n+a) \oplus \mathcal{O}(n+\deg x - a)]}_{[\mathcal{O}_{[x]}],[\mathcal{O}(n)^{\oplus 2}]}$ is equal to $q^{\deg x - 1}(q-1)$ for each $1 \leq a \leq \deg x - 1$. By an analysis similar to those of Propositions 5 and 8, one may deduce from this the following fact, which we found not easy to prove directly:

If $P \in \mathbf{F}_q[T]$ is an irreducible polynomial of degree $d \geq 2$ and if $1 \leq a \leq d-1$, then there are exactly $q^{d-1}(q-1)^2$ quadruples $(H, I, J, L) \in \mathbf{F}_q[T]^4$ consisting of polynomials of degree a, $d-a$, $a-1$, $d-a-1$, respectively, such that $HI - JL = P$.

3.2 The Hall subalgebras $H(\mathcal{A}_{\{x\}})$ and $H(\mathcal{A}_{\mathrm{tor}})$

The information provided by Theorem 10 is not sufficient to compute all products in $H(\mathcal{A})$. For instance, the elements $[\mathcal{O}_{r[x]}]$ do not appear in its statement. More generally, it remains to understand how one can express the elements $[\mathcal{O}_{\lambda[x]}]$ in terms of the elements $[\mathcal{O}_{(1^r)[x]}]$.

Let us fix a closed point x of $\mathbf{P}^1(\mathbf{F}_q)$. The subcategory $\mathcal{A}_{\{x\}}$ of $\mathcal{A}$ is k-linear, abelian, and satisfies Conditions (H1)–(H3) of Section 1.1. We can therefore consider the Hall algebra $H(\mathcal{A}_{\{x\}})$. Since the category $\mathcal{A}_{\{x\}}$ is closed under extensions in $\mathcal{A}$, the algebra $H(\mathcal{A}_{\{x\}})$ can be viewed as the subalgebra of $H(\mathcal{A})$ spanned over $\widetilde{\mathbf{Z}}$ by the isomorphism classes of objects in $\mathcal{A}_{\{x\}}$. Note that there is no difference between the Hall product $\cdot$ and the Ringel product $*$ on $H(\mathcal{A}_{\{x\}})$ since the Euler form vanishes on $K(\mathcal{A}_{\{x\}})$ by Proposition 3.

To simplify the notation, we will set $\widehat{h}_{r,x} = \sum_{|\lambda|=r}[\mathcal{O}_{\lambda[x]}]$, where the sum runs over all partitions of weight r. The ring of symmetric polynomials over the ground ring $\widetilde{\mathbf{Z}} = \mathbf{Z}[v, v^{-1}]/(v^2 - q)$ in a countable infinite set of indeterminates will be denoted by Λ. We will follow the notations of [14] and denote the complete symmetric functions, the elementary symmetric functions, and the Hall-Littlewood polynomials by $h_r \in \Lambda$, $e_r \in \Lambda$, and $P_\lambda(t) \in \Lambda[t]$, respectively (see Sections I.2 and III.2 in op. cit.). The next statement shows in particular that the algebra $H(\mathcal{A}_{\{x\}})$ is commutative.

Proposition 12 ([13], Proposition 2.3.5)

(i) There is a ring isomorphism $\Psi_x : H(\mathcal{A}_{\{x\}}) \to \Lambda$ that sends the elements $\widehat{h}_{r,x}$, $[\mathcal{O}_{(1^r)[x]}]$, and $[\mathcal{O}_{\lambda[x]}]$ of $H(\mathcal{A}_{\{x\}})$, respectively, to the elements h_r, $q_x^{-r(r-1)/2}e_r$ and $q_x^{-n(\lambda)}P_\lambda(q_x^{-1})$ of Λ, respectively, for any integer $r \geq 1$ and any partition λ.

(ii) The $\widetilde{\mathbf{Z}}$-algebra $H(\mathcal{A}_{\{x\}})$ is a polynomial algebra on the set $\{\widehat{h}_{r,x} \mid r \geq 1\}$, as well as on the set $\{[\mathcal{O}_{(1^r)[x]}] \mid r \geq 1\}$. The family $([\mathcal{O}_{r[x]}])_{r\geq 1}$ consists of algebraically independent elements and generates the $\mathbf{Q}[v]/(v^2-q)$-algebra $H(\mathcal{A}_{\{x\}}) \otimes_{\mathbf{Z}} \mathbf{Q}$.

Proof. The isomorphism between the category $\mathcal{A}_{\{x\}}$ and the category of $\mathcal{O}_{\mathbf{P}^1(\mathbf{F}_q),x}$-modules of finite length gives rise to an isomorphism between their Hall algebras. Thus $H(\mathcal{A}_{\{x\}})$ is isomorphic to the Hall algebra studied in Chapters II and III of [14]. Assertion (i) therefore follows from Paragraphs III (3.4), III.3 Example 1 (2), III.4 Example 1, and III (2.8) in op. cit.

It is well-known that Λ is the $\widetilde{\mathbf{Z}}$-algebra of polynomials either in the complete symmetric functions h_r or in the elementary symmetric functions e_r, for $r \geq 1$ (see Statements I (2.4) and I (2.8) in op. cit.). This fact implies the first assertion in Statement (ii). The second one follows from Statement III (2.16) in op. cit. and its proof. □

We now define three generating functions in $H(\mathcal{A}_{\{x\}})[[s]]$ by

$$\widehat{H}_x(s) = 1 + \sum_{r\geq 1} \widehat{h}_{r,x}\, s^r = \sum_{\beta\in \mathrm{Iso}(\mathcal{A}_{\{x\}})} \beta\, s^{\deg\beta/\deg x},$$
$$\widehat{E}_x(s) = 1 + \sum_{r\geq 1} q_x^{r(r-1)/2}\, [\mathcal{O}_{(1^r)[x]}]\, s^r,$$
$$\widehat{Q}_x(s) = 1 + \sum_{r\geq 1} (1-q_x^{-1})\, v^{r\deg x}\, [\mathcal{O}_{r[x]}]\, s^r.$$

Lemma 13 *(i) The following relations hold in $H(\mathcal{A}_{\{x\}})[[s]]$:*

$$\widehat{H}_x(s)\, \widehat{E}_x(-s) = 1 \quad \textit{and} \quad \widehat{Q}_x(s) = \frac{\widehat{H}_x(s\, v^{\deg x})}{\widehat{H}_x(s/v^{\deg x})}.$$

