Three variations on the linear independence of grouplikes in a coalgebra.

Gérard Henry Edmond Duchamp, Darij Grinberg, Vincel Ngoc Hoang Minh

Three variations on the linear independence of grouplikes in a coalgebra

Gérard H. E. Duchamp*[1], Darij Grinberg†[2], and Vincel Hoang Ngoc Minh‡[1,3]

[1]LIPN, Northen Paris University, Sorbonne Paris City, 93430 Villetaneuse, France
[2]Drexel University, Korman Center, Room 291, 15 S 33rd Street, Philadelphia PA, 19104, USA
[3]University of Lille, 1 Place Déliot, 59024 Lille, France

01-08-2021 18:28

Abstract. The grouplike elements of a coalgebra over a field are known to be linearly independent over said field. Here we prove three variants of this result. One is a generalization to coalgebras over a commutative ring (in which case the linear independence has to be replaced by a weaker statement). Another is a stronger statement that holds (under stronger assumptions) in a commutative bialgebra. The last variant is a linear independence result for characters (as opposed to grouplike elements) of a bialgebra.

*gheduchamp@gmail.com
†darijgrinberg@gmail.com
‡minh@lipn.univ-paris13.fr

Contents

1. Introduction

A classical result in the theory of coalgebras ([Sweedl69, Proposition 3.2.1 b)], [Radfor12, Lemma 2.1.12], [Abe80, Theorem 2.1.2 (i)]) says that the grouplike elements of a coalgebra over a field are linearly independent over said field. We shall prove three variants of this result. The first variant (Theorem 3.1, in Section 3) generalizes it to coalgebras over an arbitrary commutative ring (at the expense of obtaining a subtler claim than literal linear independence). The second variant (Theorem 4.7, in Section 4) gives a stronger independence claim under a stronger assumption (viz., that the coalgebra is a commutative bialgebra, and that the grouplike elements and their pairwise differences are regular). The third variant (Theorem 5.8 **(b)**, in Section 5) is a linear independence statement in the dual algebra of a bialgebra; namely, it claims that (again under certain conditions) a set of characters of a bialgebra (i.e., algebra homomorphisms from the bialgebra to the base ring) are linearly independent not just over the base ring, but over a certain subalgebra of the dual. We discuss the connection between grouplike elements and characters.

Acknowledgments

We thank Jeremy Rickard for Example 5.15 and Christophe Reutenauer for interesting (electronic) discussions about the Arrow 70 and its link with rational closures.

DG thanks the Mathematisches Forschungsinstitut Oberwolfach for its hospitality at the time this paper was finished. This research was supported through the programme "Oberwolfach Leibniz Fellows" by the Mathematisches Forschungsinstitut Oberwolfach in 2020.

2. Background

2.1. Notations and generalities

2.1.1. General conventions

We shall study coalgebras and bialgebras. We refer to the literature on Hopf algebras and bialgebras – e.g., [GriRei20, Chapter 1] or [Bourba89, Section III.11] – for these concepts.[1]

We let $\mathbb{N}$ denote the set $\{0, 1, 2, \ldots\}$.

Rings are always associative and have unity (but are not always commutative).

We fix a commutative ring $\mathbf{k}$. All algebras, linear maps and tensor signs that appear in the following are over $\mathbf{k}$ unless specified otherwise. The symbol Hom shall always stand for $\mathbf{k}$-module homomorphisms.

2.1.2. Algebras, coalgebras, bialgebras

Recall that

- a $\mathbf{k}$-algebra can be defined as a $\mathbf{k}$-module A equipped with a $\mathbf{k}$-linear map $\mu : A \otimes A \to A$ (called multiplication) and a $\mathbf{k}$-linear map $\eta : \mathbf{k} \to A$ (called unit map) satisfying the associativity axiom (which says that $\mu \circ (\mu \otimes \mathrm{id}) = \mu \circ (\mathrm{id} \otimes \mu)$) and the unitality axiom (which says that $\mu \circ (\eta \otimes \mathrm{id})$ and $\mu \circ (\mathrm{id} \otimes \eta)$ are the canonical isomorphisms from $\mathbf{k} \otimes A$ and $A \otimes \mathbf{k}$ to A).

- a $\mathbf{k}$-coalgebra is defined as a $\mathbf{k}$-module C equipped with a $\mathbf{k}$-linear map $\Delta : C \to C \otimes C$ (called comultiplication) and a $\mathbf{k}$-linear map $\epsilon : C \to \mathbf{k}$ (called counit map) satisfying the coassociativity axiom (which says that $(\Delta \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \Delta) \circ \Delta$) and the counitality axiom (which says that $(\epsilon \otimes \mathrm{id}) \circ \Delta$ and $(\mathrm{id} \otimes \epsilon) \circ \Delta$ are the canonical isomorphisms from C to $\mathbf{k} \otimes C$ and $C \otimes \mathbf{k}$).

- a $\mathbf{k}$-bialgebra means a $\mathbf{k}$-module B that is simultaneously a $\mathbf{k}$-algebra and a $\mathbf{k}$-coalgebra, with the property that the comultiplication Δ and the counit ϵ

[1] We note that terminology is not entirely standardized across the literature. What we call a "coalgebra", for example, is called a "counital coassociative cogebra" in [Bourba89, Section III.11]. What we call a "bialgebra" is called a "bigebra" in [Bourba89, Section III.11].

are **k**-algebra homomorphisms (where the **k**-algebra structure on $B \otimes B$ is the standard one, induced by the one on B).

(Note that Lie algebras are not considered to be **k**-algebras.)

The multiplication and the unit map of a **k**-algebra A will always be denoted by μ_A and η_A. Likewise, the comultiplication and the counit of a **k**-coalgebra C will always be denoted by Δ_C and ϵ_C. We will occasionally omit the subscripts when it is clear what they should be (e.g., we will write Δ instead of Δ_C when it is clear that the only coalgebra we could possibly be referring to is C).

2.1.3. Convolution and the dual algebra of a coalgebra

If C is a **k**-coalgebra, and if A is a **k**-algebra, then the **k**-module $\operatorname{Hom}(C, A)$ itself becomes a **k**-algebra using a multiplication operation known as convolution. We denote it by $\circledast$, and recall how it is defined: For any two **k**-linear maps $f, g \in \operatorname{Hom}(C, A)$, we have

$$f \circledast g = \mu_A \circ (f \otimes g) \circ \Delta_C : C \to A.$$

The map $\eta_A \circ \epsilon_C : C \to A$ is a neutral element for this operation $\circledast$.

(Note that the operation $\circledast$ is denoted by $\star$ in [GriRei20, Definition 1.4.1].)

If f is a **k**-linear map from a coalgebra C to an algebra A, and if $n \in \mathbb{N}$, then $f^{\circledast n}$ denotes the n-th power of f with respect to convolution (i.e., the n-th power of f in the algebra $(\operatorname{Hom}(C, A), \circledast, \eta_A \circ \epsilon_C)$).

If M is any **k**-module, then the dual **k**-module $\operatorname{Hom}_{\mathbf{k}}(M, \mathbf{k})$ shall be denoted by $M^\vee$. Thus, if C is a **k**-coalgebra, then its dual **k**-module $C^\vee = \operatorname{Hom}(C, \mathbf{k})$ becomes a **k**-algebra via the convolution product $\circledast$. The unity of this **k**-algebra $C^\vee$ is exactly the counit ϵ of C.

2.1.4. Grouplike elements

One of the simplest classes of elements in a coalgebra are the grouplike elements:

Definition 2.1. An element g of a **k**-coalgebra C is said to be grouplike if it satisfies $\Delta(g) = g \otimes g$ and $\epsilon(g) = 1$.

We reject the alternative definition of "grouplike" (preferred by some authors) that replaces the "$\epsilon(g) = 1$" condition by the weaker requirement "$g \neq 0$"; this definition is equivalent to ours when **k** is a field, but ill-behaved and useless when **k** is merely a commutative ring.

The following examples illustrate the notion of grouplike elements in different **k**-bialgebras.

Example 2.2. Let $q \in \mathbf{k}$. Consider the polynomial ring $\mathbf{k}[x]$ in one variable x over **k**. Define two **k**-algebra homomorphisms $\Delta : \mathbf{k}[x] \to \mathbf{k}[x] \otimes \mathbf{k}[x]$ and $\epsilon : \mathbf{k}[x] \to \mathbf{k}$ by setting

$$\Delta(x) = x \otimes 1 + 1 \otimes x \qquad \text{and} \qquad \epsilon(x) = 0.$$

Then, it is easy to check that the $\mathbf{k}$-algebra $\mathbf{k}[x]$, equipped with the comultiplication Δ and the counit ϵ, is a $\mathbf{k}$-bialgebra. This is the "standard" $\mathbf{k}$-bialgebra structure on the polynomial ring $\mathbf{k}$. If $\mathbf{k}$ is a reduced ring (i.e., a commutative ring with no nonzero nilpotent elements), then it is not hard to show that 1 is the only grouplike element of this $\mathbf{k}$-bialgebra. On the other hand, if $u \in \mathbf{k}$ satisfies $u^2 = 0$, then the element $1 + ux \in \mathbf{k}[x]$ is also grouplike.

Example 2.3. Let $q \in \mathbf{k}$. Consider the polynomial ring $\mathbf{k}[x]$ in one variable x over $\mathbf{k}$. Define two $\mathbf{k}$-algebra homomorphisms $\Delta_{\uparrow_q} : \mathbf{k}[x] \to \mathbf{k}[x] \otimes \mathbf{k}[x]$ and $\epsilon : \mathbf{k}[x] \to \mathbf{k}$ by setting

$$\Delta_{\uparrow_q}(x) = x \otimes 1 + 1 \otimes x + qx \otimes x \qquad \text{and} \qquad \epsilon(x) = 0.$$

Then, it is easy to check that the $\mathbf{k}$-algebra $\mathbf{k}[x]$, equipped with the comultiplication $\Delta_{\uparrow_q}$ and the counit ϵ, is a $\mathbf{k}$-bialgebra. This $\mathbf{k}$-bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ is known as the univariate q-infiltration bialgebra[2]. Note the following special cases:

1. If $q = 0$, then the univariate q-infiltration bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ is the "standard" $\mathbf{k}$-bialgebra $(\mathbf{k}[x], \Delta, \epsilon)$ from Example 2.2. (Indeed, $\Delta_{\uparrow_q} = \Delta$ when $q = 0$.)

2. When q is nilpotent, the univariate q-infiltration bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ is a Hopf algebra (see, e.g., [GriRei20, Definition 1.4.6] or [Radfor12, Definition 7.1.1] for the definition of this concept). In this case, the antipode of this Hopf algebra sends x to $-x/(1+qx)$.

   If $\mathbf{k}$ is a $\mathbb{Q}$-algebra, then we can say even more: Assume that $\mathbf{k}$ is a $\mathbb{Q}$-algebra and q is nilpotent. Let y be the element $\sum\limits_{k=1}^{\infty} \dfrac{1}{k!} q^{k-1} x^k$ of $\mathbf{k}[x]$. (This sum is actually finite, since q is nilpotent. It can be viewed as the result of evaluating the formal power series $\dfrac{\exp(tx) - 1}{t} \in \mathbf{k}[x][[t]]$ at $t = q$.) Consider the unique $\mathbf{k}$-algebra homomorphism $\Phi : \mathbf{k}[x] \to \mathbf{k}[x]$ that sends x to y. Then, Φ is an isomorphism from the $\mathbf{k}$-bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ to the $\mathbf{k}$-bialgebra $(\mathbf{k}[x], \Delta, \epsilon)$ (defined in Example 2.2).

   No such isomorphism exists in general when $\mathbf{k}$ is not a $\mathbb{Q}$-algebra. For example, if $\mathbf{k}$ is an $\mathbb{F}_2$-algebra, and if $q \in \mathbf{k}$ satisfies $q \neq 0$ and $q^2 = 0$, then the Hopf algebra $(\mathbf{k}[x], \Delta, \epsilon)$ has the property that its antipode is the identity, but the Hopf algebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ does not have this property. Since any $\mathbf{k}$-bialgebra isomorphism between Hopf algebras must respect their antipodes (see, e.g., [GriRei20, Corollary 1.4.27]), this precludes any $\mathbf{k}$-bialgebra isomorphism.

[2] See [ChFoLy58, Ducham01, Ducham15] for the multivariate case.

Let us return to the general case (with $\mathbf{k}$ and q arbitrary). From the above definitions of $\Delta_{\uparrow_q}$ and ϵ, it is easy to see that

$$\Delta_{\uparrow_q}(1+qx) = \underbrace{\Delta_{\uparrow_q}(1)}_{=1\otimes 1} + q \underbrace{\Delta_{\uparrow_q}(x)}_{=x\otimes 1+1\otimes x+qx\otimes x} = (1+qx)\otimes(1+qx)$$

and

$$\epsilon(1+qx) = \underbrace{\epsilon(1)}_{=1} + q\underbrace{\epsilon(x)}_{=0} = 1.$$

Thus, the element $1+qx$ of the univariate q-infiltration bialgebra is grouplike. The element 1 is grouplike as well (in fact, 1 is grouplike in any $\mathbf{k}$-bialgebra).

Example 2.4. Let p be a prime. Let $\mathbf{k}$ be a commutative $\mathbb{F}_p$-algebra. Let $q \in \mathbf{k}$. Let B be the quotient ring of the polynomial ring $\mathbf{k}[x]$ by the ideal I generated by x^p. For any $f \in \mathbf{k}[x]$, we let $\overline{f}$ denote the projection $f+I$ of f onto this quotient B. (Thus, $\overline{x}^p = \overline{x^p} = 0$.) Define two $\mathbf{k}$-algebra homomorphisms $\Delta_{\uparrow_q} : B \to B\otimes B$ and $\epsilon : B \to \mathbf{k}$ by setting

$$\Delta_{\uparrow_q}(\overline{x}) = \overline{x}\otimes 1 + 1\otimes\overline{x} + q\overline{x}\otimes\overline{x} \qquad \text{and} \qquad \epsilon(\overline{x}) = 0.$$

These homomorphisms are well-defined, because Freshman's Dream (i.e., the property of the Frobenius homomorphism to be a $\mathbb{F}_p$-algebra homomorphism) shows that

$$\begin{aligned}(\overline{x}\otimes 1 + 1\otimes\overline{x} + q\overline{x}\otimes\overline{x})^p &= (\overline{x}\otimes 1)^p + (1\otimes\overline{x})^p + q^p(\overline{x}\otimes\overline{x})^p \\ &= \underbrace{\overline{x}^p}_{=0}\otimes 1 + 1\otimes\underbrace{\overline{x}^p}_{=0} + q^p\underbrace{\overline{x}^p}_{=0}\otimes\underbrace{\overline{x}^p}_{=0} = 0\end{aligned}$$

in the commutative $\mathbb{F}_p$-algebra $B\otimes B$. The $\mathbf{k}$-algebra B, equipped with the comultiplication $\Delta_{\uparrow_q}$ and the counit ϵ, is a $\mathbf{k}$-bialgebra – actually a quotient of the univariate q-infiltration bialgebra defined in Example 2.3. Unlike the latter, it is always a Hopf algebra (whether or not q is nilpotent). Examples of grouplike elements in B are 1, $1+q\overline{x}$ and $(1+q\overline{x})^{-1} = 1 - q\overline{x} + q^2\overline{x}^2 - q^3\overline{x}^3 \pm \cdots + (-q)^{p-1}\overline{x}^{p-1}$.

Example 2.5. Consider the polynomial ring $\mathbf{k}[g,x]$ in two (commuting) variables g and x over $\mathbf{k}$. Let B be the quotient ring of this ring by the ideal J generated by gx. For any $f \in \mathbf{k}[g,x]$, we let $\overline{f}$ denote the projection $f+J$ of f onto this quotient B. Define a $\mathbf{k}$-algebra homomorphism $\Delta : B \to B\otimes B$ by

$$\Delta(\overline{g}) = \overline{g}\otimes\overline{g} \qquad \text{and} \qquad \Delta(\overline{x}) = \overline{x}\otimes 1 + 1\otimes\overline{x},$$

and define a $\mathbf{k}$-algebra homomorphism $\epsilon : B \to \mathbf{k}$ by

$$\epsilon(\overline{g}) = 1 \qquad \text{and} \qquad \epsilon(\overline{x}) = 0.$$

(It is straightforward to see that both of these homomorphisms are well-defined, since $(\overline{g}\otimes\overline{g})(\overline{x}\otimes 1 + 1\otimes\overline{x}) = 0$ and $1\cdot 0 = 0$.) These homomorphisms (taken as comultiplication and counit) turn the $\mathbf{k}$-algebra B into a $\mathbf{k}$-bialgebra. Its element $\overline{g}$ is grouplike, and so are all its powers $\overline{g}^i$.