(ii) In $H(\mathcal{A}_{\{x\}})[[s]]$, one has

$$\widehat{Q}_x(s) = \sum_{r\geq 0} \left|\mathrm{Aut}_{\mathcal{A}}(\mathcal{O}_{r[x]})\right|\, v^{-r\deg x}\, [\mathcal{O}_{r[x]}]\, s^r.$$

Proof. Following Paragraphs I (2.2) and I (2.5) of [14], we define generating series in $\Lambda[[s]]$ by

$$H(s) = 1 + \sum_{r\geq 1} h_r\, s^r \qquad \text{and} \qquad E(s) = 1 + \sum_{r\geq 1} e_r\, s^r.$$

By Formulae I (2.6) and III (2.10) in op. cit., we have in $\Lambda[[s]]$

$$H(s)E(-s) = 1 \quad \text{and} \quad 1 + \sum_{r\geq 1}(1-q_x^{-1})\, (s\, v^{\deg x})^r\, P_{(r)}(q_x^{-1}) = \frac{H(s\, v^{\deg x})}{H(s\, v^{\deg x}/q_x)}.$$

Taking the inverse images by Ψ_x, one obtains the relations in Assertion (i). As for Assertion (ii), it follows from the equality $\left|\mathrm{Aut}_{\mathcal{A}}(\mathcal{O}_{r[x]})\right| = q_x^r(1-q_x^{-1})$, valid for any $r \geq 1$ (use Formula II (1.6) of [14]). $\square$

Remark 14. The category $\mathcal{A}_{\{x\}}$ satisfying Condition (H4), the algebra $H(\mathcal{A}_{\{x\}})$ has the structure of a twisted Ringel-Green bialgebra. Since the Euler form on $K(\mathcal{A}_{\{x\}})$ vanishes, the twist in the multiplication law on $H(\mathcal{A}_{\{x\}}) \otimes_{\widetilde{\mathbf{Z}}} H(\mathcal{A}_{\{x\}})$ is trivial, so that $H(\mathcal{A}_{\{x\}})$ is a $\widetilde{\mathbf{Z}}$-bialgebra in the usual sense. (This fact is due to Zelevinsky, see [8], p. 362; moreover, $H(\mathcal{A}_{\{x\}})$ has an antipode.) Now, Λ is also a $\widetilde{\mathbf{Z}}$-bialgebra (see Example 25 in Section I.5 of [14]). We claim that the isomorphism Ψ_x defined in Proposition 12 preserves the coalgebra structures. To prove this, it suffices to compare the behaviour of the coproduct of $H(\mathcal{A}_{\{x\}})$ on the generators $\widehat{h}_{r,x}$ with the behaviour of the coproduct of Λ on their images $\Psi_x(\widehat{h}_{r,x}) = h_r$. Using the definition of the coproduct in Section 1.3 and Proposition 1 (vi), we perform the following computation in $(H(\mathcal{A}_{\{x\}}) \otimes_{\widetilde{\mathbf{Z}}} H(\mathcal{A}_{\{x\}}))[[s^{\deg x}]]$:

$$
\begin{aligned}
\Delta(\widehat{H}_x(s^{\deg x})) &= \sum_{\beta \in \mathrm{Iso}(\mathcal{A}_{\{x\}})} s^{\deg \beta}\, \Delta(\beta) \\
&= \sum_{\alpha,\beta,\gamma \in \mathrm{Iso}(\mathcal{A}_{\{x\}})} s^{\deg \beta}\, \frac{g_\alpha g_\gamma}{g_\beta}\, \phi^\beta_{\alpha\gamma}\, (\alpha \otimes \gamma) \\
&= \sum_{\alpha,\gamma \in \mathrm{Iso}(\mathcal{A}_{\{x\}})} \left(\sum_\beta \frac{g_\alpha g_\gamma}{g_\beta}\, \phi^\beta_{\alpha\gamma} \right) (s^{\deg \alpha}\alpha) \otimes (s^{\deg \gamma}\gamma) \\
&= \sum_{\alpha,\gamma \in \mathrm{Iso}(\mathcal{A}_{\{x\}})} (s^{\deg \alpha}\alpha) \otimes (s^{\deg \gamma}\gamma) \\
&= \widehat{H}_x(s^{\deg x}) \otimes \widehat{H}_x(s^{\deg x}). \qquad (2)
\end{aligned}
$$

Therefore $\Delta(\widehat{h}_{r,x}) = \sum_{s=0}^r \widehat{h}_{s,x} \otimes \widehat{h}_{r-s,x}$ in $H(\mathcal{A}_{\{x\}}) \otimes_{\widetilde{\mathbf{Z}}} H(\mathcal{A}_{\{x\}})$. A similar formula holds for the images of the complete symmetric functions h_r by the coproduct of Λ (see loc. cit.), and our claim follows.

We now turn to the subcategory $\mathcal{A}_{\mathrm{tor}}$ of $\mathcal{A}$ consisting of all torsion sheaves. The Hall algebra $H(\mathcal{A}_{\mathrm{tor}})$ may be viewed as the subspace of $H(\mathcal{A})$ spanned by the isomorphism classes of objects in $\mathcal{A}_{\mathrm{tor}}$. By Proposition 2 (v) the category $\mathcal{A}_{\mathrm{tor}}$ is the direct sum of the categories $\mathcal{A}_{\{x\}}$, so the Hall algebra $H(\mathcal{A}_{\mathrm{tor}})$ is canonically isomorphic to the tensor product over $\widetilde{\mathbf{Z}}$ of the Hall algebras $H(\mathcal{A}_{\{x\}})$ (this is Proposition 2.3.5 (a) in [13]). We also note that the Hall product $\cdot$ and the Ringel product $*$ coincide on $H(\mathcal{A}_{\mathrm{tor}})$ because the Euler form vanishes on $K(\mathcal{A}_{\mathrm{tor}})$ by Proposition 3.

We define elements $\widehat{h}_r$, $\widehat{e}_r$, and $\widehat{q}_r$ of $H(\mathcal{A}_{\mathrm{tor}})$ for $r \geq 1$ by means of the generating functions

$$
\begin{aligned}
\widehat{H}(s) &= 1 + \sum_{r\geq 1} \widehat{h}_r s^r = \prod_{x \in \mathbf{P}^1(\mathbf{F}_q)} \widehat{H}_x(s^{\deg x}), \qquad (3)\\
\widehat{E}(s) &= 1 + \sum_{r\geq 1} \widehat{e}_r s^r = \prod_{x \in \mathbf{P}^1(\mathbf{F}_q)} \widehat{E}_x(-s^{\deg x}),\\
\widehat{Q}(s) &= 1 + \sum_{r\geq 1} \widehat{q}_r s^r = \prod_{x \in \mathbf{P}^1(\mathbf{F}_q)} \widehat{Q}_x(s^{\deg x}).
\end{aligned}
$$

These equalities are meant to hold in $H(\mathcal{A}_{\mathrm{tor}})[[s]]$; in the right-hand side of the above equations, the products are over the set of all closed points of $\mathbf{P}^1(\mathbf{F}_q)$.

Lemma 15 *(i) One has the relations*

$$
\widehat{H}(s)\, \widehat{E}(s) = 1 \quad \textit{and} \quad \widehat{Q}(s) = \frac{\widehat{H}(sv)}{\widehat{H}(s/v)},
$$

or equivalently, for each $r \geq 1$,

$$\widehat{h}_r + \sum_{s=1}^{r-1} \widehat{h}_s \, \widehat{e}_{r-s} + \widehat{e}_r = 0,$$

$$(q^r - 1) \, \widehat{h}_r = v^r \widehat{q}_r + \sum_{s=1}^{r-1} v^{r-s} \, \widehat{h}_s \, \widehat{q}_{r-s}.$$

(ii) The three families $(\widehat{h}_r)_{r\geq 1}$, $(\widehat{e}_r)_{r\geq 1}$, and $(\widehat{q}_r)_{r\geq 1}$ consist of algebraically independent elements.

Proof. Assertion (i) follows from Lemma 13 (i). Let Γ be the subalgebra of $H(\mathcal{A}_{\mathrm{tor}})$ generated by the subalgebras $H(\mathcal{A}_{\{x\}})$ with $x \neq \infty$. Then $H(\mathcal{A}_{\mathrm{tor}})$ is the algebra of polynomials in the indeterminates $\widehat{h}_{r,\infty}$ with coefficients in Γ. It is easy to see that $\widehat{h}_r - \widehat{h}_{r,\infty}$ belongs to $\Gamma[\widehat{h}_{1,\infty}, \cdots, \widehat{h}_{r-1,\infty}]$, which proves the algebraic independence of the elements $\widehat{h}_r$. The algebraic independence of the other two families can then be deduced from Assertion (i), which completes the proof of Assertion (ii). □

3.3 A subalgebra of $H(\mathcal{A})$

The Ringel algebra $H(\mathcal{A})$ turns out to be made of two parts: the first one is the Ringel algebra $H(\mathcal{A}_{\mathrm{tor}})$ described in Section 3.2, while the second one is a certain subalgebra B_1 related to locally free sheaves. In this section, we explain this decomposition and use it to define a subalgebra B of $H(\mathcal{A})$ which will be related in Section 4 to the quantum affine algebra $U_q(\widehat{\mathfrak{sl}_2})$.

It will be necessary for us to extend the ground ring of the Ringel algebra $H(\mathcal{A})$ and of certain $\widetilde{\mathbf{Z}}$-submodules B of it from $\widetilde{\mathbf{Z}}$ to a $\widetilde{\mathbf{Z}}$-algebra R. The R-module $B \otimes_{\widetilde{\mathbf{Z}}} R$ will be denoted by $B_{(R)}$.

We first define the q-numbers, setting as usual $[a] = (v^a - v^{-a})/(v - v^{-1})$ for $a \in \mathbf{Z}$. We set $[a]! = \prod_{i=1}^{a} [i]$ for $a \geq 1$, and agree that $[0]! = 1$. Remark that each $[a]$ or $[a]!$ is a product of a non-zero integer by a power of v.

We next record the following consequence of Theorem 10 and of Proposition 3.

Lemma 16 *(i) For all $m, n \in \mathbf{Z}$, one has*

$$[\mathcal{O}(m+1)] * [\mathcal{O}(n)] - v^2 \, [\mathcal{O}(n)] * [\mathcal{O}(m+1)] = \\ v^2 \, [\mathcal{O}(m)] * [\mathcal{O}(n+1)] - [\mathcal{O}(n+1)] * [\mathcal{O}(m)]. \quad (4)$$

(ii) If $n_1 < \cdots < n_r$ is an increasing sequence of integers and if $c_1, \ldots, c_r$ is a sequence of positive integers, then one has

$$[\mathcal{O}(n_1)]^{*c_1} * \cdots * [\mathcal{O}(n_r)]^{*c_r} = \left(\prod_{i=1}^{r} q^{c_i(c_i-1)/2} [c_i]! \right) v^{\sum_{1\leq i<j\leq r} (n_j - n_i + 1) c_i c_j} \left[\bigoplus_{i=1}^{r} \mathcal{O}(n_i)^{\oplus c_i} \right].$$

Proof. Assertion (i) can be proved by a tedious case by case examination, using Relations (i)–(iii) in Theorem 10 and Proposition 3. To prove Assertion (ii), one first computes

$$\begin{aligned}[\mathcal{O}(n_i)]^{*c_i} &= v^{c_i(c_i-1)/2}\,[\mathcal{O}(n_i)]^{c_i} \\ &= v^{c_i(c_i-1)/2}\left(\prod_{a=1}^{c_i}\frac{q^a-1}{q-1}\right)[\mathcal{O}(n_i)^{\oplus c_i}] \\ &= q^{c_i(c_i-1)/2}\,[c_i]!\,[\mathcal{O}(n_i)^{\oplus c_i}],\end{aligned}$$

using Theorem 10 (i), and then

$$\begin{aligned}&[\mathcal{O}(n_1)]^{*c_1}*\cdots*[\mathcal{O}(n_r)]^{*c_r} \\ &\quad= v^{\sum_{1\le i<j\le r}(n_j-n_i+1)c_ic_j}\,[\mathcal{O}(n_1)]^{*c_1}\cdots[\mathcal{O}(n_r)]^{*c_r} \\ &\quad= \left(\prod_{i=1}^{r}q^{c_i(c_i-1)/2}[c_i]!\right)v^{\sum_{1\le i<j\le r}(n_j-n_i+1)c_ic_j}\,[\mathcal{O}(n_1)^{\oplus c_1}]\cdots[\mathcal{O}(n_r)^{\oplus c_r}] \\ &\quad= \left(\prod_{i=1}^{r}q^{c_i(c_i-1)/2}[c_i]!\right)v^{\sum_{1\le i<j\le r}(n_j-n_i+1)c_ic_j}\left[\bigoplus_{i=1}^{r}\mathcal{O}(n_i)^{\oplus c_i}\right],\end{aligned}$$

using Theorem 10 (ii). □

We now need two other pieces of notation. We denote by C the set of all sequences of non-negative integers $\underline{c}=(c_n)_{n\in\mathbf{Z}}$ that have only finitely many non-zero terms, and for $\underline{c}\in C$, we set

$$X_{\underline{c}}=\prod_{n\in\mathbf{Z}}[\mathcal{O}(n)]^{*c_n},$$

the products being computed using the multiplication $*$ and the ascending order on $\mathbf{Z}$. We denote the $\widetilde{\mathbf{Z}}$-submodule of $H(\mathcal{A})$ spanned by the isomorphism classes of locally free sheaves by B_1.