Example 2.6. Let M be a monoid, and let $(\mathbf{k}[M], \mu_M, 1_M)$ be the monoid algebra of M. As a $\mathbf{k}$-module, $\mathbf{k}[M]$ is $\mathbf{k}^{(M)}$, the set of finitely supported functions $M \to \mathbf{k}$. As usual, we identify each $w \in M$ with the indicator function $\delta_w \in \mathbf{k}^{(M)} = \mathbf{k}[M]$ that sends w to $1_\mathbf{k}$ and all other elements of M to 0. Thus, M becomes a basis of $\mathbf{k}[M]$. The multiplication on $\mathbf{k}[M]$ is given by $\mathbf{k}$-bilinearly extending the multiplication of M from this basis to the entire $\mathbf{k}$-module $\mathbf{k}[M]$. Thus, $\mathbf{k}[M]$ becomes a $\mathbf{k}$-algebra, with unity equal to the neutral element of M (or, more precisely, its indicator function).

The $\mathbf{k}$-module dual $(\mathbf{k}[M])^\vee$ of $\mathbf{k}[M]$ can be identified with $\mathbf{k}^M$, the set of all functions $M \to \mathbf{k}$, via the natural $\mathbf{k}$-bilinear pairing between $\mathbf{k}^M$ and $\mathbf{k}^{(M)}$ given by

$$\langle S \mid P \rangle = \sum_{w \in M} S(w) P(w) \qquad \text{for all } S \in \mathbf{k}^M \text{ and } P \in \mathbf{k}[M] = \mathbf{k}^{(M)}. \tag{1}$$

The $\mathbf{k}$-linear map $\Delta_\odot : \mathbf{k}[M] \to \mathbf{k}[M] \otimes \mathbf{k}[M]$ that sends each $w \in M$ to $w \otimes w$ is a $\mathbf{k}$-algebra homomorphism; it is called the diagonal comultiplication. The $\mathbf{k}$-linear map $\epsilon : \mathbf{k}[M] \to \mathbf{k}$ sending each $w \in M$ to $1_\mathbf{k}$ is a $\mathbf{k}$-algebra homomorphism as well. Equipping $\mathbf{k}[M]$ with these two maps $\Delta_\odot$ and ϵ, we obtain a $\mathbf{k}$-bialgebra $\mathcal{B} = (\mathbf{k}[M], \mu_M, 1_M, \Delta_\odot, \epsilon)$, in which every $w \in M$ is grouplike. More generally, a $\mathbf{k}$-linear combination $\sum_{w \in M} a_w w$ (with $a_w \in \mathbf{k}$) is grouplike in $\mathcal{B}$ if and only if the a_w of orthogonal idempotents (i.e., satisfy $a_w^2 = a_w$ for all $w \in M$, $a_v a_w = 0$ for any distinct $v, w \in M$ and $\sum_{w \in M} a_w = 1$). We call $\mathcal{B}$ the monoid bialgebra of M.

If M is a group, then $\mathcal{B}$ is a Hopf algebra. The converse is also true when $\mathbf{k}$ is nontrivial.

We remark that there is some overlap between monoid bialgebras and q-infiltration bialgebras. Indeed, let M be the monoid $\{x^n \mid n \in \mathbb{N}\}$ of all monomials in one variable x. Let $q \in \mathbf{k}$, and let $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ be the univariate q-infiltration bialgebra as in Example 2.3. Then, the $\mathbf{k}$-algebra homomorphism $\mathbf{k}[x] \to \mathbf{k}[M]$ that sends x to $1 + qx$ is a homomorphism of $\mathbf{k}$-bialgebras from the univariate q-infiltration bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ to the monoid bialgebra $\mathcal{B} = (\mathbf{k}[M], \mu_M, 1_M, \Delta_\odot, \epsilon)$. When q is invertible, this homomorphism is an isomorphism.

3. Grouplikes in a coalgebra

Let us first state a simple fact in commutative algebra:

Theorem 3.1. *Let $g_1, g_2, \ldots, g_n$ be n elements of a commutative ring A. Let $c_1, c_2, \ldots, c_n$ be n further elements of A. Assume that*

$$\sum_{i=1}^{n} c_i g_i^k = 0 \qquad \textit{for all } k \in \mathbb{N}. \tag{2}$$

Then,

$$c_i \prod_{j \neq i} (g_i - g_j) = 0 \qquad \text{for all } i \in \{1, 2, \ldots, n\}. \tag{3}$$

Proof. Consider the ring $A[[t]]$ of formal power series in one variable t over A. In this ring, we have

$$\sum_{i=1}^{n} c_i \cdot \underbrace{\frac{1}{1 - tg_i}}_{= \sum\limits_{k \in \mathbb{N}} (tg_i)^k} = \sum_{i=1}^{n} c_i \cdot \sum_{k \in \mathbb{N}} \underbrace{(tg_i)^k}_{= t^k g_i^k} = \sum_{i=1}^{n} c_i \cdot \sum_{k \in \mathbb{N}} t^k g_i^k = \sum_{k \in \mathbb{N}} \underbrace{\sum_{i=1}^{n} c_i g_i^k}_{\substack{=0 \\ \text{(by (2))}}} t^k = 0.$$

Multiplying this equality by $\prod\limits_{j=1}^{n} (1 - tg_j)$, we obtain

$$\sum_{i=1}^{n} c_i \prod_{j \neq i} (1 - tg_j) = 0. \tag{4}$$

This is an equality in the polynomial ring $A[t]$ (which is a subring of $A[[t]]$).

Now consider the ring $A\left[t, t^{-1}\right]$ of Laurent polynomials in t over A. There is an A-algebra homomorphism $A[t] \to A\left[t, t^{-1}\right]$, $t \mapsto t^{-1}$ (by the universal property of $A[t]$). Applying this homomorphism to both sides of the equality (4), we obtain

$$\sum_{i=1}^{n} c_i \prod_{j \neq i} \left(1 - t^{-1} g_j\right) = 0.$$

Hence,

$$\begin{aligned} \sum_{i=1}^{n} c_i \prod_{j \neq i} \underbrace{(t - g_j)}_{= t\left(1 - t^{-1} g_j\right)} &= \sum_{i=1}^{n} c_i \prod_{j \neq i} \left(t \left(1 - t^{-1} g_j\right)\right) = \sum_{i=1}^{n} c_i t^{n-1} \prod_{j \neq i} \left(1 - t^{-1} g_j\right) \\ &= t^{n-1} \underbrace{\sum_{i=1}^{n} c_i \prod_{j \neq i} \left(1 - t^{-1} g_j\right)}_{=0} = 0. \end{aligned} \tag{5}$$

This is an equality in the polynomial ring $A[t]$ (which is a subring of $A\left[t, t^{-1}\right]$); hence, we can substitute arbitrary values for t in it.

Now, fix $h \in \{1, 2, \ldots, n\}$. Substitute g_h for t in the equality (5). The result is

$$\sum_{i=1}^{n} c_i \prod_{j \neq i} (g_h - g_j) = 0.$$

Hence,

$$0 = \sum_{i=1}^{n} c_i \prod_{j \neq i} \left(g_h - g_j\right) = c_h \prod_{j \neq h} \left(g_h - g_j\right) + \sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \neq h}} c_i \underbrace{\prod_{j \neq i} \left(g_h - g_j\right)}_{\substack{=0 \\ \text{(since } g_h - g_h = 0 \text{ is among} \\ \text{the factors of this product)}}}$$

$$\text{(here, we have split off the addend for } i = h \text{ from the sum)}$$

$$= c_h \prod_{j \neq h} \left(g_h - g_j\right) + \underbrace{\sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \neq h}} c_i 0}_{=0} = c_h \prod_{j \neq h} \left(g_h - g_j\right).$$

Now forget that we fixed h. Thus, we have shown that $c_h \prod_{j \neq h} \left(g_h - g_j\right) = 0$ for all $h \in \{1, 2, \ldots, n\}$. Renaming h as i, we obtain (3). Theorem 3.1 is proven. □

Our first main result is now the following:

Theorem 3.2. *Let $g_1, g_2, \ldots, g_n$ be n grouplike elements of a $\mathbf{k}$-coalgebra C. Let $c_1, c_2, \ldots, c_n \in \mathbf{k}$. Assume that $\sum_{i=1}^{n} c_i g_i = 0$. Then,*

$$c_i \prod_{j \neq i} \left(g_i - g_j\right) = 0 \qquad \text{in } \operatorname{Sym} C \text{ for all } i \in \{1, 2, \ldots, n\}.$$

Here, $\operatorname{Sym} C$ *denotes the symmetric algebra of the* $\mathbf{k}$*-module* C*.*

Our proof of this theorem will rely on a certain family of maps defined for any $\mathbf{k}$-coalgebra:

Definition 3.3. Let C be a $\mathbf{k}$-coalgebra. We then define a sequence of $\mathbf{k}$-linear maps $\Delta^{(-1)}, \Delta^{(0)}, \Delta^{(1)}, \ldots$, where $\Delta^{(k)}$ is a $\mathbf{k}$-linear map from C to $C^{\otimes(k+1)}$ for any integer $k \geq -1$. Namely, we define them recursively by setting $\Delta^{(-1)} = \epsilon$ and $\Delta^{(0)} = \mathrm{id}_C$ and $\Delta^{(k)} = \left(\mathrm{id}_C \otimes \Delta^{(k-1)}\right) \otimes \Delta$ for all $k \geq 1$. These maps $\Delta^{(k)}$ are known as the iterated comultiplications of C, and studied further, e.g., in [GriRei20, Exercise 1.4.20].

Proof of Theorem 3.2. Every grouplike element $g \in C$ and every $k \in \mathbb{N}$ satisfy

$$\Delta^{(k-1)} g = g^{\otimes k} \tag{6}$$

(where $g^{\otimes k}$ means $\underbrace{g \otimes g \otimes \cdots \otimes g}_{k \text{ times}} \in C^{\otimes k}$). Indeed, this can be easily proven by induction on k.

The g_i (for all $i \in \{1,2,\ldots,n\}$) are grouplike. Thus, (6) (applied to $g = g_i$) shows that $\Delta^{(k-1)} g_i = g_i^{\otimes k}$ for each $k \in \mathbb{N}$ and each $i \in \{1,2,\ldots,n\}$. Hence, applying the $\mathbf{k}$-linear map $\Delta^{(k-1)}$ to both sides of the equality $\sum\limits_{i=1}^{n} c_i g_i = 0$, we obtain

$$\sum_{i=1}^{n} c_i g_i^{\otimes k} = 0 \tag{7}$$

for each $k \in \mathbb{N}$.

But recall that the symmetric algebra $\operatorname{Sym} C$ is defined as a quotient of the tensor algebra $T(C)$. Hence, there is a canonical projection from $T(C)$ to $\operatorname{Sym} C$ that sends each tensor $x_1 \otimes x_2 \otimes \cdots \otimes x_m \in T(C)$ to $x_1 x_2 \cdots x_m \in \operatorname{Sym} C$. In particular, this projection sends $g_i^{\otimes k}$ to g_i^k for each $i \in \{1,2,\ldots,n\}$ and each $k \in \mathbb{N}$. Thus, applying this projection to both sides of (7), we obtain $\sum\limits_{i=1}^{n} c_i g_i^k = 0$ in $\operatorname{Sym} C$ for all $k \in \mathbb{N}$. Thus, Theorem 3.1 can be applied to $A = \operatorname{Sym} C$. We conclude that

$$c_i \prod_{j \neq i} \left(g_i - g_j\right) = 0 \qquad \text{in } \operatorname{Sym} C \text{ for all } i \in \{1,2,\ldots,n\}.$$

This proves Theorem 3.2. □

From Theorem 3.2, we obtain the following classical fact [Radfor12, Lemma 2.1.12]:

Corollary 3.4. *Assume that* $\mathbf{k}$ *is a field. Let* $g_1, g_2, \ldots, g_n$ *be* n *distinct grouplike elements of a* $\mathbf{k}$*-coalgebra* C*. Then,* $g_1, g_2, \ldots, g_n$ *are* $\mathbf{k}$*-linearly independent.*

Proof of Corollary 3.4. The $\mathbf{k}$-module C is free (since $\mathbf{k}$ is a field). Thus, the $\mathbf{k}$-algebra $\operatorname{Sym} C$ is isomorphic to a polynomial algebra over $\mathbf{k}$, and thus is an integral domain (again since $\mathbf{k}$ is a field). Its elements $g_i - g_j$ for $j \neq i$ are nonzero (since $g_1, g_2, \ldots, g_n$ are distinct), and thus their products $\prod\limits_{j \neq i} \left(g_i - g_j\right)$ (for $i \in \{1,2,\ldots,n\}$) are nonzero as well (since $\operatorname{Sym} C$ is an integral domain).

Let $c_1, c_2, \ldots, c_n \in \mathbf{k}$ be such that $\sum\limits_{i=1}^{n} c_i g_i = 0$. Then, Theorem 3.2 yields

$$c_i \prod_{j \neq i} \left(g_i - g_j\right) = 0 \qquad \text{in } \operatorname{Sym} C \text{ for all } i \in \{1,2,\ldots,n\}.$$

We can cancel the $\prod\limits_{j \neq i} \left(g_i - g_j\right)$ factors from this equality (since these factors $\prod\limits_{j \neq i} \left(g_i - g_j\right)$ are nonzero, and since $\operatorname{Sym} C$ is an integral domain). Thus, we obtain the equalities $c_i = 0$ in $\operatorname{Sym} C$ for all $i \in \{1,2,\ldots,n\}$. In other words, $c_i = 0$ in $\mathbf{k}$ for all $i \in \{1,2,\ldots,n\}$ (since $\mathbf{k}$ embeds into $\operatorname{Sym} C$).

Now, forget that we fixed $c_1, c_2, \ldots, c_n$. We thus have proven that if $c_1, c_2, \ldots, c_n \in \mathbf{k}$ are such that $\sum\limits_{i=1}^{n} c_i g_i = 0$, then $c_i = 0$ for all $i \in \{1,2,\ldots,n\}$. In other words, $g_1, g_2, \ldots, g_n$ are $\mathbf{k}$-linearly independent. This proves Corollary 3.4. □

Remark 3.5. Example 2.3 illustrates why we required $\mathbf{k}$ to be a field in Corollary 3.4. Indeed, if $q \in \mathbf{k}$ is a zero-divisor but nonzero, then the two grouplike elements 1 and $1 + qx$ of the $\mathbf{k}$-bialgebra in Example 2.3 fail to be $\mathbf{k}$-linearly independent. Theorem 3.2, however, provides a weaker version of linear independence that is still satisfied.

4. Grouplikes over id-unipotents in a bialgebra

4.1. The notion of id-unipotence

In this section, we shall use the following concept:

Definition 4.1. Let B be a $\mathbf{k}$-bialgebra. An element $b \in B$ is said to be id-unipotent if there exists some $m \in \mathbb{Z}$ such that every nonnegative integer $n > m$ satisfies

$$(\eta\epsilon - \mathrm{id})^{\circledast n}(b) = 0 \tag{8}$$

(where id means id_B). We shall refer to such an m as a degree-upper bound of b.

Before we move on to studying id-unipotent elements, let us show several examples:

Example 4.2. Let B be a connected graded $\mathbf{k}$-bialgebra. (The word "graded" here means "$\mathbb{N}$-graded", and it is assumed that all structure maps $\mu, \eta, \Delta, \epsilon$ preserve the grading. The word "connected" means that the 0-th homogeneous component B_0 is isomorphic to $\mathbf{k}$.) Then, each $b \in B$ is id-unipotent, and if $b \in B$ is homogeneous of degree k, then k is a degree-upper bound of b.