Proposition 17 *(i) B_1 is a subalgebra of $H(\mathcal{A})$.*

(ii) If R is a $\widetilde{\mathbf{Z}}$-algebra containing $\mathbf{Q}$, then the family $(X_{\underline{c}})_{c\in C}$ is a basis of the R-module $(B_1)_{(R)}$.

(iii) The multiplication in the Ringel algebra $H(\mathcal{A})$ induces an isomorphism of $\widetilde{\mathbf{Z}}$-modules from $B_1\otimes_{\widetilde{\mathbf{Z}}}H(\mathcal{A}_{\mathrm{tor}})$ onto $H(\mathcal{A})$.

Proof. Assertion (i) comes from the fact that $\mathcal{A}_{\mathrm{lf}}$ is a subcategory of $\mathcal{A}$ closed under extensions (Proposition 2 (i)) and from the definition of the product $*$ in $H(\mathcal{A})$. Assertion (ii) follows from Lemma 16 (ii). Proposition 2 (iv) says that any coherent sheaf $\mathcal{F}$ is isomorphic to the direct sum of a torsion coherent sheaf $\mathcal{F}_0$ and a locally free sheaf $\mathcal{F}_1$, and since $\mathcal{A}$ satisfies the Krull-Schmidt property, the isomorphism class of $\mathcal{F}$ determines those of $\mathcal{F}_0$ and $\mathcal{F}_1$. Together with Theorem 10 (iv), this proves Assertion (iii). □

Remark 18. As mentioned in Section 3.2, the subalgebra $H(\mathcal{A}_{\rm tor})$ of $H(\mathcal{A})$ is a Hopf algebra. Let us adopt Sweedler's notation and denote the image of an element $a \in H(\mathcal{A}_{\rm tor})$ under the coproduct by $\Delta(a) = \sum_{(a)} a_{(1)} \otimes a_{(2)}$. The Hopf algebra $H(\mathcal{A}_{\rm tor})$ acts on $H(\mathcal{A})$ through the adjoint representation, which is the homomorphism ad : $H(\mathcal{A}_{\rm tor}) \to \mathrm{End}_{\widetilde{\mathbf{Z}}}(H(\mathcal{A}))$ defined by

$$a * x = \sum_{(a)} \big(\mathrm{ad}(a_{(1)}) \cdot x\big) * a_{(2)},$$

for all $a \in H(\mathcal{A}_{\rm tor})$ and $x \in H(\mathcal{A})$. Relating the adjoint action to Hecke operators, Kapranov has shown that B_1 is a $H(\mathcal{A}_{\rm tor})$-submodule of $H(\mathcal{A})$ (see Proposition 4.1.1 in [13]). Assertion (iii) of Proposition 17 can then be interpreted, in the language of Hopf algebras, as stating that $H(\mathcal{A})$ is the smash product of the Hopf algebra $H(\mathcal{A}_{\rm tor})$ by the $H(\mathcal{A}_{\rm tor})$-module algebra B_1.

The following result gives a commutation relation between certain elements of B_1 and certain elements of $H(\mathcal{A}_{\rm tor})$.

Lemma 19 *For $n \in \mathbf{Z}$ and $r \geq 1$, one has*

$$\widehat{h}_r * [\mathcal{O}(n)] = [r+1]\ [\mathcal{O}(n+r)]\ +\ \sum_{s=0}^{r-1} [s+1]\ [\mathcal{O}(n+s)] * \widehat{h}_{r-s}. \tag{5}$$

Proof. We will use the generating series $\widehat{E}_x(s)$ and $\widehat{H}(s)$. We set

$$X(t) = \sum_{n \in \mathbf{Z}} [\mathcal{O}(n)]\ t^n$$

and compute, using Relations (iv) and (vi) in Theorem 10:

$$\begin{aligned}
\widehat{E}_x(-s^{\deg x}) * X(t) &= \sum_{n\in\mathbf{Z},\ r\geq 0} (-1)^r\ s^{r \deg x}\ t^n\ q_x^{r(r-1)/2}\ [\mathcal{O}_{(1^r)[x]}] * [\mathcal{O}(n)] \\
&= \sum_{n\in\mathbf{Z},\ r\geq 0} (-1)^r\ s^{r \deg x}\ t^n\ q_x^{r(r-1)/2} \\
&\qquad \times \Big([\mathcal{O}(n)] * [\mathcal{O}_{(1^r)[x]}] + v^{(1-2r)\deg x}\ [\mathcal{O}(n+\deg x)] * [\mathcal{O}_{(1^{r-1})[x]}]\Big) \\
&= X(t) * \widehat{E}_x(-s^{\deg x})\ \Big(1 - (s/tv)^{\deg x}\Big).
\end{aligned}$$

In view of Formula (3) and Lemma 13 (i), we therefore have

$$\widehat{H}(s) * X(t) = X(t) * \widehat{H}(s) \prod_{x \in \mathbf{P}^1(\mathbf{F}_q)} \frac{1}{1-(s/tv)^{\deg x}},$$

after expansion of the rational functions $1/(1-(s/tv)^{\deg x})$ in powers of s/tv.