Example 4.3. Let q, $\mathbf{k}[x]$, $\Delta_{\uparrow_q}$ and ϵ be as in Example 2.3. Assume that q is nilpotent, with $q^m = 0$ for some $m \in \mathbb{N}$. It is easy to see (by induction on n) that $(\eta\epsilon - \mathrm{id})^{\circledast n}(x) = -(-q)^{n-1}x^n$ in $\mathbf{k}[x]$ for each $n \geq 1$. Thus, for each $n > m$, we have $(\eta\epsilon - \mathrm{id})^{\circledast n}(x) = -(-q)^{n-1}x^n = 0$ (since $q^m = 0$ and thus $(-q)^{n-1} = 0$). Hence, the element x is id-unipotent in $\mathbf{k}[x]$, with m being a degree-upper bound of x. Combining this observation with Corollary 4.24 further below, it follows easily that every element of $\mathbf{k}[x]$ is id-unipotent (albeit m will not always be a degree-upper bound).

Example 4.4. Let p, $\mathbf{k}$, q and B be as in Example 2.4. It is easy to see (by induction on n) that $(\eta\epsilon - \mathrm{id})^{\circledast n}(\overline{x}) = -(-q)^{n-1}\overline{x}^n$ for each $n \geq 1$. Thus, for each $n \geq p$, we have $(\eta\epsilon - \mathrm{id})^{\circledast n}(\overline{x}) = -(-q)^{n-1}\overline{x}^n = 0$ (since $\overline{x}^p = 0$ and thus $\overline{x}^n = 0$). Hence, the element $\overline{x}$ is id-unipotent in B, with $p - 1$ being a degree-upper bound of $\overline{x}$.

Remark 4.5. The notion of id-unipotence is connected with the classical notion of Δ_+-nilpotence, but it is a weaker notion. Let us briefly describe the latter notion and the connection.

Consider a $\mathbf{k}$-bialgebra B with comultiplication Δ, counit ϵ and unit map η. Then, we have a canonical direct sum decomposition $B = \mathbf{k}1_B \oplus B_+$ of the $\mathbf{k}$-module B, where $B_+ = \ker(\epsilon)$ (and where $1_B = \epsilon(1_\mathbf{k})$ is the unity of B). The corresponding projections are $\eta\epsilon$ (projecting B onto $\mathbf{k}1_B$) and $\mathrm{id} - \eta\epsilon$ (projecting B onto B_+). Thus, we set $\overline{\mathrm{id}} = \mathrm{id} - \eta\epsilon : B \to B$ (this projection, in a way, "eliminates the constant term"). For each $k \in \mathbb{N}$, we define a map

$$\Delta_+^{(k)} = \overline{\mathrm{id}}^{\otimes(k+1)} \circ \Delta^{(k)} : B \to B^{\otimes(k+1)},$$

where $\overline{\mathrm{id}}^{\otimes(k+1)} = \overline{\mathrm{id}} \otimes \overline{\mathrm{id}} \otimes \cdots \otimes \overline{\mathrm{id}}$ (with $k+1$ tensorands) and where $\Delta^{(k)} : B \to B^{\otimes(k+1)}$ is the iterated comultiplication from Definition 3.3.

Now, an element x of B is said to be $\underline{\Delta_+\text{-nilpotent}}$ if there exists some $m \in \mathbb{Z}$ such that every nonnegative integer $k > m$ satisfies

$$\Delta_+^{(k)}(b) = 0. \tag{9}$$

It is easy to see that every $n \geq 1$ satisfies

$$(\eta\epsilon - \mathrm{id})^{\circledast n} = (-\overline{\mathrm{id}})^{\circledast n} = (-1)^n \mu^{(n-1)} \circ \Delta_+^{(n-1)},$$

where $\mu^{(n-1)} : B^{\otimes n} \to B$ is the "iterated multiplication" map that sends each pure tensor $b_1 \otimes b_2 \otimes \cdots \otimes b_n$ to $b_1 b_2 \cdots b_n \in B$. Thus, every Δ_+-nilpotent element of B is id-unipotent. The converse, however, is not true. For instance, the element $\overline{x}$ in Example 4.4 is id-unipotent but (in general) not Δ_+-nilpotent. (But the elements x in Example 4.3 and b in Example 4.2 are Δ_+-nilpotent.)[3]

4.2. The linear independence

We shall also use a slightly generalized notion of linear independence:

Definition 4.6. Let $g_1, g_2, \ldots, g_n$ be some elements of a $\mathbf{k}$-algebra A. Let S be a subset of A.

(a) We say that the elements $g_1, g_2, \ldots, g_n$ are $\underline{\text{left } S\text{-linearly independent}}$ if every n-tuple $(s_1, s_2, \ldots, s_n) \in S^n$ of elements of S satisfying $\sum_{i=1}^{n} s_i g_i = 0$ must satisfy $(s_i = 0 \text{ for all } i)$.

[3] Nevertheless, at least in one important case, the two concepts are closely intertwined. Namely, if $\mathbf{k}$ is a $\mathbb{Q}$-algebra and B is cocommutative, then we have the following chain of equivalences:

$$(\text{every } b \in B \text{ is id-unipotent}) \Longleftrightarrow (B = \mathcal{U}(\mathrm{Prim}(B))) \Longleftrightarrow (\text{every } b \in B \text{ is } \Delta_+\text{-nilpotent}),$$

where "$B = \mathcal{U}(\mathrm{Prim}(B))$" means that B is the universal enveloping bialgebra (see [Bourba98, ch II §1] for the definition) of its primitive elements. The two equivalence signs follow easily from [DMTCN14, Theorem 1] (noticing that a filtration as in [DMTCN14, Theorem 1 condition 1] forces every $b \in B$ to be Δ_+-nilpotent). This is a variant of the well-known Cartier–Quillen–Milnor–Moore theorem [Car07, MM65] that relies on (formal) convergence of infinite sums instead of primitive generation of the Hopf algebra.

(b) The notion of "right S-linearly independent" is defined in the same way as "left S-linearly independent", except that the sum $\sum_{i=1}^{n} s_i g_i$ is replaced by $\sum_{i=1}^{n} g_i s_i$.

(c) If the $\mathbf{k}$-algebra A is commutative, then these two notions are identical, and we just call them "S-linearly independent".

We also recall that an element a of a commutative ring A is said to be regular if it is a non-zero-divisor – i.e., if it has the property that whenever b is an element of A satisfying $ab = 0$, then $b = 0$.

We can now state the second of our main theorems:

Theorem 4.7. *Let B be a commutative $\mathbf{k}$-bialgebra. Let L denote the set of all id-unipotent elements of B.*

Let $g_1, g_2, \ldots, g_n$ be n grouplike elements of B. Let us make two assumptions:

- *Assumption 1: For any $1 \leq i < j \leq n$, the element $g_i - g_j$ of B is regular.*
- *Assumption 2: For any $1 \leq i \leq n$, the element g_i of B is regular.*

Then, $g_1, g_2, \ldots, g_n$ are L-linearly independent.

Before we prove this theorem, some remarks are in order.

Remark 4.8. The L in Theorem 4.7 is a $\mathbf{k}$-submodule of B. (This is easily seen directly: If $u \in B$ and $v \in B$ are id-unipotent with degree-upper bounds p and q, respectively, then $\lambda u + \mu v$ is id-unipotent with degree-upper bound $\max\{p, q\}$ for any $\lambda, \mu \in \mathbf{k}$.)

It can be shown that L is a $\mathbf{k}$-subalgebra of B. (See Corollary 4.24 further below; we will not need this to prove Theorem 4.7.) We do not know if L is a $\mathbf{k}$-subcoalgebra of B.

Remark 4.9. Example 2.5 illustrates why we required Assumption 2 to hold in Theorem 4.7. Indeed, in this example, $\overline{g}$ is grouplike, and $\overline{x}$ is id-unipotent (with degree-upper bound 1), so the equality $\overline{xg} = \overline{gx} = 0$ shows that even the single grouplike element $\overline{g}$ is not L-linearly independent.

The necessity of Assumption 1 can be illustrated by Remark 3.5 again.

Question 1. Is the requirement for B to be commutative necessary? (It is certainly needed for our proof.)

To prove Theorem 4.7, we shall use a few lemmas. The first one is a classical result [GriRei20, Exercise 1.5.11(a)]:

Lemma 4.10. *Let C be a $\mathbf{k}$-bialgebra. Let A be a commutative $\mathbf{k}$-algebra. Let $p : C \to A$ and $q : C \to A$ be two $\mathbf{k}$-algebra homomorphisms. Then, the map $p \circledast q : C \to A$ is also a $\mathbf{k}$-algebra homomorphism.*

Proof of Lemma 4.10. Let $a \in C$ and $b \in C$. We shall prove that $(p \circledast q)(ab) = (p \circledast q)(a) \cdot (p \circledast q)(b)$.

Using Sweedler notation, write $\Delta(a) = \sum_{(a)} a_{(1)} \otimes a_{(2)}$ and $\Delta(b) = \sum_{(b)} b_{(1)} \otimes b_{(2)}$. Then, the multiplicativity of Δ yields $\Delta(ab) = \sum_{(a)} \sum_{(b)} a_{(1)} b_{(1)} \otimes a_{(2)} b_{(2)}$. Thus,

$$
\begin{aligned}
(p \circledast q)(ab) &= \sum_{(a)} \sum_{(b)} \underbrace{p\left(a_{(1)} b_{(1)}\right)}_{\substack{= p\left(a_{(1)}\right) p\left(b_{(1)}\right) \\ \text{(since } p \text{ is a } \mathbf{k}\text{-algebra} \\ \text{homomorphism)}}} \underbrace{q\left(a_{(2)} b_{(2)}\right)}_{\substack{= q\left(a_{(2)}\right) q\left(b_{(2)}\right) \\ \text{(since } q \text{ is a } \mathbf{k}\text{-algebra} \\ \text{homomorphism)}}} \\
&= \sum_{(a)} \sum_{(b)} p\left(a_{(1)}\right) p\left(b_{(1)}\right) q\left(a_{(2)}\right) q\left(b_{(2)}\right) \\
&= \underbrace{\left(\sum_{(a)} p\left(a_{(1)}\right) q\left(a_{(2)}\right) \right)}_{= (p \circledast q)(a)} \cdot \underbrace{\left(\sum_{(b)} p\left(b_{(1)}\right) q\left(b_{(2)}\right) \right)}_{= (p \circledast q)(b)} \\
&\qquad \text{(since } A \text{ is commutative)} \\
&= (p \circledast q)(a) \cdot (p \circledast q)(b).
\end{aligned}
$$

Now, forget that we fixed a and b. We thus have proven that $(p \circledast q)(ab) = (p \circledast q)(a) \cdot (p \circledast q)(b)$ for each $a, b \in C$. An even simpler argument shows that $(p \circledast q)(1) = 1$. Combining these results, we conclude that $p \circledast q : C \to A$ is a $\mathbf{k}$-algebra homomorphism. This completes the proof of Lemma 4.10. ☐

Lemma 4.11. *Let B be a commutative $\mathbf{k}$-bialgebra. Let $k \in \mathbb{N}$. Then, $\mathrm{id}^{\circledast k} : B \to B$ is a $\mathbf{k}$-algebra homomorphism.*

Proof of Lemma 4.11. This follows by straightforward induction on k. Indeed, the base case $k = 0$ follows from the fact that $\eta_B \epsilon_B$ is a $\mathbf{k}$-algebra homomorphism, while the induction step uses Lemma 4.10 (applied to $C = B$ and $A = B$) and the fact that id_B is a $\mathbf{k}$-algebra homomorphism. ☐

Lemma 4.12. *Let B be a $\mathbf{k}$-bialgebra. Let $g \in B$ be any grouplike element. Let $k \in \mathbb{N}$. Then, $\mathrm{id}^{\circledast k}(g) = g^k$. (Here, id means id_B.)*

Proof of Lemma 4.12. This follows easily by induction on k. ☐

Lemma 4.13. *Let B be a $\mathbf{k}$-bialgebra. Let $b \in B$ be id-unipotent and nonzero. Let m be a degree-upper bound of b. Then, $m \in \mathbb{N}$.*

Proof of Lemma 4.13. Assume the contrary. Thus, m is negative (since m is an integer). Therefore, every $n \in \mathbb{N}$ satisfies $n > m$. Hence, by the definition of a

degree-upper bound, we must have $(\eta\epsilon - \mathrm{id})^{\circledast n}(b) = 0$ for each $n \in \mathbb{N}$. Thus, in particular, we have $(\eta\epsilon - \mathrm{id})^{\circledast 0}(b) = 0$ and $(\eta\epsilon - \mathrm{id})^{\circledast 1}(b) = 0$. Hence,

$$\underbrace{(\eta\epsilon - \mathrm{id})^{\circledast 0}(b)}_{=0} - \underbrace{(\eta\epsilon - \mathrm{id})^{\circledast 1}(b)}_{=0} = 0.$$

This contradicts

$$\underbrace{(\eta\epsilon - \mathrm{id})^{\circledast 0}}_{=\eta\epsilon}(b) - \underbrace{(\eta\epsilon - \mathrm{id})^{\circledast 1}}_{=\eta\epsilon-\mathrm{id}}(b) = (\eta\epsilon)(b) - (\eta\epsilon - \mathrm{id})(b) = \mathrm{id}(b) = b \neq 0$$

(since b is nonzero). This contradiction completes the proof of Lemma 4.13. □

Lemma 4.14. *Let B be a $\mathbf{k}$-bialgebra. Let $b \in B$ be id-unipotent. Let m be a degree-upper bound of b. Then, in the ring $B[[t]]$ of power series[4], we have*

$$(1-t)^{m+1} \sum_{k\in\mathbb{N}} \mathrm{id}^{\circledast k}(b)\, t^k = \sum_{k=0}^{m} (-1)^k (\eta\epsilon - \mathrm{id})^{\circledast k}(b)\, t^k (1-t)^{m-k}.$$

(Here, id *means* id_B*.)*

Proof of Lemma 4.14. We know that m is a degree-upper bound of b. In other words, we have $(\eta\epsilon - \mathrm{id})^{\circledast n}(b) = 0$ for every nonnegative integer $n > m$ (by (8)). In other words, we have

$$(\eta\epsilon - \mathrm{id})^{\circledast k}(b) = 0 \qquad \text{for every nonnegative integer } k > m. \tag{10}$$

Let ι denote the canonical inclusion $B \hookrightarrow B[[t]]$. This is an injective $\mathbf{k}$-algebra homomorphism, and will be regarded as an inclusion.

The convolution algebra $(\mathrm{Hom}(B,B), \circledast)$ embeds in the convolution algebra $(\mathrm{Hom}(B, B[[t]]), \circledast)$ (indeed, there is an injective $\mathbf{k}$-algebra homomorphism from the former to the latter, which sends each $f \in \mathrm{Hom}(B,B)$ to $\iota \circ f \in \mathrm{Hom}(B, B[[t]])$). Again, we shall regard this embedding as an inclusion (so we will identify each $f \in \mathrm{Hom}(B,B)$ with $\iota \circ f$).

The convolution algebra $(\mathrm{Hom}(B, B[[t]]), \circledast)$ has unity $\eta\epsilon = \eta_{B[[t]]}\epsilon_B$. Thus, from the classical power-series identity $(1-u)^{-1} = \sum\limits_{k\in\mathbb{N}} u^k$, we obtain the equality

$$(\eta\epsilon - tf)^{\circledast(-1)} = \sum_{k\in\mathbb{N}} (tf)^{\circledast k} = \sum_{k\in\mathbb{N}} t^k f^{\circledast k} \tag{11}$$

for every $f \in \mathrm{Hom}(B, B[[t]])$.

[4]This ring is defined in the usual way even if B is not commutative. Thus, t will commute with every power series in $B[[t]]$.