Now in the formal power series ring $\mathbf{Z}[[s]]$, one has

$$\prod_{x \in \mathbf{P}^1(\mathbf{F}_q)} \frac{1}{1-s^{\deg x}} = \frac{1}{(1-s)(1-qs)},$$

where the product in the left hand side runs over all closed points of $\mathbf{P}^1(\mathbf{F}_q)$. The previous equality follows from the calculation of the zeta function of $\mathbf{P}^1(\mathbf{F}_q)$ (see Section C.1 of [11] for a proof). Therefore,

$$\widehat{H}(s) * X(t) = X(t) * \widehat{H}(s)\ \frac{1}{(1-s/tv)(1-sv/t)}, \tag{6}$$

which is equivalent to our assertion. □

Remark 20. Lemma 13 (ii) shows that the elements $\psi_r \in H(\mathcal{A}_{\mathrm{tor}})$ defined in Formula (5.2) of [13] satisfy

$$\widehat{Q}(s) = 1 + \sum_{r\geq 1} v^{-r}\, \psi_r\, s^r.$$

On the other hand, using Relation (6) above and Lemma 15 (i), one obtains

$$\widehat{Q}(s) * X(t) = X(t) * \widehat{Q}(s)\ \frac{1-s/tq}{1-sq/t}.$$

We thus recover Formula (5.2.5) in [13].

Finally, let B_0 be the subalgebra of $H(\mathcal{A}_{\mathrm{tor}})$ generated by the family $(\widehat{h}_r)_{r\geq 1}$, and let B be the subalgebra of the Ringel algebra $H(\mathcal{A})$ generated by B_0 and B_1. Let also D be the set of all sequences of non-negative integers $\underline{d} = (d_r)_{r\geq 1}$ that have only finitely many non-zero terms, and for $d \in D$, set

$$\widehat{h}_{\underline{d}} = \prod_{r\geq 1} \widehat{h}_r^{d_r}, \quad \widehat{e}_{\underline{d}} = \prod_{r\geq 1} \widehat{e}_r^{d_r}, \quad \text{and} \quad \widehat{q}_{\underline{d}} = \prod_{r\geq 1} \widehat{q}_r^{d_r}.$$

Proposition 21 *Let R be a field of characteristic 0 which is also a $\widetilde{\mathbf{Z}}$-algebra.*

(i) The algebra $B_{(R)}$ is generated by the elements $[\mathcal{O}(n)]$ for $n \in \mathbf{Z}$ and the elements $\widehat{h}_r$ for $r \geq 1$.

(ii) The families $(X_{\underline{c}} * \widehat{h}_{\underline{d}})_{(\underline{c},\underline{d})\in C\times D}$, $(X_{\underline{c}} * \widehat{e}_{\underline{d}})_{(\underline{c},\underline{d})\in C\times D}$, and $(X_{\underline{c}} * \widehat{q}_{\underline{d}})_{(\underline{c},\underline{d})\in C\times D}$ are three bases of the R-module $B_{(R)}$.

Proof. Proposition 17 (iii) implies that the multiplication $*$ induces an isomorphism of $\widetilde{\mathbf{Z}}$-modules from $B_1 \otimes_{\widetilde{\mathbf{Z}}} B_0$ onto $B_1 * B_0$. Lemma 19 implies that $B_1 * B_0$ is a subalgebra of the Ringel algebra $H(\mathcal{A})$, obviously equal to B. Since the $\widetilde{\mathbf{Z}}$-modules B_0 and B_1 are free (see Lemma 15 (ii)), the multiplication $*$ in the Ringel algebra $H(\mathcal{A})_{(R)}$ induces an isomorphism of R-modules from $(B_1)_{(R)} \otimes_R (B_0)_{(R)}$ to $B_{(R)}$.

Lemma 15 shows that $(B_0)_{(R)}$ is a polynomial algebra on each of the three set of indeterminates: $\{\widehat{h}_r \mid r \geq 1\}$, $\{\widehat{e}_r \mid r \geq 1\}$, or $\{\widehat{q}_r \mid r \geq 1\}$. Thus the families $(\widehat{h}_{\underline{d}})_{\underline{d}\in D}$, $(\widehat{e}_{\underline{d}})_{\underline{d}\in D}$, and $(\widehat{q}_{\underline{d}})_{\underline{d}\in D}$ are three bases of the R-vector space $(B_0)_{(R)}$. Both assertions of our proposition follow now from Proposition 17 (ii). □

Remark 22. In view of Remark 18, the fact that B is a subalgebra of $H(\mathcal{A})$ should be considered as a consequence of the fact that B_0 is a sub-bialgebra of $H(\mathcal{A}_{\mathrm{tor}})$, itself a consequence of Formulae (2) and (3).

4 Link with the quantum affine algebra $U_q(\widehat{\mathfrak{sl}_2})$

Our aim now is to describe the relationship between the Hall algebra $H(\mathcal{A})$ investigated in Section 3 and the quantum affine algebra $U_q(\widehat{\mathfrak{sl}_2})$. In the original definitions of the latter, q is an indeterminate. It will however be more convenient for us to deal with a specialized version of $U_q(\widehat{\mathfrak{sl}_2})$, in which q is the number of elements of the finite field that we have chosen at the beginning of Section 3. We therefore fix for the remainder of this paper a field R of characteristic 0 together with a square root v of the number q.

In this section, we first recall the definition of the R-algebra $U_q(\widehat{\mathfrak{sl}_2})$ in its loop-like realization and define a certain subalgebra V^+ in it. We then present an elementary proof of Kapranov's result asserting that the R-algebra V^+ is isomorphic to the R-algebra $B_{(R)}$ defined in Section 3.3. We end with several comments, observing that Kapranov's approach to $U_q(\widehat{\mathfrak{sl}_2})$ sheds a new light on certain recent constructions by Beck, Chari, and Pressley [2].

4.1 Definition of $U_q(\widehat{\mathfrak{sl}_2})$

Following Drinfeld [7], we define $U_q(\widehat{\mathfrak{sl}_2})$ as the R-algebra generated by elements $K^{\pm 1}$, $C^{\pm 1/2}$, h_r, where $r \in \mathbf{Z} \setminus \{0\}$, and $x_n^{\pm}$, where $n \in \mathbf{Z}$, submitted to the relations

$$\begin{aligned}
&K\,K^{-1} = K^{-1}\,K = 1, && \\
&C^{1/2}\,C^{-1/2} = C^{-1/2}\,C^{1/2} = 1, && \\
&C^{1/2} \quad \text{is central}, && \\
&[K, h_r] = 0 && \text{for } r \in \mathbf{Z} \setminus \{0\}, \\
&K\,x_n^{\pm} = v^{\pm 2} x_n^{\pm}\,K && \text{for } n \in \mathbf{Z}, \\
&[h_r, h_s] = \delta_{r,-s}\,\frac{[2r]}{r}\,\frac{C^r - C^{-r}}{v - v^{-1}} && \text{for } r, s \in \mathbf{Z} \setminus \{0\}, \\
&[h_r, x_n^{\pm}] = \pm\frac{[2r]}{r}\,C^{\mp |r|/2} x_{n+r}^{\pm} && \text{for } n, r \in \mathbf{Z},\ r \neq 0, \\
&x_{m+1}^{\pm}\,x_n^{\pm} - v^{\pm 2} x_n^{\pm}\,x_{m+1}^{\pm} = v^{\pm 2} x_m^{\pm}\,x_{n+1}^{\pm} - x_{n+1}^{\pm}\,x_m^{\pm} && \text{for } m, n \in \mathbf{Z}, \\
&[x_m^+, x_n^-] = \frac{C^{(m-n)/2}\psi_{m+n}^+ - C^{(n-m)/2}\psi_{m+n}^-}{v - v^{-1}} && \text{for } m, n \in \mathbf{Z},
\end{aligned} \tag{7}$$

where the elements $\psi_{\pm r}^{\pm}$ are defined by the generating functions

$$\sum_{r \geq 0} \psi_{\pm r}^{\pm}\, s^{\pm r} = K^{\pm 1} \exp\left(\pm (v - v^{-1}) \sum_{r \geq 1} h_{\pm r}\, s^{\pm r} \right)$$

for $r \geq 0$ and are defined to be zero for $r \leq -1$.

Relying in part on previous work of Damiani [5], Beck [1] made precise the link between this definition and Drinfeld and Jimbo's original definition [6, 12] of $U_q(\widehat{\mathfrak{sl}_2})$ as the quantized enveloping algebra associated to the generalized Cartan matrix $\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$ of type $A_1^{(1)}$.

Let V^+ be the subalgebra of $U_q(\widehat{\mathfrak{sl}_2})$ generated by the elements x_n^+ and $h_r\,C^{r/2}$, for $n \in \mathbf{Z}$ and $r \geq 1$. The aim of Section 4 is to prove the following result.

Theorem 23 ([13], Theorem 5.2.1) *The R-algebras $B_{(R)}$ and V^+ are isomorphic.*

4.2 Structure of $U_q(\widehat{\mathfrak{sl}_2})$

Following Section 1 of [2], we define elements $\widetilde{\psi}^{\pm}_{\pm r}$ for $r \geq 1$ by

$$1 \pm \sum_{r\geq 1}(v - v^{-1})\,\widetilde{\psi}^{\pm}_{\pm r}\,s^{\pm r} \;=\; \exp\left(\pm(v-v^{-1})\sum_{r\geq 1} h_{\pm r}\,C^{\pm r/2}\,s^{\pm r}\right). \tag{8}$$

Let us denote by

- $N^{\pm}$ the subalgebra generated by the elements $x_n^{\pm}$, where $n \in \mathbf{Z}$;
- H the subalgebra generated by the elements $K^{\pm 1}$, $C^{\pm 1/2}$, and h_r, where $r \in \mathbf{Z} \setminus \{0\}$;
- $H^{\pm}$ the subalgebra generated by the elements $\widetilde{\psi}^{\pm}_{\pm r}$, where $r \geq 1$;
- H^0 the subalgebra generated by the elements $K^{\pm 1}$ and $C^{\pm 1/2}$.

Proposition 24

(i) The multiplication induces a linear isomorphism $N^- \otimes_R H \otimes_R N^+ \to U_q(\widehat{\mathfrak{sl}_2})$.

(ii) The multiplication induces a linear isomorphism $H^- \otimes_R H^0 \otimes_R H^+ \to H$.

(iii) The generators $\widetilde{\psi}^+_r$ $(r \geq 1)$ of the algebra H^+ are algebraically independent.

(iv) The family of products $\left(\prod_{n\in\mathbf{Z}}(x_n^+)^{c_n}\right)_{\underline{c}\in C}$, performed in the ascending order of $\mathbf{Z}$, is a basis of N^+.

Proof. It is asserted in Proposition 12.2.2 of [4] that the map $N^- \otimes_R H \otimes_R N^+ \to U_q(\widehat{\mathfrak{sl}_2})$ induced by the multiplication of $U_q(\widehat{\mathfrak{sl}_2})$ is surjective. The defining relations of $U_q(\widehat{\mathfrak{sl}_2})$ imply easily that the map $H^- \otimes_R H^0 \otimes_R H^+ \to H$ induced by the multiplication of $U_q(\widehat{\mathfrak{sl}_2})$ is also surjective. The algebra $H^{\pm}$ is generated by the pairwise commuting elements $\widetilde{\psi}^{\pm}_{\pm r}$ for $r \geq 1$, which shows that the monomials $\left(\prod_{r\geq 1}(\widetilde{\psi}^{\pm}_{\pm r})^{d_r}\right)$, for $\underline{d} \in D$, span the R-vector space $H^{\pm}$. Similarly, the family of elements $(K^a C^{b/2})_{(a,b)\in\mathbf{Z}^2}$ span the R-vector space H^0. Finally, an easy induction shows that the products $\left(\prod_{n\in\mathbf{Z}}(x^{\pm}_{\pm n})^{c_n}\right)$, performed in the ascending order of $\mathbf{Z}$ and for $\underline{c} \in C$, span the R-vector space $N^{\pm}$. Consequently, the elements

$$M(a,b,\underline{c}',\underline{c}'',\underline{d}',\underline{d}'') = \left(\prod_{n\in\mathbf{Z}}(x^-_{-n})^{c'_n}\right)\left(\prod_{r\geq 1}(\widetilde{\psi}^-_{-r})^{d'_r}\right)K^a C^{b/2}\left(\prod_{r\geq 1}(\widetilde{\psi}^+_{r})^{d''_r}\right)\left(\prod_{n\in\mathbf{Z}}(x^+_{n})^{c''_n}\right),$$

where $a, b \in \mathbf{Z}$, $\underline{c}', \underline{c}'' \in C$, and $\underline{d}', \underline{d}'' \in D$, span the R-vector space $U_q(\widehat{\mathfrak{sl}_2})$.