Now,

$$\sum_{k\in\mathbb{N}} \mathrm{id}^{\circledast k}(b)\, t^k = \underbrace{\left(\sum_{k\in\mathbb{N}} t^k\, \mathrm{id}^{\circledast k}\right)}_{\substack{=(\eta\epsilon - t\,\mathrm{id})^{\circledast(-1)} \\ \text{(by (11), applied to } f=\mathrm{id})}} (b)$$
$$= (\eta\epsilon - t\,\mathrm{id})^{\circledast(-1)}(b)\,. \tag{12}$$

But

$$\eta\epsilon - t\,\mathrm{id} = \eta\epsilon\,(1-t) - t\,(\mathrm{id} - \eta\epsilon) = \left(\eta\epsilon - t\,(\mathrm{id}-\eta\epsilon)\,\frac{1}{1-t}\right)(1-t)$$

and therefore

$$\begin{aligned}(\eta\epsilon - t\,\mathrm{id})^{\circledast(-1)} &= \left(\left(\eta\epsilon - t\,(\mathrm{id}-\eta\epsilon)\,\frac{1}{1-t}\right)(1-t)\right)^{\circledast(-1)} \\ &= (1-t)^{-1}\cdot\left(\eta\epsilon - t\,(\mathrm{id}-\eta\epsilon)\,\frac{1}{1-t}\right)^{\circledast(-1)} \\ &= (1-t)^{-1}\cdot\sum_{k\in\mathbb{N}} t^k\left((\mathrm{id}-\eta\epsilon)\,\frac{1}{1-t}\right)^{\circledast k}\end{aligned}$$

(by (11), applied to $f = (\mathrm{id} - \eta\epsilon)\,\dfrac{1}{1-t}$). Hence, (12) becomes

$$\begin{aligned}
\sum_{k\in\mathbb{N}} \mathrm{id}^{\circledast k}(b)\,t^k &= \underbrace{(\eta\epsilon - t\,\mathrm{id})^{\circledast(-1)}}_{=(1-t)^{-1}\cdot\sum\limits_{k\in\mathbb{N}} t^k\left((\mathrm{id}-\eta\epsilon)\frac{1}{1-t}\right)^{\circledast k}}(b) \\
&= (1-t)^{-1}\cdot\sum_{k\in\mathbb{N}} t^k \underbrace{\left((\mathrm{id}-\eta\epsilon)\,\frac{1}{1-t}\right)^{\circledast k}(b)}_{=(\mathrm{id}-\eta\epsilon)^{\circledast k}(b)\left(\frac{1}{1-t}\right)^k} \\
&= (1-t)^{-1}\cdot\sum_{k\in\mathbb{N}} \left(\underbrace{\mathrm{id}-\eta\epsilon}_{=-(\eta\epsilon-\mathrm{id})}\right)^{\circledast k}(b)\left(\frac{t}{1-t}\right)^k \\
&= (1-t)^{-1}\cdot\sum_{k\in\mathbb{N}} \underbrace{(-(\eta\epsilon-\mathrm{id}))^{\circledast k}}_{=(-1)^k(\eta\epsilon-\mathrm{id})^{\circledast k}}(b)\left(\frac{t}{1-t}\right)^k \\
&= (1-t)^{-1}\cdot\underbrace{\sum_{k\in\mathbb{N}} (-1)^k(\eta\epsilon-\mathrm{id})^{\circledast k}(b)\left(\frac{t}{1-t}\right)^k}_{\substack{\text{All addends of this sum for } k>m \text{ are}\\ \text{zero, due to (10).}}} \\
&= (1-t)^{-1}\cdot\sum_{k=0}^{m} (-1)^k(\eta\epsilon-\mathrm{id})^{\circledast k}(b)\left(\frac{t}{1-t}\right)^k.
\end{aligned}$$

Multiplying both sides of this equality by $(1-t)^{m+1}$, we get

$$\begin{aligned}
(1-t)^{m+1}\sum_{k\in\mathbb{N}} \mathrm{id}^{\circledast k}(b)\,t^k &= (1-t)^m\cdot\sum_{k=0}^{m}(-1)^k(\eta\epsilon-\mathrm{id})^{\circledast k}(b)\left(\frac{t}{1-t}\right)^k \\
&= \sum_{k=0}^{m}(-1)^k(\eta\epsilon-\mathrm{id})^{\circledast k}(b)\,t^k(1-t)^{m-k}.
\end{aligned}$$

This proves Lemma 4.14. □

Lemma 4.15. *Let A be a commutative ring. Let $m \in \mathbb{N}$ and $u \in A$. Let $F(t) \in A[t]$ be a polynomial of degree $\leq m$. Set*

$$G(t) = t^m F\left(\frac{u}{t}\right) \in A\left[t, t^{-1}\right].$$

Then, $G(t)$ is actually a polynomial in $A[t]$ and satisfies

$$G(u) = u^m F(1). \tag{13}$$

Proof of Lemma 4.15. We have $G(t) = t^m F\left(\frac{u}{t}\right) \in A[t]$ because $F(t)$ has degree $\leq m$. It remains to show that $G(u) = u^m F(1)$. It is tempting to argue this by substituting u for t in the equality $G(t) = t^m F\left(\frac{u}{t}\right)$, but this is not completely justified (we cannot arbitrarily substitute u for t in an equality of Laurent polynomials unless we know that u is invertible[5]). But we can argue as follows instead:

The polynomial $F(t)$ has degree $\leq m$. Hence, we can write it in the form $F(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_m t^m$ for some $a_0, a_1, \ldots, a_m \in A$. Consider these $a_0, a_1, \ldots, a_m$. Thus, $F(1) = a_0 + a_1 1 + a_2 1^2 + \cdots + a_m 1^m = a_0 + a_1 + a_2 + \cdots + a_m$ and $F\left(\frac{u}{t}\right) = a_0 + a_1 \frac{u}{t} + a_2 \left(\frac{u}{t}\right)^2 + \cdots + a_m \left(\frac{u}{t}\right)^m$. The definition of $G(t)$ yields

$$\begin{aligned} G(t) &= t^m \underbrace{F\left(\frac{u}{t}\right)}_{= a_0 + a_1 \frac{u}{t} + a_2 \left(\frac{u}{t}\right)^2 + \cdots + a_m \left(\frac{u}{t}\right)^m} = t^m \left(a_0 + a_1 \frac{u}{t} + a_2 \left(\frac{u}{t}\right)^2 + \cdots + a_m \left(\frac{u}{t}\right)^m\right) \\ &= a_0 t^m + a_1 u t^{m-1} + a_2 u^2 t^{m-2} + \cdots + a_m u^m t^0. \end{aligned}$$

Substituting u for t in this equality of polynomials, we obtain

$$\begin{aligned} G(u) &= a_0 u^m + a_1 u u^{m-1} + a_2 u^2 u^{m-2} + \cdots + a_m u^m u^0 \\ &= a_0 u^m + a_1 u^m + a_2 u^m + \cdots + a_m u^m = u^m \underbrace{\left(a_0 + a_1 + a_2 + \cdots + a_m\right)}_{= F(1)} = u^m F(1), \end{aligned}$$

and thus Lemma 4.15 is proven. □

Proof of Theorem 4.7. Let $b_1, b_2, \ldots, b_n \in L$ be such that $\sum_{i=1}^{n} b_i g_i = 0$. We must show that $b_i = 0$ for all i.

Assume the contrary. Thus, there exists some i such that $b_i \neq 0$. We WLOG assume that **each** i satisfies $b_i \neq 0$, since otherwise we can just drop the violating b_i and the corresponding g_i and reduce the problem to a smaller value of n.

For each $i \in \{1, 2, \ldots, n\}$, the element $b_i \in B$ is id-unipotent (since it belongs to L) and thus has a degree-upper bound. We let m_i be the **smallest** degree-upper bound of b_i. This is well-defined, because Lemma 4.13 (applied to $b = b_i$) shows that every degree-upper bound of b_i must be $\in \mathbb{N}$. Thus, each m_i belongs to $\mathbb{N}$.

For each $i \in \{1, 2, \ldots, n\}$, Lemma 4.14 (applied to $b = b_i$ and $m = m_i$) shows that in the ring $B[[t]]$, we have

$$\begin{aligned} &(1-t)^{m_i+1} \sum_{k \in \mathbb{N}} \mathrm{id}^{\circledast k}(b_i)\, t^k \\ &= \sum_{k=0}^{m_i} (-1)^k \left(\eta\epsilon - \mathrm{id}\right)^{\circledast k}(b_i)\, t^k\, (1-t)^{m_i - k} \end{aligned} \tag{14}$$

[5] since the universal property of the Laurent polynomial ring $A\left[t, t^{-1}\right]$ is only stated for invertible elements

(since m_i is a degree-upper bound of b_i). The right-hand side of this equality is a polynomial in t of degree $\leq m_i$. Denote this polynomial by $Q_i(t)$. Hence, (14) becomes

$$(1-t)^{m_i+1} \sum_{k \in \mathbb{N}} \mathrm{id}^{\circledast k}(b_i)\, t^k = Q_i(t),$$

so that

$$\sum_{k \in \mathbb{N}} \mathrm{id}^{\circledast k}(b_i)\, t^k = \frac{Q_i(t)}{(1-t)^{m_i+1}}. \tag{15}$$

Now, let $k \in \mathbb{N}$. Lemma 4.11 yields that the map $\mathrm{id}^{\circledast k}$ is a $\mathbf{k}$-algebra homomorphism. Thus,

$$\mathrm{id}^{\circledast k}\left(\sum_{i=1}^{n} b_i g_i\right) = \sum_{i=1}^{n} \mathrm{id}^{\circledast k}(b_i) \underbrace{\mathrm{id}^{\circledast k}(g_i)}_{\substack{=g_i^k \\ \text{(by Lemma 4.12,} \\ \text{since } g_i \text{ is grouplike)}}} = \sum_{i=1}^{n} \mathrm{id}^{\circledast k}(b_i)\, g_i^k.$$

Hence,

$$\sum_{i=1}^{n} \mathrm{id}^{\circledast k}(b_i)\, g_i^k = \mathrm{id}^{\circledast k}\left(\underbrace{\sum_{i=1}^{n} b_i g_i}_{=0}\right) = 0. \tag{16}$$

Forget that we fixed k. We thus have proved (16) for each $k \in \mathbb{N}$. Now, in the commutative ring $B[[t]]$, we have

$$\sum_{i=1}^{n} \underbrace{\frac{Q_i(tg_i)}{(1-tg_i)^{m_i+1}}}_{\substack{=\sum_{k\in\mathbb{N}} \mathrm{id}^{\circledast k}(b_i)(tg_i)^k \\ \text{(by substituting } tg_i \\ \text{for } t \text{ in (15))}}} = \sum_{i=1}^{n} \sum_{k \in \mathbb{N}} \mathrm{id}^{\circledast k}(b_i) \underbrace{(tg_i)^k}_{=t^k g_i^k} = \sum_{i=1}^{n} \sum_{k \in \mathbb{N}} \mathrm{id}^{\circledast k}(b_i)\, t^k g_i^k$$

$$= \sum_{k \in \mathbb{N}} \underbrace{\sum_{i=1}^{n} \mathrm{id}^{\circledast k}(b_i)\, g_i^k}_{\substack{=0 \\ \text{(by (16))}}} t^k = 0.$$

Multiplying this equality by $\prod_{j=1}^{n} (1-tg_j)^{m_j+1}$, we obtain

$$\sum_{i=1}^{n} Q_i(tg_i) \prod_{j \neq i} (1-tg_j)^{m_j+1} = 0.$$

This is an equality in the polynomial ring $B[t]$. Hence, we can apply the B-algebra homomorphism

$$B[t] \to B\left[t, t^{-1}\right], \qquad t \mapsto t^{-1}$$

(into the Laurent polynomial ring $B\left[t, t^{-1}\right]$) to this equality. We obtain

$$\sum_{i=1}^{n} Q_i\left(\frac{g_i}{t}\right) \prod_{j \neq i}\left(1-\frac{g_j}{t}\right)^{m_j+1} = 0.$$

Multiplying this equality with $t^{m_1+m_2+\cdots+m_n+n-1}$, we transform this equality into

$$\sum_{i=1}^{n} t^{m_i} Q_i\left(\frac{g_i}{t}\right) \prod_{j \neq i}\left(t-g_j\right)^{m_j+1} = 0 \tag{17}$$

(an equality in the Laurent polynomial ring $B\left[t, t^{-1}\right]$).

For each $i \in \{1, 2, \ldots, n\}$, we set

$$R_i(t) = t^{m_i} Q_i\left(\frac{g_i}{t}\right) \in B\left[t, t^{-1}\right].$$

This $R_i(t)$ is actually a polynomial in $B[t]$ (since Q_i is a polynomial of degree $\leq m_i$). Using the definition of $R_i(t)$, the equality (17) rewrites as

$$\sum_{i=1}^{n} R_i(t) \prod_{j \neq i}\left(t-g_j\right)^{m_j+1} = 0. \tag{18}$$

Now fix $h \in \{1, 2, \ldots, n\}$. We have $m_h \in \mathbb{N}$ (since each m_i belongs to $\mathbb{N}$), so that $m_h + 1$ is a positive integer. Therefore, $0^{m_h+1} = 0$. In other words, $\left(g_h - g_h\right)^{m_h+1} = 0$.

The equality (18) is an equality in the polynomial ring $B[t]$ (since each m_i belongs to $\mathbb{N}$, and since each $R_i(t)$ is a polynomial in $B[t]$), so we can substitute g_h for t in it. We thus obtain

$$\sum_{i=1}^{n} R_i\left(g_h\right) \prod_{j \neq i}\left(g_h-g_j\right)^{m_j+1} = 0. \tag{19}$$

But all addends on the left hand side of this equality are 0 except for the addend with $i = h$ (since the product $\prod_{j \neq i}\left(g_h-g_j\right)^{m_j+1}$ contains the factor $\left(g_h-g_h\right)^{m_h+1} = 0$ unless $i = h$). Thus, the equality (19) simplifies to

$$R_h\left(g_h\right) \prod_{j \neq h}\left(g_h-g_j\right)^{m_j+1} = 0.$$

Since all the factors $g_h - g_j$ (with $j \neq h$) are regular elements of B (by Assumption 1), we can cancel $\prod_{j \neq h}\left(g_h-g_j\right)^{m_j+1}$ from this equality, and obtain $R_h\left(g_h\right) = 0$.

But recall that $Q_h(t) \in B[t]$ is a polynomial of degree $\leq m_h$, and we have $R_h(t) = t^{m_h} Q_h\left(\frac{g_h}{t}\right)$ (by the definition of R_h). Hence, (13) (applied to $A = B$, $m = m_h$, $u = g_h$, $F(t) = Q_h(t)$ and $G(t) = R_h(t)$) yields $R_h\left(g_h\right) = g_h^{m_h} Q_h(1)$. Hence,

$g_h^{m_h} Q_h(1) = R_h(g_h) = 0$, so that $Q_h(1) = 0$ (since Assumption 2 shows that $g_h \in B$ is regular).

But the definition of Q_h yields

$$Q_h(t) = \sum_{k=0}^{m_h} (-1)^k (\eta\epsilon - \mathrm{id})^{\circledast k}(b_h)\, t^k (1-t)^{m_h - k}.$$

Substituting 1 for t in this equality, we find

$$\begin{aligned} Q_h(1) &= \sum_{k=0}^{m_h} (-1)^k (\eta\epsilon - \mathrm{id})^{\circledast k}(b_h) \underbrace{1^k}_{=1} \underbrace{(1-1)^{m_h-k}}_{=0^{m_h-k}=\begin{cases}1, & \text{if } k = m_h;\\ 0, & \text{if } k \neq m_h\end{cases}} \\ &= \sum_{k=0}^{m_h} (-1)^k (\eta\epsilon - \mathrm{id})^{\circledast k}(b_h) \begin{cases}1, & \text{if } k = m_h;\\ 0, & \text{if } k \neq m_h\end{cases} \\ &= (-1)^{m_h} (\eta\epsilon - \mathrm{id})^{\circledast m_h}(b_h). \end{aligned}$$

Hence, $(-1)^{m_h} (\eta\epsilon - \mathrm{id})^{\circledast m_h}(b_h) = Q_h(1) = 0$. Therefore, $(\eta\epsilon - \mathrm{id})^{\circledast m_h}(b_h) = 0$.

Recall that m_h is the smallest degree upper-bound of b_h (since this is how m_h was defined). Thus, every nonnegative integer $n > m_h$ satisfies the equality $(\eta\epsilon - \mathrm{id})^{\circledast n}(b_h) = 0$ (by the definition of a degree upper-bound). Since $n = m_h$ also satisfies this equality (because we just showed that $(\eta\epsilon - \mathrm{id})^{\circledast m_h}(b_h) = 0$), we thus conclude that every nonnegative integer $n > m_h - 1$ satisfies $(\eta\epsilon - \mathrm{id})^{\circledast n}(b_h) = 0$. In other words, $m_h - 1$ is a degree-upper bound of b_h (by the definition of a degree upper-bound). Thus, m_h is not the **smallest** degree-upper bound of b_h (since $m_h - 1$ is smaller). This contradicts our definition of m_h. This contradiction completes our proof of Theorem 4.7. □

4.3. Appendix: The id-unipotents form a subalgebra

In this subsection, we shall show that the id-unipotent elements in a commutative **k**-bialgebra form a **k**-subalgebra. The proof will rely on a sequence of lemmas. We begin with two identities for binomial coefficients:

Lemma 4.16. *Let $N \in \mathbb{N}$. Let $(a_0, a_1, \ldots, a_N)$ and $(b_0, b_1, \ldots, b_N)$ be two $(N+1)$-tuples of rational numbers. Assume that*

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0, 1, \ldots, N\}.$$

Then,

$$a_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \qquad \text{for each } n \in \{0, 1, \ldots, N\}.$$

Lemma 4.17. *Let $a, b, m \in \mathbb{N}$. Then,*

$$\binom{m}{a}\binom{m}{b} = \sum_{i=a}^{a+b} \binom{i}{a}\binom{a}{a+b-i}\binom{m}{i}.$$

Both of these lemmas are not hard to prove; they are also easily found in the literature (e.g., Lemma 4.16 is [Grinbe17, Proposition 7.26], while Lemma 4.17 is [Grinbe17, Proposition 3.37]). Note that we have

$$\binom{n}{i} = 0 \tag{20}$$

for any $n, i \in \mathbb{N}$ satisfying $i > n$. Thus, the nonzero addends on the right hand side in Lemma 4.17 don't start until $i = \max\{a, b\}$.

The following modified version of Lemma 4.16 will be useful to us:[6]

Lemma 4.18. *Let A be an abelian group, written additively. Let $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ be two sequences of elements of A. Assume that*

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \mathbb{N}.$$

Then,

$$a_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \qquad \text{for each } n \in \mathbb{N}.$$

First proof of Lemma 4.18. The proof of Lemma 4.16 that was given in [Grinbe17, proof of Proposition 7.26] can be immediately reused as a proof of Lemma 4.18 (after removing all inequalities of the form "$n \leq N$", and after replacing every appearance of "$\{0, 1, \ldots, N\}$" by "$\mathbb{N}$"). □

Second proof of Lemma 4.18 (sketched). We will interpret binomial transforms in terms of sequence transformations (see [GoF04] for motivations and details). A row-finite matrix will mean a family

$$(M[n,k])_{n,k\geq 0} \qquad \text{with } M[n,k] \in \mathbf{k}$$

(i.e., a matrix of type $(\mathbb{N}, \mathbb{N})$ with elements in $\mathbf{k}$, in the terminology of [Bourba89, Chapter II, §10]) with the property that for every fixed row index n, the sequence $(M[n,k])_{k\geq 0}$ has finite support. We let $\mathcal{L}(\mathbf{k}^{\mathbb{N}})$ be the algebra of row-finite matrices; its product is given by the usual formula[7]

$$(M_1 M_2)[i,j] = \sum_{k\in\mathbb{N}} M_1[i,k] M_2[k,j]\ . \tag{21}$$

[6] An "abelian group, written additively" means an abelian group whose binary operation is denoted by $+$ and whose neutral element is denoted by 0.

[7] This is just the definition in [Bourba89, Chapter II, §10, (3)], extended a bit.

Any row-finite matrix $M \in \mathcal{L}(\mathbf{k}^{\mathbb{N}})$ canonically acts on $A^{\mathbb{N}}$ for any $\mathbf{k}$-module A: Namely, if $a = (a_n)_{n\geq 0} \in A^{\mathbb{N}}$ is a sequence of elements of A, then Ma is defined to be the sequence $(b_n)_{n\geq 0} \in A^{\mathbb{N}}$ with

$$b_n = \sum_{k\geq 0} M[n,k]\, a_k \qquad \text{for all } n \in \mathbb{N}. \tag{22}$$

This action gives rise to a $\mathbf{k}$-algebra homomorphism

$$\Phi_1 : \ \mathcal{L}(\mathbf{k}^{\mathbb{N}}) \to \operatorname{End}(A^{\mathbb{N}}), \tag{23}$$

which is injective in the case when $A = \mathbf{k}$ (but neither injective nor surjective in the general case). Applying this to $\mathbf{k} = \mathbb{Q}$ and $A = \mathbb{Q}$, we thus have an injective $\mathbb{Q}$-algebra homomorphism $\Phi_1 : \ \mathcal{L}(\mathbb{Q}^{\mathbb{N}}) \to \operatorname{End}(\mathbb{Q}^{\mathbb{N}})$. We also have a $\mathbb{Q}$-vector space isomorphism

$$\begin{aligned} \mathbb{Q}^{\mathbb{N}} &\xrightarrow{\cong} \mathbb{Q}[[z]], \\ (a_n)_{n\in\mathbb{N}} &\mapsto \sum_{n\geq 0} a_n \frac{z^n}{n!} \end{aligned}$$

(where z is a formal variable), thus a $\mathbb{Q}$-algebra isomorphism $\operatorname{End}(\mathbb{Q}^{\mathbb{N}}) \to \operatorname{End}(\mathbb{Q}[[z]])$. Composing the latter with Φ_1, we get an injective $\mathbb{Q}$-algebra homomorphism $\Phi_2 : \mathcal{L}(\mathbb{Q}^{\mathbb{N}}) \to \operatorname{End}(\mathbb{Q}[[z]])$. Explicitly, for any power series $f = f(z) = \sum\limits_{n\geq 0} a_n \frac{z^n}{n!} \in \mathbb{Q}[[z]]$ and any row-finite matrix $M \in \mathcal{L}(\mathbb{Q}^{\mathbb{N}})$, we have

$$\Phi_2(M)(f) = \sum_{n\geq 0} b_n \frac{z^n}{n!} = \sum_{n\geq 0} \sum_{k\geq 0} M[n,k]\, a_k \frac{z^n}{n!}\,. \tag{24}$$

Now, let $M_1 \in \mathcal{L}(\mathbb{Z}^{\mathbb{N}}) \subseteq \mathcal{L}(\mathbb{Q}^{\mathbb{N}})$ be the row-finite matrix whose entries are

$$M_1[n,i] := (-1)^i \binom{n}{i}. \tag{25}$$

Then, the assumption in Lemma 4.18 is saying that $b = M_1 a$, where $a, b \in A^{\mathbb{N}}$ are given by $a = (a_n)_{n\geq 0}$ and $b = (b_n)_{n\geq 0}$. Likewise, the claim of Lemma 4.18 is saying that $a = M_1 b$. Hence, in order to prove Lemma 4.18, it suffices to show that $M_1^2 a = a$. Thus, it suffices to show that $M_1^2 = I_{\mathcal{L}(\mathbb{Z}^{\mathbb{N}})}$ (the identity matrix in $\mathcal{L}(\mathbb{Z}^{\mathbb{N}})$).

But this can be done via the injective $\mathbb{Z}$-algebra homomorphism $\Phi_2 : \ \mathcal{L}(\mathbb{Q}^{\mathbb{N}}) \to \operatorname{End}(\mathbb{Q}[[z]])$. Indeed, a direct calculation shows that any $f \in \mathbb{Q}[[z]]$ satisfies

$$\Phi_2(M_1)(f)(z) = f(-z)e^z,$$

and hence

$$\Phi_2(M_1^2)(f)(z) = \Phi_2(M_1)(f(-z)e^z) = (f(-(-z))e^{-z})e^z = f(z).$$

This shows that $\Phi_2(M_1^2) = \mathrm{id} = \Phi_2(I_{\mathcal{L}(\mathbb{Q}^{\mathbb{N}})})$. Since Φ_2 is injective, this entails $M_1^2 = I_{\mathcal{L}(\mathbb{Q}^{\mathbb{N}})} = I_{\mathcal{L}(\mathbb{Z}^{\mathbb{N}})}$ and proves Lemma 4.18 (as every abelian group is a $\mathbb{Z}$-module). $\square$

Our next lemma is a classical fact about finite differences:

Lemma 4.19. *Let A be an abelian group, written additively. Let $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ be a sequence of elements of A. Let $m \geq -1$ be an integer. Then, the following two statements are equivalent:*

1. *We have $\sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = 0$ for every integer $n > m$.*
2. *There exist $m+1$ elements $c_0, c_1, \ldots, c_m$ of A such that every $n \in \mathbb{N}$ satisfies $a_n = \sum_{i=0}^{m} \binom{n}{i} c_i$.*

The sequences $(a_0, a_1, a_2, \ldots)$ satisfying these two equivalent statements can be regarded as a generalization of polynomial sequences (i.e., sequences whose n-th entry is given by evaluating a fixed integer-valued polynomial at n).

Proof of Lemma 4.19. We must prove the equivalence of Statement 1 and Statement 2. We shall do so by proving the implications $1 \Longrightarrow 2$ and $2 \Longrightarrow 1$ separately:

Proof of the implication $1 \Longrightarrow 2$: Let us first show that Statement 1 implies Statement 2.

Indeed, assume that Statement 1 holds. In other words, we have

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = 0 \tag{26}$$

for every integer $n > m$.

We shall now show that Statement 2 holds.

Indeed, let us set

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \tag{27}$$

for each $n \in \mathbb{N}$. Then, for every integer $n > m$, we have

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = 0$$

(by (26)). Renaming n as i in this statement, we obtain the following: For every integer $i > m$, we have

$$b_i = 0. \tag{28}$$

Furthermore, recall that $b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i$ for each $n \in \mathbb{N}$. Thus, Lemma 4.16 shows that we have

$$a_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \tag{29}$$

for each $n \in \mathbb{N}$.

Now, let $n \in \mathbb{N}$. Let $N = \max\{n, m\}$; then, $N \geq n$ and $N \geq m$. Thus, $0 \leq n \leq N$ and $0 \leq m \leq N$. Now, comparing

$$\begin{aligned}
\sum_{i=0}^{N} \binom{n}{i} (-1)^i b_i &= \sum_{i=0}^{n} \underbrace{\binom{n}{i} (-1)^i}_{=(-1)^i \binom{n}{i}} b_i + \sum_{i=n+1}^{N} \underbrace{\binom{n}{i}}_{\substack{=0 \\ \text{(by (20),} \\ \text{since } i \geq n+1 > n)}} (-1)^i b_i \\
&\qquad \text{(here, we have split the sum at } i = n \text{, since } 0 \leq n \leq N) \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i + \underbrace{\sum_{i=n+1}^{N} 0 (-1)^i b_i}_{=0} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \\
&= a_n \qquad \text{(by (29))}
\end{aligned}$$

with

$$\begin{aligned}
\sum_{i=0}^{N} \binom{n}{i} (-1)^i b_i &= \sum_{i=0}^{m} \binom{n}{i} (-1)^i b_i + \sum_{i=m+1}^{N} \binom{n}{i} (-1)^i \underbrace{b_i}_{\substack{=0 \\ \text{(by (28),} \\ \text{since } i \geq m+1 > m)}} \\
&\qquad \text{(here, we have split the sum at } i = m \text{, since } 0 \leq m \leq N) \\
&= \sum_{i=0}^{m} \binom{n}{i} (-1)^i b_i + \underbrace{\sum_{i=m+1}^{N} \binom{n}{i} (-1)^i 0}_{=0} = \sum_{i=0}^{m} \binom{n}{i} (-1)^i b_i,
\end{aligned}$$

we obtain

$$a_n = \sum_{i=0}^{m} \binom{n}{i} (-1)^i b_i.$$

Forget that we fixed n. We thus have proved that every $n \in \mathbb{N}$ satisfies $a_n = \sum_{i=0}^{m} \binom{n}{i} (-1)^i b_i$. Thus, there exist $m+1$ elements $c_0, c_1, \ldots, c_m$ of A such that every $n \in \mathbb{N}$ satisfies $a_n = \sum_{i=0}^{m} \binom{n}{i} c_i$ (namely, these $m+1$ elements are given by $c_i = (-1)^i b_i$). In other words, Statement 2 holds.

We thus have proved the implication $1 \Longrightarrow 2$.

Proof of the implication $2 \Longrightarrow 1$: Let us now show that Statement 2 implies Statement 1.

Indeed, assume that Statement 2 holds. That is, there exist $m+1$ elements $c_0, c_1, \ldots, c_m$ of A such that every $n \in \mathbb{N}$ satisfies

$$a_n = \sum_{i=0}^{m} \binom{n}{i} c_i. \tag{30}$$

Consider these $c_0, c_1, \ldots, c_m$.

We must prove that Statement 1 holds. In other words, we must prove that we have $\sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = 0$ for every integer $n > m$.

Extend the $(m+1)$-tuple $(c_0, c_1, \ldots, c_m) \in A^{m+1}$ to an infinite sequence $(c_0, c_1, c_2, \ldots) \in A^{\mathbb{N}}$ by setting

$$(c_i = 0 \qquad \text{for all integers } i > m). \tag{31}$$

Furthermore, define a sequence $(d_0, d_1, d_2, \ldots) \in A^{\mathbb{N}}$ by setting

$$\left(d_i = (-1)^i c_i \qquad \text{for all } i \in \mathbb{N}\right). \tag{32}$$

Then, each $i \in \mathbb{N}$ satisfies

$$(-1)^i \underbrace{d_i}_{\substack{=(-1)^i c_i \\ \text{(by (32))}}} = \underbrace{(-1)^i (-1)^i}_{=(-1)^{2i}=1} c_i = c_i. \tag{33}$$

Let $n \in \mathbb{N}$. Let $N = \max\{n, m\}$; then, $N \geq n$ and $N \geq m$. Thus, $0 \leq n \leq N$ and $0 \leq m \leq N$. Now, comparing

$$\sum_{i=0}^{N} \binom{n}{i} c_i = \sum_{i=0}^{n} \binom{n}{i} c_i + \sum_{i=n+1}^{N} \underbrace{\binom{n}{i}}_{\substack{=0 \\ \text{(by (20),} \\ \text{since } i \geq n+1 > n)}} c_i$$

(here, we have split the sum at $i = n$, since $0 \leq n \leq N$)

$$= \sum_{i=0}^{n} \binom{n}{i} c_i + \underbrace{\sum_{i=n+1}^{N} 0 c_i}_{=0} = \sum_{i=0}^{n} \binom{n}{i} c_i$$

with

$$\sum_{i=0}^{N} \binom{n}{i} c_i = \sum_{i=0}^{m} \binom{n}{i} c_i + \sum_{i=m+1}^{N} \binom{n}{i} \underbrace{c_i}_{\substack{=0 \\ \text{(by (31),} \\ \text{since } i \geq m+1 > m)}}$$

(here, we have split the sum at $i = m$, since $0 \leq m \leq N$)

$$= \sum_{i=0}^{m} \binom{n}{i} c_i + \underbrace{\sum_{i=m+1}^{N} \binom{n}{i} 0}_{=0} = \sum_{i=0}^{m} \binom{n}{i} c_i = a_n \qquad \text{(by (30))},$$

we obtain

$$a_n = \sum_{i=0}^{n} \binom{n}{i} \underbrace{c_i}_{\substack{=(-1)^i d_i \\ \text{(by (33))}}} = \sum_{i=0}^{n} \binom{n}{i} (-1)^i d_i = \sum_{i=0}^{n} (-1)^i \binom{n}{i} d_i.$$

Now, forget that we fixed n. We thus have shown that $a_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} d_i$ for each $n \in \mathbb{N}$. Thus, Lemma 4.18 (applied to d_n and a_n instead of a_n and b_n) shows that

$$d_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \mathbb{N}. \tag{34}$$

Now, let $n > m$ be an integer. Then, (31) (applied to $i = n$) yields $c_n = 0$. But (32) (applied to $i = n$) yields $d_n = (-1)^n \underbrace{c_n}_{=0} = 0$. But (34) yields $d_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i$. Comparing the latter two equalities, we obtain $\sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = 0$.

Forget that we fixed n. We thus have shown that $\sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = 0$ for every integer $n > m$. In other words, Statement 1 holds.