Now observe that the definition of $U_q(\widehat{\mathfrak{sl}_2})$ implies the existence of an automorphism T of the R-algebra $U_q(\widehat{\mathfrak{sl}_2})$ such that

$$T(x_n^{\pm}) = x_{n\mp 1}^{\pm}, \quad T(K^{\pm 1}) = K^{\pm 1}C^{\mp 1}, \quad T(C^{\pm 1/2}) = C^{\pm 1/2}, \quad T(h_r) = h_r,$$

for all $n, r \in \mathbf{Z}$ with $r \neq 0$. (Using Proposition 3.10.2 (b) and Definition 4.6 of [1], one can easily see that T is the automorphism of $U_q(\widehat{\mathfrak{sl}_2})$ that lifts the translation along the fundamental weight to the braid group of the extended affine Weyl group of $\mathfrak{sl}_2$.) On the other hand, observe, as a consequence of the Poincaré-Birkhoff-Witt theorem for $U_q(\widehat{\mathfrak{sl}_2})$ (Proposition 6.1 in [1]), that the set of elements

$$\left\{M(a, b, \underline{c}', \underline{c}'', \underline{d}', \underline{d}'') \;\middle|\; a, b \in \mathbf{Z},\ \underline{c}', \underline{c}'' \in C,\ \underline{d}', \underline{d}'' \in D,\ n < 0 \Rightarrow c'_n = c''_n = 0\right\}$$

is linearly independent over R. Using this and the automorphism T, one proves the linear independence over R of the family of elements $(M(a, b, \underline{c}', \underline{c}'', \underline{d}', \underline{d}''))_{(a,b,\underline{c}',\underline{c}'',\underline{d}',\underline{d}'')\in\mathbf{Z}^2\times C^2\times D^2}$.

This family is therefore a basis of $U_q(\widehat{\mathfrak{sl}_2})$, which entails simultaneously all the assertions of the lemma. □

Let us remark that the algebra H^+ is the subalgebra denoted by $\mathbf{U}^+(0)$ in [2] (see Proposition 1.3 (iii) of that paper for instance). Following Section 1 of [2], we now define elements $\widetilde{P}_r$ and P_r of H^+, for $r \geq 1$, by the following generating functions:

$$\widetilde{P}(s) = 1 + \sum_{r\geq 1} \widetilde{P}_r s^r \quad = \quad \exp\left(\sum_{r\geq 1} \frac{h_r\, C^{r/2}}{[r]}\, s^r\right), \tag{9}$$

$$P(s) = 1 + \sum_{r\geq 1} P_r s^r \quad = \quad \exp\left(-\sum_{r\geq 1} \frac{h_r\, C^{r/2}}{[r]}\, s^r\right). \tag{10}$$

For sequences $\underline{c} = (c_n)_{n\in\mathbf{Z}} \in C$ and $\underline{d} = (d_r)_{r\geq 1} \in D$, we define

$$x_{\underline{c}}^+ = \prod_{n\in\mathbf{Z}} (x_n^+)^{c_n}, \quad \widetilde{P}_{\underline{d}} = \prod_{r\geq 1} \widetilde{P}_r^{d_r}, \quad P_{\underline{d}} = \prod_{r\geq 1} P_r^{d_r}, \quad \text{and} \quad \widetilde{\psi}_{\underline{d}}^+ = \prod_{r\geq 1} (\widetilde{\psi}_r^+)^{d_r}.$$

Proposition 25 *(i) The algebra V^+ is generated by the elements x_n^+ and $\widetilde{P}_r$, for $n \in \mathbf{Z}$ and $r \geq 1$.*

(ii) The families $(x_{\underline{c}}^+ \widetilde{P}_{\underline{d}})_{(\underline{c},\underline{d})\in C\times D}$, $(x_{\underline{c}}^+ P_{\underline{d}})_{(\underline{c},\underline{d})\in C\times D}$, and $(x_{\underline{c}}^+ \widetilde{\psi}_{\underline{d}}^+)_{(\underline{c},\underline{d})\in C\times D}$ are three bases of the R-vector space V^+.

Proof. By definition, V^+ is the subalgebra of $U_q(\widehat{\mathfrak{sl}_2})$ generated by the elements x_n^+ and $h_r C^{r/2}$, for $n \in \mathbf{Z}$ and $r \geq 1$. Assertion (i) follows therefore from the definition of the elements $\widetilde{P}_r$ (Formula (9)) and from the fact that the scalars $[r]$ do not vanish in the field R for any $r \geq 1$.

Proposition 2.8 in [2] states that for all integers $n \geq 0$ and $r \geq 1$, one has

$$\widetilde{P}_r\, x_n^+ = [r+1]\, x_{n+r}^+ \; + \; \sum_{s=0}^{r-1} [s+1]\, x_{n+s}^+\, \widetilde{P}_{r-s}. \tag{11}$$

Applying a well-chosen power of the automorphism T defined in the proof of Proposition 24, one immediately sees that Formula (11) holds more generally for any $n \in \mathbf{Z}$. Together with Proposition 24 (i), this shows that the multiplication map induces a linear isomorphism from $N^+ \otimes_R H^+$ onto V^+.

By Formulae (1.8) and (1.9) in [2], we have the following relations in $H^+[[s]]$:

$$\widetilde{P}(s)\ P(s) = 1 \quad \text{and} \quad \frac{\widetilde{P}(sv)}{\widetilde{P}(s/v)} = 1 + \sum_{r\geq 1} (v - v^{-1})\ \widetilde{\psi}_r^+\ s^r,$$

or, equivalently, for each $r \geq 1$:

$$\widetilde{P}_r + \sum_{s=1}^{r-1} \widetilde{P}_s P_{r-s} + P_r = 0,$$

$$[r]\ \widetilde{P}_r = \widetilde{\psi}_r^+ + \sum_{s=1}^{r-1} v^{-s}\ \widetilde{P}_s\ \widetilde{\psi}_{r-s}^+.$$

Together with Assertion (iii) of Proposition 24, this implies that H^+ is a polynomial algebra on each of the three set of indeterminates: $\{\widetilde{\psi}_r \mid r \geq 1\}$, $\{\widetilde{P}_r \mid r \geq 1\}$, or $\{P_r \mid r \geq 1\}$. Thus the families $(\widetilde{P}_{\underline{d}})_{\underline{d}\in D}$, $(P_{\underline{d}})_{\underline{d}\in D}$, and $(\widetilde{\psi}_{\underline{d}}^+)_{\underline{d}\in D}$ are three bases of the R-vector space H^+. Assertion (ii) follows from this and from Proposition 24 (iv). $\square$

Theorem 23 is now evident. The isomorphism sends $[\mathcal{O}(n)]$ to x_n^+, $\widehat{h}_r$ to $\widetilde{P}_r$, $\widehat{e}_r$ to P_r, and $\widehat{q}_r$ to $(v - v^{-1})\widetilde{\psi}_r^+$, respectively. Relations (4) and (5) correspond to Relations (7) and (11).

4.3 Concluding remarks

As mentioned in the introduction, Ringel was the first one to discover relations between Hall algebras and quantized enveloping algebras. In [18] he noticed that, in his context, the natural basis of the Hall algebra corresponds to a Poincaré-Birkhoff-Witt type basis of Lusztig's integral form of the positive part of the quantized enveloping algebra. Here a similar phenomenon occurs:

- by Lemma 16 (ii), the element $[\mathcal{O}(n_1)^{\oplus c_1} \oplus \cdots \oplus \mathcal{O}(n_r)^{\oplus c_r}]$ of $H(\mathcal{A})$ is equal, up to a power of v, to the product of divided powers

$$\left(\frac{1}{[c_1]!}[\mathcal{O}(n_1)]^{*c_1}\right) * \cdots * \left(\frac{1}{[c_r]!}[\mathcal{O}(n_r)]^{*c_r}\right);$$

- by Lemma 2.3 in [2], the monomials in the $\widehat{h}_r$ for $r \geq 1$ correspond to the elements of a Poincaré-Birkhoff-Witt basis of Lusztig's integral form of H^+.

These observations are likely to be part of a more complete statement for which one would need a version of the Hall algebra $H(\mathcal{A})$ (or at least of the algebra B) with a generic parameter q as well as an integral version of Proposition 24.

The elements P_r, $\widetilde{P}_r$, and $\widetilde{\psi}_r$ play important rôles for $U_q(\widehat{\mathfrak{sl}_2})$, namely in the classification of the finite-dimensional simple $U_q(\widehat{\mathfrak{sl}_2})$-modules (see Theorem 12.2.6 in [4]) and in the construction of a Poincaré-Birkhoff-Witt basis of Lusztig's integral form of $U_q(\widehat{\mathfrak{sl}_2})$ (see Theorem 2 of [2]). The relations (8), (9), and (10) defining them, though explicit, look rather artificial. Kapranov's isomorphism $B_{(R)} \to V^+$ helps show where these elements come from: they are the standard generators of the algebra of symmetric polynomials (elementary symmetric functions, complete symmetric functions, Hall-Littlewood polynomials) carried over to the Hall algebras $H(\mathcal{A}_{\{x\}})$ and averaged over the closed points of $\mathbf{P}^1(\mathbf{F}_q)$.

References

[1] J. Beck, *Braid group action and quantum affine algebras*, Commun. Math. Phys. **165** (1994), 555–568.

[2] J. Beck, V. Chari, and A. Pressley, *An algebraic characterization of the affine canonical basis*, Duke Math. J. **99** (1999), 455–487.

[3] N. Bourbaki, "Algèbre", Chapitre 10 (Masson, Paris, 1980).

[4] V. Chari and A. Pressley, "A guide to quantum groups" (Cambridge University Press, Cambridge, 1995).

[5] I. Damiani, *A basis of type Poincaré-Birkhoff-Witt for the quantum algebra of $\widehat{sl}(2)$*, J. Algebra **161** (1993), 291–310.

[6] V. G. Drinfeld, *Hopf algebras and the quantum Yang-Baxter equation*, Dokl. Akad. Nauk SSSR **283** (1985), 1060–1064 (= Soviet Math. Dokl. **32** (1985), 254–258).

[7] V. G. Drinfeld, *A new realization of Yangians and of quantum affine algebras*, Dokl. Akad. Nauk SSSR **296** (1987), 13–17 (= Soviet Math. Dokl. **36** (1988), 212–216).

[8] J. A. Green, *Hall algebras, hereditary algebras and quantum groups*, Invent. Math. **120** (1995), 361–377.

[9] J. A. Green, *Quantum groups, Hall algebras and quantized shuffles*, in "Finite reductive groups: related structures and representations" (Luminy, 1994, ed. M. Cabanes), Progress in Mathematics 141 (Birkhäuser, Boston, MA, 1997), pp. 273–290.

[10] A. Grothendieck, *Sur la classification des fibrés holomorphes sur la sphère de Riemann*, Amer. J. Math. **79** (1957), 121–138.

[11] R. Hartshorne, "Algebraic geometry", Graduate Texts in Mathematics 52 (Springer-Verlag, New York, Heidelberg, 1977).

[12] M. Jimbo, *A q-difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation*, Lett. Math. Phys. **10** (1985), 63–69.

[13] M. M. Kapranov, *Eisenstein series and quantum affine algebras*, J. Math. Sci. (New York) **84** (1997), 1311–1360.

[14] I. G. Macdonald, "Symmetric functions and Hall polynomials", 2nd edition, Oxford mathematical monographs (Clarendon Press, Oxford, 1995).

[15] C. M. Ringel, *Hall algebras and quantum groups*, Invent. Math. **101** (1990), 583–591.

[16] C. M. Ringel, *Hall algebras*, Banach Cent. Publ. **26** (1) (1990), 433–447.

[17] C. M. Ringel, *From representations of quivers via Hall and Loewy algebras to quantum groups*, in "Proceedings of the international conference on algebra dedicated to the memory of A. I. Malcev" (Novosibirsk, 1989, eds. L. A. Bokut, Yu. L. Ershov and A. I. Kostrikin), Contemporary Mathematics 131 Part 2 (American Mathematical Society, Providence, RI, 1992), pp. 381–401.

[18] C. M. Ringel, *PBW-bases of quantum groups*, J. Reine Angew. Math. **470** (1996), 51–88.

[19] C. M. Ringel, *Green's theorem on Hall algebras*, in "Representation theory of algebras and related topics" (Mexico City, 1994, eds. R. Bautista, R. Martínez-Villa and J. A. E. Peña), CMS Conference Proceedings 19 (American Mathematical Society, Providence, RI, 1996), pp. 185–245.

Institut de Recherche Mathématique Avancée
Université Louis Pasteur et CNRS
7, rue René Descartes
F-67084 Strasbourg Cedex
France

E-mail: `baumann@math.u-strasbg.fr`, `kassel@math.u-strasbg.fr`
Fax: +33 (0) 3 88 61 90 69
Web: `http://www-irma.u-strasbg.fr/~kassel/`