We thus have proved the implication $2 \Longrightarrow 1$.

Having now shown both implications $1 \Longrightarrow 2$ and $2 \Longrightarrow 1$, we conclude that Statement 1 and Statement 2 are equivalent. This proves Lemma 4.19. □

Definition 4.20. Let A be an abelian group, written additively. Let $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ be a sequence of elements of A. Let $m \geq -1$ be an integer. We say that the sequence $(a_0, a_1, a_2, \ldots)$ is m-polynomial if the two equivalent statements 1 and 2 of Lemma 4.19 are satisfied.

Lemma 4.21. *Let A be an abelian group, written additively. Let $p \geq -1$ and $q \geq -1$ be two integers such that $p + q \geq -1$. Let $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ be a p-polynomial sequence of elements of A. Let $(b_0, b_1, b_2, \ldots) \in A^{\mathbb{N}}$ be a q-polynomial sequence of elements of A. Then, $(a_0 b_0, a_1 b_1, a_2 b_2, \ldots) \in A^{\mathbb{N}}$ is a $(p+q)$-polynomial sequence of elements of A.*

Proof of Lemma 4.21. We have assumed that the sequence $(a_0, a_1, a_2, \ldots)$ is p-polynomial. In other words, this sequence satisfies the two equivalent statements 1 and 2 of Lemma 4.19 for $m = p$ (by the definition of "p-polynomial"). Thus, in particular, it satisfies Statement 2 of Lemma 4.19 for $m = p$. In other words, there exist $p + 1$ elements $c_0, c_1, \ldots, c_p$ of A such that every $n \in \mathbb{N}$ satisfies $a_n = \sum_{i=0}^{p} \binom{n}{i} c_i$. Consider these $c_0, c_1, \ldots, c_p$, and denote them by $u_0, u_1, \ldots, u_p$. Thus, $u_0, u_1, \ldots, u_p$ are $p + 1$ elements of A with the property that every $n \in \mathbb{N}$ satisfies

$$a_n = \sum_{i=0}^{p} \binom{n}{i} u_i. \tag{35}$$

The same argument (but applied to the sequence $(b_0, b_1, b_2, \ldots)$ and the integer q instead of the sequence $(a_0, a_1, a_2, \ldots)$ and the integer p) helps us construct $q+1$ elements $v_0, v_1, \ldots, v_q$ of A with the property that every $n \in \mathbb{N}$ satisfies

$$b_n = \sum_{i=0}^{q} \binom{n}{i} v_i. \tag{36}$$

Consider these $q+1$ elements $v_0, v_1, \ldots, v_q$.

For each $i \in \mathbb{N}$, we set

$$w_i = \sum_{\substack{(j,k) \in \mathbb{N} \times \mathbb{N}; \\ j \leq p;\ k \leq q; \\ j \leq i \leq j+k}} \binom{i}{j} \binom{j}{j+k-i} u_j v_k. \tag{37}$$

Thus, if $i \in \mathbb{N}$ satisfies $i > p+q$, then

$$w_i = 0. \tag{38}$$

[*Proof of* (38)*:* Let $i \in \mathbb{N}$ satisfy $i > p+q$. Then, there exists no $(j,k) \in \mathbb{N} \times \mathbb{N}$ satisfying $j \leq p$ and $k \leq q$ and $j \leq i \leq j+k$ (since any such (j,k) would satisfy $i \leq \underbrace{j}_{\leq p} + \underbrace{k}_{\leq q} \leq p+q$, which would contradict $i > p+q$). Hence, the sum on the right hand side of (37) is empty, and thus equals 0. Therefore, (37) rewrites as $w_i = 0$. This proves (38).]

Let $n \in \mathbb{N}$. Then, (35) yields

$$a_n = \sum_{i=0}^{p} \binom{n}{i} u_i = \sum_{j=0}^{p} \binom{n}{j} u_j.$$

Meanwhile, (36) yields

$$b_n = \sum_{i=0}^{q} \binom{n}{i} v_i = \sum_{k=0}^{q} \binom{n}{k} v_k.$$

Multiplying these two equalities, we obtain

$$a_n b_n = \left(\sum_{j=0}^{p} \binom{n}{j} u_j\right)\left(\sum_{k=0}^{q} \binom{n}{k} v_k\right) = \underbrace{\sum_{j=0}^{p}\sum_{k=0}^{q}}_{= \sum\limits_{\substack{(j,k)\in\mathbb{N}\times\mathbb{N};\\ j\le p;\ k\le q}}} \underbrace{\binom{n}{j}\binom{n}{k}}_{\substack{=\sum\limits_{i=j}^{j+k}\binom{i}{j}\binom{j}{j+k-i}\binom{n}{i} \\ \text{(by Lemma 4.17,} \\ \text{applied to } m=n,\ a=j \text{ and } b=k)}} u_j v_k$$

$$= \sum_{\substack{(j,k)\in\mathbb{N}\times\mathbb{N};\\ j\le p;\ k\le q}} \underbrace{\sum_{i=j}^{j+k}}_{= \sum\limits_{\substack{i\in\mathbb{N};\\ j\le i\le j+k}}} \binom{i}{j}\binom{j}{j+k-i}\binom{n}{i} u_j v_k$$

$$= \underbrace{\sum_{\substack{(j,k)\in\mathbb{N}\times\mathbb{N};\\ j\le p;\ k\le q}} \sum_{\substack{i\in\mathbb{N};\\ j\le i\le j+k}}}_{= \sum\limits_{i\in\mathbb{N}} \sum\limits_{\substack{(j,k)\in\mathbb{N}\times\mathbb{N};\\ j\le p;\ k\le q;\\ j\le i\le j+k}}} \binom{i}{j}\binom{j}{j+k-i}\binom{n}{i} u_j v_k$$

$$= \sum_{i\in\mathbb{N}} \sum_{\substack{(j,k)\in\mathbb{N}\times\mathbb{N};\\ j\le p;\ k\le q;\\ j\le i\le j+k}} \binom{i}{j}\binom{j}{j+k-i}\binom{n}{i} u_j v_k$$

$$= \sum_{i\in\mathbb{N}} \binom{n}{i} \underbrace{\sum_{\substack{(j,k)\in\mathbb{N}\times\mathbb{N};\\ j\le p;\ k\le q;\\ j\le i\le j+k}} \binom{i}{j}\binom{j}{j+k-i} u_j v_k}_{\substack{=w_i \\ \text{(by (37))}}}$$

$$= \sum_{i\in\mathbb{N}} \binom{n}{i} w_i = \underbrace{\sum_{\substack{i\in\mathbb{N};\\ i\le p+q}}}_{= \sum\limits_{i=0}^{p+q}} \binom{n}{i} w_i + \sum_{\substack{i\in\mathbb{N};\\ i>p+q}} \binom{n}{i} \underbrace{w_i}_{\substack{=0 \\ \text{(by (38))}}}$$

$$= \sum_{i=0}^{p+q} \binom{n}{i} w_i + \underbrace{\sum_{\substack{i\in\mathbb{N};\\ i>p+q}} \binom{n}{i} 0}_{=0} = \sum_{i=0}^{p+q} \binom{n}{i} w_i.$$

Forget that we fixed n. We thus have shown that every $n \in \mathbb{N}$ satisfies $a_n b_n = \sum\limits_{i=0}^{p+q} \binom{n}{i} w_i$. Hence, there exist $p+q+1$ elements $c_0, c_1, \ldots, c_{p+q}$ of A such that every

$n \in \mathbb{N}$ satisfies $a_n b_n = \sum_{i=0}^{p+q} \binom{n}{i} c_i$ (namely, these $p+q+1$ elements are given by $c_i = w_i$). In other words, Statement 2 of Lemma 4.19 with m and $(a_0, a_1, a_2, \ldots)$ replaced by $p+q$ and $(a_0 b_0, a_1 b_1, a_2 b_2, \ldots)$ is satisfied. Thus, the two equivalent statements 1 and 2 of Lemma 4.19 with m and $(a_0, a_1, a_2, \ldots)$ replaced by $p+q$ and $(a_0 b_0, a_1 b_1, a_2 b_2, \ldots)$ is satisfied. In other words, the sequence $(a_0 b_0, a_1 b_1, a_2 b_2, \ldots)$ is $(p+q)$-polynomial (by the definition of "$(p+q)$-polynomial"). This proves Lemma 4.21. ☐

Lemma 4.22. *Let B be a $\mathbf{k}$-bialgebra. Let $b \in B$. Let $m \geq -1$ be an integer.*
Then, m is a degree-upper bound of b if and only if the sequence

$$\left(\mathrm{id}^{\circledast 0}(b), \mathrm{id}^{\circledast 1}(b), \mathrm{id}^{\circledast 2}(b), \ldots\right)$$

is m-polynomial.

Proof of Lemma 4.22. The elements $\eta\epsilon$ and id of the convolution algebra $(\mathrm{Hom}(B,B), \circledast)$ commute (since $\eta\epsilon$ is the unity of this algebra). Thus, the binomial formula shows that

$$(\eta\epsilon - \mathrm{id})^{\circledast n} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \mathrm{id}^{\circledast i}$$

for every $n \in \mathbb{N}$ (again because $\eta\epsilon$ is the unity of the convolution algebra). Hence, for every $n \in \mathbb{N}$, we have

$$(\eta\epsilon - \mathrm{id})^{\circledast n}(b) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \mathrm{id}^{\circledast i}(b). \tag{39}$$

Now, we have the following chain of equivalences:

$$\begin{aligned}
&(m \text{ is a degree-upper bound of } b) \\
\iff &\left((\eta\epsilon - \mathrm{id})^{\circledast n}(b) = 0 \text{ for every integer } n > m\right) \\
&\qquad \text{(by the definition of a "degree-upper bound")} \\
\iff &\left(\sum_{i=0}^{n} (-1)^i \binom{n}{i} \mathrm{id}^{\circledast i}(b) = 0 \text{ for every integer } n > m\right) \\
&\qquad \text{(by (39))} \\
\iff &\left(\text{Statement 1 of Lemma 4.19 holds for } A = B \text{ and } a_i = \mathrm{id}^{\circledast i}(b)\right) \\
\iff &\left(\text{the sequence } \left(\mathrm{id}^{\circledast 0}(b), \mathrm{id}^{\circledast 1}(b), \mathrm{id}^{\circledast 2}(b), \ldots\right) \text{ is } m\text{-polynomial}\right) \\
&\qquad \text{(by the definition of "}m\text{-polynomial").}
\end{aligned}$$

This proves Lemma 4.22. ☐

Proposition 4.23. *Let B be a commutative $\mathbf{k}$-bialgebra. Let $b, c \in B$. Let $p, q \geq -1$ be two integers with $p + q \geq -1$. Assume that p is a degree-upper bound of b. Assume that q is a degree-upper bound of c. Then, $p + q$ is a degree-upper bound of bc.*

Proof of Proposition 4.23. For each $k \in \mathbb{N}$, we know that the map $\mathrm{id}^{\circledast k} : B \to B$ is a $\mathbf{k}$-algebra homomorphism (by Lemma 4.11), and thus satisfies $\mathrm{id}^{\circledast k}(bc) = \mathrm{id}^{\circledast k}(b) \cdot \mathrm{id}^{\circledast k}(c)$. Hence,

$$\begin{aligned} &\left(\mathrm{id}^{\circledast 0}(bc), \mathrm{id}^{\circledast 1}(bc), \mathrm{id}^{\circledast 2}(bc), \ldots\right) \\ &= \left(\mathrm{id}^{\circledast 0}(b)\,\mathrm{id}^{\circledast 0}(c), \mathrm{id}^{\circledast 1}(b)\,\mathrm{id}^{\circledast 1}(c), \mathrm{id}^{\circledast 2}(b)\,\mathrm{id}^{\circledast 2}(c), \ldots\right). \end{aligned} \tag{40}$$

Lemma 4.22 (applied to $m = p$) shows that p is a degree-upper bound of b if and only if the sequence $\left(\mathrm{id}^{\circledast 0}(b), \mathrm{id}^{\circledast 1}(b), \mathrm{id}^{\circledast 2}(b), \ldots\right)$ is p-polynomial. Thus, the sequence $\left(\mathrm{id}^{\circledast 0}(b), \mathrm{id}^{\circledast 1}(b), \mathrm{id}^{\circledast 2}(b), \ldots\right)$ is p-polynomial (since p is a degree-upper bound of b). The same argument (applied to c and q instead of b and p) shows that the sequence $\left(\mathrm{id}^{\circledast 0}(c), \mathrm{id}^{\circledast 1}(c), \mathrm{id}^{\circledast 2}(c), \ldots\right)$ is q-polynomial. Hence, Lemma 4.21 (applied to $A = B$, $a_i = \mathrm{id}^{\circledast i}(b)$ and $b_i = \mathrm{id}^{\circledast i}(c)$) shows that $\left(\mathrm{id}^{\circledast 0}(b)\,\mathrm{id}^{\circledast 0}(c), \mathrm{id}^{\circledast 1}(b)\,\mathrm{id}^{\circledast 1}(c), \mathrm{id}^{\circledast 2}(b)\,\mathrm{id}^{\circledast 2}(c), \ldots\right)$ is a $(p+q)$-polynomial sequence of elements of B. In view of (40), this rewrites as follows:
$\left(\mathrm{id}^{\circledast 0}(bc), \mathrm{id}^{\circledast 1}(bc), \mathrm{id}^{\circledast 2}(bc), \ldots\right)$ is a $(p+q)$-polynomial sequence of elements of B.

But Lemma 4.22 (applied to $p+q$ and bc instead of m and b) shows that $p+q$ is a degree-upper bound of bc if and only if the sequence $\left(\mathrm{id}^{\circledast 0}(bc), \mathrm{id}^{\circledast 1}(bc), \mathrm{id}^{\circledast 2}(bc), \ldots\right)$ is $(p+q)$-polynomial. Hence, $p+q$ is a degree-upper bound of bc (since the sequence $\left(\mathrm{id}^{\circledast 0}(bc), \mathrm{id}^{\circledast 1}(bc), \mathrm{id}^{\circledast 2}(bc), \ldots\right)$ is $(p+q)$-polynomial). This proves Proposition 4.23. ☐

Corollary 4.24. *Let B be a commutative $\mathbf{k}$-bialgebra. Let L denote the set of all id-unipotent elements of B. Then, L is a $\mathbf{k}$-subalgebra of B.*

Proof of Corollary 4.24. We have already seen in Remark 4.8 that L is a $\mathbf{k}$-submodule of B. Thus, it suffices to show that $1 \in L$ and that all $b, c \in L$ satisfy $bc \in L$.

It is easy to see that $1 \in L$: Indeed, it is easy to see (by induction) that $(\eta\epsilon - \mathrm{id})^{\circledast n}(1) = 0$ for every positive integer n. Thus, 0 is a degree-upper bound of 1. Hence, the element 1 is id-unipotent, i.e., we have $1 \in L$.

It remains to show that all $b, c \in L$ satisfy $bc \in L$. So let $b, c \in L$ be arbitrary. Thus, b and c are two id-unipotent elements of B. Clearly, $b \in B$ has a degree-upper bound (since b is id-unipotent); let us denote this bound by p. We WLOG assume that p is nonnegative (since otherwise, we can replace p by 0). Likewise, we can find a nonnegative degree-upper bound q of c. Now, Proposition 4.23 shows that

$p+q$ is a degree-upper bound of bc. Hence, bc is id-unipotent. In other words, $bc \in L$.

We thus have shown that all $b, c \in L$ satisfy $bc \in L$. As we have seen, this concludes the proof of Corollary 4.24. □

5. Linear independence in the dual algebra

So far we have considered grouplike elements in coalgebras and bialgebras. A related (and, occasionally, equivalent) concept are the characters of an algebra.

5.1. Some words on characters

We recall that a character of a $\mathbf{k}$-algebra A means a $\mathbf{k}$-algebra homomorphism from A to $\mathbf{k}$. Before we study linear independence questions for characters, let us briefly survey their relation to grouplike elements.

The simplest way to connect characters with grouplike elements is the following (easily verified) fact:

Proposition 5.1. *Let C be a $\mathbf{k}$-coalgebra that is free as a $\mathbf{k}$-module. Let $c \in C$. Consider the $\mathbf{k}$-linear map $c^{\vee\vee} : C^\vee \to \mathbf{k}$ that sends each $f \in C^\vee$ to $f(c) \in \mathbf{k}$. Then, $c^{\vee\vee}$ is a character of the $\mathbf{k}$-algebra $C^\vee$ if and only if c is grouplike in C.*

Proof of Proposition 5.1 (sketched). We shall prove the two equivalences

$$\begin{aligned} &(\Delta(c) = c \otimes c) \\ &\iff \left(c^{\vee\vee}(f \circledast g) = c^{\vee\vee}(f) \cdot c^{\vee\vee}(g) \text{ for all } f, g \in C^\vee\right) \end{aligned} \tag{41}$$

and

$$(\epsilon(c) = 1) \iff \left(c^{\vee\vee}(\epsilon) = 1\right). \tag{42}$$

Indeed, the equivalence (42) follows from the fact that $c^{\vee\vee}(\epsilon) = \epsilon(c)$ (which is a direct consequence of the definition of $c^{\vee\vee}$). Let us now prove the equivalence (41).

The $\mathbf{k}$-module C is free. Hence, it is easy to prove the following fact:

> *Fact 1:* Let x and y be two elements of $C \otimes C$. Then, $x = y$ if and only if we have
>
> $$(f \otimes g)(x) = (f \otimes g)(y) \qquad \text{for all } f, g \in C^\vee.$$

Fact 1 is often stated as "the pure tensors in $C^\vee \otimes C^\vee$ separate $C \otimes C$". It can be proved by picking a basis $(e_i)_{i \in I}$ of C and its corresponding dual "basis" $\left(e_i^*\right)_{i \in I}$ of $C^\vee$ (with $e_i^*(e_j)$ being the Kronecker delta $\delta_{i,j}$ for all $i, j \in I$), and arguing that $\left(e_i^* \otimes e_j^*\right)_{(i,j) \in I \times I}$ is the dual "basis" to the basis $\left(e_i \otimes e_j\right)_{(i,j) \in I \times I}$ of $C \otimes C$.

Applying Fact 1 to $x = \Delta(c)$ and $y = c \otimes c$, we obtain the following equivalence:

$$\begin{aligned} &(\Delta(c) = c \otimes c) \\ &\iff \left((f \otimes g)(\Delta(c)) = (f \otimes g)(c \otimes c) \text{ for all } f, g \in C^\vee\right). \end{aligned} \tag{43}$$

But the multiplication map $\mu_{\mathbf{k}} : \mathbf{k} \otimes \mathbf{k} \to \mathbf{k}$ of $\mathbf{k}$ is bijective; thus, for any $f, g \in C^\vee$, we have the following chain of equivalences:

$$\begin{aligned} &((f \otimes g)(\Delta(c)) = (f \otimes g)(c \otimes c)) \\ &\iff (\mu_{\mathbf{k}}((f \otimes g)(\Delta(c))) = \mu_{\mathbf{k}}((f \otimes g)(c \otimes c))) \\ &\iff ((f \circledast g)(c) = f(c) \cdot g(c)) \\ &\qquad \left(\begin{array}{c} \text{since } \mu_{\mathbf{k}}((f \otimes g)(\Delta(c))) = \underbrace{(\mu_{\mathbf{k}} \circ (f \otimes g) \circ \Delta)}_{\substack{= f \circledast g \\ \text{(by the definition of } \circledast\text{)}}}(c) = (f \circledast g)(c) \\ \\ \text{and } \mu_{\mathbf{k}}((f \otimes g)(c \otimes c)) = \mu_{\mathbf{k}}(f(c) \otimes g(c)) = f(c) \cdot g(c) \end{array} \right) \\ &\iff \left(c^{\vee\vee}(f \circledast g) = c^{\vee\vee}(f) \cdot c^{\vee\vee}(g)\right) \\ &\qquad \left(\begin{array}{c} \text{since the definition of } c^{\vee\vee} \text{ yields } c^{\vee\vee}(f \circledast g) = (f \circledast g)(c) \\ \text{and } c^{\vee\vee}(f) = f(c) \text{ and } c^{\vee\vee}(g) = g(c) \end{array} \right). \end{aligned}$$

Hence, the equivalence (43) is saying the same thing as the equivalence (41). Thus, the latter equivalence is proven.

We have now proved both equivalences (41) and (42). But the definition of grouplike elements yields the following chain of equivalences:

$$\begin{aligned} &(c \text{ is grouplike in } C) \\ &\iff (\Delta(c) = c \otimes c) \text{ and } (\epsilon(c) = 1) \\ &\iff \left(c^{\vee\vee}(f \circledast g) = c^{\vee\vee}(f) \cdot c^{\vee\vee}(g) \text{ for all } f, g \in C^\vee\right) \text{ and } \left(c^{\vee\vee}(\epsilon) = 1\right) \\ &\qquad \text{(by (41) and (42))} \\ &\iff \left(c^{\vee\vee} \text{ is a } \mathbf{k}\text{-algebra homomorphism from } C^\vee \text{ to } \mathbf{k}\right) \\ &\qquad \left(\text{since the map } c^{\vee\vee} \text{ is } \mathbf{k}\text{-linear, and } \epsilon \text{ is the unity of the } \mathbf{k}\text{-algebra } C^\vee\right) \\ &\iff \left(c^{\vee\vee} \text{ is a character of the } \mathbf{k}\text{-algebra } C^\vee\right). \end{aligned}$$

This proves Proposition 5.1. □

Proposition 5.1 can be used to characterize the characters of some algebras as grouplikes. To wit: If A is a $\mathbf{k}$-algebra that is finite free as a $\mathbf{k}$-module, then the dual $\mathbf{k}$-module $A^\vee$ canonically receives the structure of a $\mathbf{k}$-coalgebra[8], whose dual $(A^\vee)^\vee$ is canonically isomorphic to the $\mathbf{k}$-algebra A (via the standard $\mathbf{k}$-module

[8]This structure can be defined as follows: Its comultiplication $\Delta_{A^\vee} : A^\vee \to A^\vee \otimes A^\vee$ is the composition of the map $\mu_A^\vee : A^\vee \to (A \otimes A)^\vee$ (which is the dual of the multiplication $\mu_A : A \otimes A \to A$ of A) with the canonical isomorphism $(A \otimes A)^\vee \to A^\vee \otimes A^\vee$ (which exists because A is finite free). The counit $\epsilon_{A^\vee} : A^\vee \to \mathbf{k}$ of $A^\vee$ is the dual of the unit map $\eta_A : \mathbf{k} \to A$ of A.

isomorphism $A \to (A^\vee)^\vee$). Thus, Proposition 5.1 yields that the characters of a $\mathbf{k}$-algebra A that is finite free as a $\mathbf{k}$-module are precisely the grouplike elements of its dual coalgebra $A^\vee$.

There are some ways to extend this result to $\mathbf{k}$-algebras A that are not finite free; the best-known case is when $\mathbf{k}$ is a field. In this case, every $\mathbf{k}$-algebra A has a Hopf dual A^o (also known as the zero dual or Sweedler dual), which is a $\mathbf{k}$-coalgebra whose grouplike elements are precisely the characters of A. (See [Sweedl69, Section 6.0] for the definition and fundamental properties of this Hopf dual and [Duc97, DucTol09] for questions linked to rationality.) When $\mathbf{k}$ is not a field, this Hopf dual is not defined any more. Indeed, the canonical map $M^\vee \otimes N^\vee \to (M \otimes N)^\vee$ that is defined for any two $\mathbf{k}$-modules M and N is known to be injective when $\mathbf{k}$ is a field, but may fail to be injective even when $\mathbf{k}$ is an integral domain[9]. Other concepts can be used to salvage the relation between grouplikes and characters: bases in duality, dual laws constructed directly [Bui12, BDMKT16, Ducham01], pseudo-coproducts [PatReu02, Section 2]. We shall not delve on these things; but the upshot for us is that while the concepts of characters of an algebra and grouplike elements of a coalgebra are closely connected, neither concept subsumes the other.

For this reason, our third main result[10] will be stated directly in the language of characters on a bialgebra (i.e., algebra morphisms from this bialgebra to the base ring).

5.2. Examples of characters

Before we state our result, let us see some examples of characters of $\mathbf{k}$-bialgebras. The following notation will come rather useful:

Definition 5.2. Let a be an element of a ring. Then, the Kleene star a^* of a is defined to be the sum $\sum\limits_{i=0}^{\infty} a^i = 1 + a + a^2 + a^3 + \cdots$, assuming that this sum is well-defined (e.g., because a is nilpotent or the sum converges for some other reason). Note that $a^* = \dfrac{1}{1-a}$ whenever a^* is defined.

The dual $\mathcal{B}^\vee$ of a $\mathbf{k}$-bialgebra $\mathcal{B}$ is a $\mathbf{k}$-algebra, thus a ring; oftentimes, this ring has a topology on it. (For example, if $\mathcal{B}$ is graded, with $\mathcal{B} = \bigoplus_{n \geq 0} \mathcal{B}_n$, then its dual $\mathcal{B}^\vee = \prod\limits_{n \geq 0} (\mathcal{B}_n)^\vee$ has a product topology[11].) Oftentimes, this causes the Kleene stars of some elements of $\mathcal{B}^\vee$ to be well-defined. As we shall soon see, characters of $\mathcal{B}$ are oftentimes found among such Kleene stars.

[9] This will happen when $M^\vee \otimes N^\vee$ has torsion (see Subsection 5.4 and Proposition 5.14 in particular).

[10] which has been briefly announced at `https://mathoverflow.net/questions/310354`

[11] In this case, $\mathbf{k}$ is usually considered as endowed with the discrete topology. See [Bourba98, Ch. II, §5.1] for an application to the combinatorics of the free Lie algebra and the free group.

5.2.1. Characters of polynomial rings

We begin with polynomial rings: noncommutative and commutative.

Example 5.3. Consider the $\mathbf{k}$-algebra $\mathbf{k}\langle x, y\rangle$ of polynomials in two noncommuting variables x, y over $\mathbf{k}$. As a $\mathbf{k}$-module, it has a basis consisting of words in the alphabet $\{x, y\}$. A character of this $\mathbf{k}$-algebra is uniquely determined by the images α and β of x and y (indeed, this follows from the universal property of $\mathbf{k}\langle x, y\rangle$). We can identify the dual $(\mathbf{k}\langle x, y\rangle)^\vee$ with the ring $\mathbf{k}\langle\langle x, y\rangle\rangle$ of noncommutative power series in x, y (by means of the bilinear form that sends two equal words to 1 and sends two distinct words to 0). Thus, the character of $\mathbf{k}\langle x, y\rangle$ that sends x and y to α and β is explicitly given as the Kleene star

$$(\alpha.x + \beta.y)^* = \sum_{n\geq 0} (\alpha.x + \beta.y)^n.$$

This characterizes all characters of $\mathbf{k}\langle x, y\rangle$. A similar characterization can be given for noncommutative polynomial rings in multiple variables.

Example 5.4. Consider the $\mathbf{k}$-algebra $\mathbf{k}[x, y]$ of polynomials in two commuting variables x, y over $\mathbf{k}$. As a $\mathbf{k}$-module, it has a basis consisting of monomials in x, y. A character of this $\mathbf{k}$-algebra is uniquely determined by the images α and β of x and y (indeed, this follows from the universal property of $\mathbf{k}[x, y]$). We can identify the dual $(\mathbf{k}[x, y])^\vee$ with the ring $\mathbf{k}[[x, y]]$ of power series in x, y (by means of the bilinear form that sends two equal monomials to 1 and sends two distinct monomials to 0). Thus, the character of $\mathbf{k}[x, y]$ that sends x and y to α and β is explicitly given as the Kleene star

$$(\alpha.x + \beta.y - \alpha\beta.xy)^* = \sum_{n\geq 0} (\alpha.x + \beta.y - \alpha\beta.xy)^n.$$

This characterizes all characters of $\mathbf{k}[x, y]$. A similar characterization can be given for polynomial rings in multiple variables.

It is worth saying that the $\mathbf{k}$-algebra Λ of symmetric functions ([GriRei20, Chapter 2]) is a polynomial ring in infinitely many variables over $\mathbf{k}$, and thus its characters can be described as in Example 5.4. These characters have multiple names: they are known as virtual alphabets, or as big Witt vectors, or as specializations.

5.2.2. Characters of monoid rings

Example 5.3 and Example 5.4 have a common generalization. In fact, both noncommutative and commutative polynomial rings are particular cases of monoid rings of trace monoids. Let us thus briefly discuss characters of monoid rings. Let $(M, \star, 1_M)$ be a monoid, and let $\mathcal{A} = \mathbf{k}[M]$ be its monoid algebra (see Example 2.6). As in Example 2.6, we define the standard pairing $\langle . \mid . \rangle : \mathbf{k}^M \otimes \mathbf{k}[M] \to \mathbf{k}$ by (1). The multiplication of $\mathbf{k}[M]$ can thus be written as

$$P \star Q := \sum_{uv=w} \langle P \mid u\rangle \langle Q \mid v\rangle \, w \tag{44}$$

(where u, v, w range over M).

If the map $\star : M \times M \to M$ has finite fibers[12] (this is condition (D) in [Bourba89, Ch. III, §2.10]), then we can extend the formula (44) to arbitrary $P, Q \in \mathbf{k}^M$ (as opposed to merely $P, Q \in \mathbf{k}[M]$). In this case, the $\mathbf{k}$-algebra $\left(\mathbf{k}^M, \star, 1_M\right)$ is called the total algebra of M, and its product is the Cauchy product between series. For every $S \in \mathbf{k}^M$, the family $(\langle S \mid m\rangle\, m)_{m\in M}$ is summable[13], and its sum is $S = \sum\limits_{m\in M} \langle S \mid m\rangle\, m$. We set $M_+ := M \setminus \{1_M\}$ and, for all series $S \in \mathbf{k}^M$, we likewise set $S_+ = S - \langle S \mid 1_M\rangle . 1_M = \sum\limits_{m\in M_+} \langle S \mid m\rangle\, m$. In order for the family $((S_+)^n)_{n\geq 0}$ to be summable, it is sufficient that the iterated multiplication map $\mu^* : (M_+)^* \to M$ defined by

$$\mu^*[m_1, \ldots, m_n] = m_1 \cdots m_n \text{ (product within } M) \tag{45}$$

have finite fibers (where we have written the word $[m_1, \ldots, m_n] \in (M_+)^*$ as a list to avoid confusion).[14]

Now, we assume that this condition (i.e., that μ^* has finite fibers) is satisfied. Then, $\sum\limits_{n\geq 0} (S_+)^n = (1 - S_+)^{-1}$ is the Kleene star $(S_+)^*$ of S_+ (see Definition 5.2).

Define the series $\underline{M} = \sum\limits_{m\in M} m \in \mathbf{k}^M$; this is called the characteristic series of the monoid M. This series $\underline{M}$ is invertible[15], and its inverse is[16]

$$\begin{aligned} \underline{M}^{-1} &= (-\underline{M}_+)^* = \sum_{n\geq 0} (-\underline{M}_+)^n = 1 - M_+ + (M_+)^2 \pm \cdots \\ &= \sum_{m\in M} \mu(m)\, m, \end{aligned} \tag{46}$$

where $\mu(m)$ is defined to be the m-th coordinate of $\underline{M}^{-1}$. This defines a function $\mu : M \to \mathbf{k}$, which is called the Möbius function of M. Note that it is easy to see that $\mu(1_M) = 1_{\mathbf{k}}$, and thus the equality (46) is equivalent to

$$\underline{M} = \Big(- \sum_{m\in M_+} \mu(m)\, m \Big)^*. \tag{47}$$

[12] Recall that a map $f : X \to Y$ between two sets X and Y has finite fibers if and only if for each $y \in Y$, the preimage $f^{-1}(y)$ is finite.

[13] We say that a family $(a_s)_{s\in S}$ of elements of $\mathbf{k}^M$ is summable if for any given $n \in M$, all but finitely many $s \in S$ satisfy $\langle a_s \mid n\rangle = 0$. Such a summable family will always have a well-defined infinite sum $\sum\limits_{s\in S} a_s \in \mathbf{k}^M$, whence the name "summable".

[14] Furthermore, this condition is also necessary (if S_+ is generic) if $\mathbf{k} = \mathbb{Z}$. These monoids are called "locally finite" in [1].

[15] Here we are using the condition that μ^* has finite fibers, these monoids are called locally finite in [1].

[16] Here we are using the fact that $\underline{M}_+ = \underline{M} - 1$, so that $1 + \underline{M}_+ = \underline{M}$.

Every character χ of the $\mathbf{k}$-algebra $(\mathbf{k}[M], \star, 1_M)$ can now be written in the form[17]

$$\chi = \sum_{m \in M} \chi(m)\, m = \big(- \sum_{m \in M_+} \chi(m)\mu(m)\, m \big)^*. \tag{48}$$

(This follows immediately from (47) by applying the continuous $\mathbf{k}$-algebra homomorphism $\mathbf{k}^M \to \mathbf{k}^M$ that sends each $m \in M$ to $\chi(m)m$. The word "continuous" here refers to the product topology on $\mathbf{k}^M$.)

Example 5.5. The celebrated arithmetic Möbius function $\mu : \mathbb{N}_+ \to \mathbb{Z}$ is the Möbius function of the multiplicative monoid $(\mathbb{N}_+, \cdot, 1)$. It is a particular case of the Möbius function of a trace monoid, i.e., of a monoid defined by commutation relations. In a nutshell, a trace monoid is determined by a reflexive undirected graph ϑ with vertex set X (called the alphabet). The monoid is generated by all vertices $x \in X$, subject to the relations $xy = yx$ for all edges $\{x, y\}$ of ϑ. This monoid is called $M(X, \vartheta)$ (see [DuKr93]). It always satisfies the condition that μ^* has finite fibers. Its Möbius function is given by

$$\sum_{m \in M} \mu(m)\, m = \sum_{\substack{C \subseteq X; \\ C \text{ is a clique of } \vartheta}} (-1)^{|C|} \prod_{x \in C} x \tag{49}$$

(see [CaFo69, Théorème 2.4]).

In particular, if $X = \{x_1, x_2, \ldots, x_n\}$ and ϑ is the complete graph ϑ_{full} (so that $xy = yx$ for all $x, y \in X$), the monoid $M(X, \vartheta_{full})$ is the free abelian monoid $\{X^\alpha\}_{\alpha \in \mathbb{N}^{(X)}}$, and then we have $\mu(X^\alpha) = 0$ if the monomial X^α contains a square and $\mu(X^\alpha) = (-1)^{|\alpha|}$ if X^α is square-free[18]. In this case, (48) becomes

$$\chi = \Big(1 - (1 - \chi(x_1)x_1)(1 - \chi(x_2)x_2) \cdots (1 - \chi(x_n)x_n)\Big)^*. \tag{50}$$

For example, every character of $\mathbf{k}[x, y]$ is of the form

$$\chi = \Big(1 - (1 - \chi(x)x)(1 - \chi(y)y)\Big)^* = \Big(\chi(x)x + \chi(y)y - \chi(x)\chi(y)xy\Big)^*.$$

This recovers the $(\alpha.x + \beta.y - \alpha\beta.xy)^*$ formula from Example 5.4.

On the other end, with no commutations ($\vartheta = \{(x, x)\}_{x \in X}$), we have $M(X, \vartheta) = X^*$, and the monoid $M(X, \vartheta)$ is the free monoid on X; now, the Möbius function is supported on $X \cup \{1_{X^*}\}$ with $\mu(1) = 1$ and $\mu(x) = -1$ for all $x \in X$. Thus, every character on $\mathbf{k}\langle X \rangle$ is of the form

$$\chi = \Big(\sum_{x \in X} \chi(x)\, x \Big)^* \tag{51}$$

(Kleene star of the plane property, see [DuMiNg19]). For $n = 2$, this recovers the $(\alpha.x + \beta.y)^*$ formula from Example 5.3.

[17] We regard χ as an element of $\mathbf{k}^M$, since the standard pairing $\langle . \mid . \rangle$ allows us to identify the dual of $\mathbf{k}[M]$ with $\mathbf{k}^M$.

[18] When X is the set of all prime numbers, one recovers the classical Möbius function.

5.3. Characters on bialgebras

We begin with a simple fact:

Proposition 5.6. *Let $\mathcal{B}$ be a $\mathbf{k}$-bialgebra. Then, the set $\Xi(\mathcal{B})$ of characters of $\mathcal{B}$ is a monoid for the convolution product $\circledast$.*

Proof. We know that $\mathcal{B}^\vee$ is a $\mathbf{k}$-algebra under convolution, and thus a monoid. Hence, we just need to prove that $\Xi(\mathcal{B})$ is a submonoid of this monoid $\mathcal{B}^\vee$. But this follows from the following two observations:

- If $p, q \in \Xi(\mathcal{B})$, then $p \circledast q \in \Xi(\mathcal{B})$. (This is a consequence of Lemma 4.10, applied to $C = \mathcal{B}$ and $A = \mathbf{k}$.)
- The neutral element $\underbrace{\eta_{\mathbf{k}}}_{=\mathrm{id}} \epsilon_{\mathcal{B}} = \epsilon_{\mathcal{B}}$ of $\circledast$ belongs to $\Xi(\mathcal{B})$.

Thus, Proposition 5.6 is proved. □

The convolution monoid $\Xi(\mathcal{B})$ is not always a group.

Example 5.7. Fix $q \in \mathbf{k}$. Let $\mathcal{B}$ be the univariate q-infiltration bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ from Example 2.3. It is easy to see (by induction on m) that

$$\Delta_{\uparrow_q}(x^m) = \sum_{\substack{(i,j,k)\in\mathbb{N}^3; \\ i+j+k=m}} \binom{m}{i,j,k} q^j x^{i+j} \otimes x^{j+k} \tag{52}$$

holds in $\mathcal{B}$ for every $m \in \mathbb{N}$, where $\binom{m}{i,j,k}$ denotes the multinomial coefficient $\dfrac{m!}{i!j!k!}$. (This is actually a particular case of a beautiful formula that holds for any multivariate q-infiltration algebra[19].)

As a $\mathbf{k}$-module, the dual $\mathcal{B}^\vee$ of $\mathcal{B}$ can be identified with the $\mathbf{k}$-module $\mathbf{k}[[x]]$ of formal power series in x over $\mathbf{k}$ (by equating $x^j \in \mathbf{k}[[x]]$ with the $\mathbf{k}$-linear form on $\mathcal{B}$ that sends $x^j \in \mathcal{B}$ to 1 and sends any other power of x in $\mathcal{B}$ to 0). We denote the convolution product $\circledast$ on the dual algebra $\mathcal{B}^\vee$ by $\uparrow_q$. Thus, $\uparrow_q$ is a binary operation on $\mathcal{B}^\vee = \mathbf{k}[[x]]$.

The monoid of characters of $\mathcal{B}$ is $\Xi(\mathcal{B}) = \{(\alpha x)^*\}_{\alpha\in\mathbf{k}}$, where we are using the Kleene star notation $s^* = \dfrac{1}{1-s} = 1 + s + s^2 + \cdots$ (the multiplication being that of

[19] Namely,

$$\Delta_{\uparrow_q}(w) = \sum_{I\cup J=\{1,2,\ldots,m\}} q^{|I\cap J|} w[I] \otimes w[J] \tag{53}$$

for any word w of length m. See "Shuffles, stuffles and other dual laws" in `https://mathoverflow.net/questions/214927/` for details.

$\mathbf{k}[[x]]$). For any $\alpha, \beta \in \mathbf{k}$, we have

$$\begin{aligned}
(\alpha x)^* \uparrow_q (\beta x)^* &= \sum_{m\geq 0} \langle (\alpha x)^* \uparrow_q (\beta x)^* \mid x^m \rangle \, x^m \\
&= \sum_{m\geq 0} \langle (\alpha x)^* \otimes (\beta x)^* \mid \Delta_{\uparrow_q}(x^m) \rangle \, x^m \\
&= \sum_{m\geq 0} \sum_{\substack{(i,j,k)\in\mathbb{N}^3; \\ i+j+k=m}} \binom{m}{i,j,k} q^j \langle (\alpha x)^* \otimes (\beta x)^* \mid x^{i+j} \otimes x^{j+k} \rangle x^m \\
&\qquad \text{(by (52))} \\
&= \sum_{m\geq 0} x^m \sum_{\substack{(i,j,k)\in\mathbb{N}^3; \\ i+j+k=m}} \binom{m}{i,j,k} q^j \alpha^{i+j} \beta^{j+k} = \sum_{m\geq 0} x^m (q\alpha\beta + \alpha + \beta)^m \\
&= \big((q\alpha\beta + \alpha + \beta)x\big)^*.
\end{aligned}$$

In particular, when $q = 0$, we recover the law of composition of characters for the shuffle product:

$$(\alpha x)^* \sqcup\!\sqcup (\beta x)^* = \big((\alpha + \beta)x\big)^*;$$

thus, the monoid of characters $\Xi(\mathcal{B})$ is (in this case) isomorphic with the additive group $(\mathbf{k}, +, 0)$.
When $q \in \mathbf{k}^\times$, the monoid of characters $\Xi(\mathcal{B})$ is isomorphic with the multiplicative monoid $(\mathbf{k}, \cdot, 1)$ through $(\alpha x)^* \mapsto q\alpha + 1$; in particular, it has a zero element $(\alpha x)^*$ with $\alpha = -\dfrac{1}{q}$.

Theorem 5.8. *Let $\mathcal{B}$ be a $\mathbf{k}$-bialgebra. As usual, let $\Delta = \Delta_{\mathcal{B}}$ and $\epsilon = \epsilon_{\mathcal{B}}$ be its comultiplication and its counit.*

Let $\mathcal{B}_+ = \ker(\epsilon)$. For each $N \geq 0$, let $\mathcal{B}_+^N = \underbrace{\mathcal{B}_+ \cdot \mathcal{B}_+ \cdot \cdots \cdot \mathcal{B}_+}_{N \text{ times}}$, where $\mathcal{B}_+^0 = \mathcal{B}$. Note that $\left(\mathcal{B}_+^0, \mathcal{B}_+^1, \mathcal{B}_+^2, \ldots\right)$ is called the standard decreasing filtration of $\mathcal{B}$.

For each $N \geq -1$, we define a $\mathbf{k}$-submodule $\mathcal{B}_N^\vee$ of $\mathcal{B}^\vee$ by

$$\mathcal{B}_N^\vee = (\mathcal{B}_+^{N+1})^\perp = \left\{ f \in \mathcal{B}^\vee \mid f\left(\mathcal{B}_+^{N+1}\right) = 0 \right\}. \tag{54}$$

Thus, $\left(\mathcal{B}_{-1}^\vee, \mathcal{B}_0^\vee, \mathcal{B}_1^\vee, \ldots\right)$ is an increasing filtration of $\mathcal{B}_\infty^\vee := \bigcup\limits_{N\geq -1} \mathcal{B}_N^\vee$ with $\mathcal{B}_{-1}^\vee = 0$. Then:

- ***(a)*** *We have $\mathcal{B}_p^\vee \circledast \mathcal{B}_q^\vee \subseteq \mathcal{B}_{p+q}^\vee$ for any $p, q \geq -1$ (where we set $\mathcal{B}_{-2}^\vee = 0$). Hence, $\mathcal{B}_\infty^\vee$ is a subalgebra of the convolution algebra $\mathcal{B}^\vee$.*
- ***(b)*** *Assume that $\mathbf{k}$ is an integral domain. Then, the set $\Xi(\mathcal{B})^\times$ of invertible characters (i.e., of invertible elements of the monoid $\Xi(\mathcal{B})$ from Proposition 5.6) is left $\mathcal{B}_\infty^\vee$-linearly independent.*

Proof of Theorem 5.8. The map $\epsilon : \mathcal{B} \to \mathbf{k}$ is a $\mathbf{k}$-algebra homomorphism; hence, its kernel $\mathcal{B}_+$ is an ideal of $\mathcal{B}$. Thus, $\mathcal{B}_+ = \mathcal{B}\mathcal{B}_+$, so that

$$\mathcal{B}_+^N = \mathcal{B}_+^{N-1}\mathcal{B}_+ \qquad \text{for each } N \geq 1. \tag{55}$$

Let us define a left action $\triangleright$ of the $\mathbf{k}$-algebra $\mathcal{B}$ on $\mathcal{B}^\vee$ by setting

$$\langle u \triangleright f \mid v \rangle = \langle f \mid vu \rangle \qquad \text{for all } f \in \mathcal{B}^\vee \text{ and } u, v \in \mathcal{B}.$$

Here, $\langle g \mid b \rangle$ means $g(b)$ whenever $g \in \mathcal{B}^\vee$ and $b \in \mathcal{B}$. Thus, $\mathcal{B}^\vee$ is a left $\mathcal{B}$-module. For a given $u \in \mathcal{B}$, we shall refer to the operator $\mathcal{B}^\vee \to \mathcal{B}^\vee$, $f \mapsto u \triangleright f$ as shifting by u or the u-left shift operator; it generalizes Schützenberger's right u^{-1} in automata theory [BeRe88, Schütz61].

In the following, we shall use a variant of Sweedler notation: Given an $u \in B$, instead of writing $\sum\limits_{(u)} u_1 \otimes u_2$ for $\Delta(u)$, we will write $\sum\limits_{(u)} u^{(1)} \otimes u^{(2)}$ for $\Delta(u) - u \otimes 1 - 1 \otimes u$. Thus,

$$\Delta(u) = u \otimes 1 + 1 \otimes u + \sum_{(u)} u^{(1)} \otimes u^{(2)} \tag{56}$$

for each $u \in \mathcal{B}$. Moreover, if $u \in \mathcal{B}_+$, then all of the $u^{(1)}$ and $u^{(2)}$ can be chosen to belong to $\mathcal{B}_+$ themselves (because it is easy to check that $\Delta(u) - u \otimes 1 - 1 \otimes u = ((\mathrm{id} - \eta\epsilon) \otimes (\mathrm{id} - \eta\epsilon))(\Delta(u)) \in ((\mathrm{id} - \eta\epsilon) \otimes (\mathrm{id} - \eta\epsilon))(\mathcal{B} \otimes \mathcal{B}) = \mathcal{B}_+ \otimes \mathcal{B}_+$, since $(\mathrm{id} - \eta\epsilon)(\mathcal{B}) = \mathcal{B}_+$). We shall understand, in the following, that we choose $u^{(1)}$ and $u^{(2)}$ from $\mathcal{B}_+$ when $u \in \mathcal{B}_+$.

The following two lemmas give simple properties of the left action $\triangleright$:

Lemma 5.9. *Let $f_1, f_2 \in \mathcal{B}^\vee$ and $u \in \mathcal{B}_+ = \ker(\epsilon)$. Then,*

$$u \triangleright (f_1 \circledast f_2) = (u \triangleright f_1) \circledast f_2 + f_1 \circledast (u \triangleright f_2) + \sum_{(u)} (u^{(1)} \triangleright f_1) \circledast (u^{(2)} \triangleright f_2). \tag{57}$$

Proof. Immediate by direct computation. □

Lemma 5.10. *Let $k \geq 0$, and let $f \in \mathcal{B}_k^\vee$ and $u \in \mathcal{B}_+$. Then, $u \triangleright f \in \mathcal{B}_{k-1}^\vee$.*

Proof. Easy using (55). □

Let us now proceed with the proof of Theorem 5.8.

(a) We shall first show that $\mathcal{B}_p^\vee \circledast \mathcal{B}_q^\vee \subseteq \mathcal{B}_{p+q}^\vee$ for any $p, q \geq -1$.

Indeed, we proceed by strong induction on $p+q$. Let $f_1 \in \mathcal{B}_p^\vee$ and $f_2 \in \mathcal{B}_q^\vee$. We intend to show that $f_1 \circledast f_2 \in \mathcal{B}_{p+q}^\vee$. This is trivial if p or q is -1, since $\mathcal{B}_{-1}^\vee = 0$. Thus, we WLOG assume $p, q \geq 0$.

Hence, $\mathcal{B}_+^{p+q+1} = \mathcal{B}_+^{p+q}\mathcal{B}_+$ by (55). Thus, the $\mathbf{k}$-module $\mathcal{B}_+^{p+q+1}$ is spanned by the products uv for $u \in \mathcal{B}_+^{p+q}$ and $v \in \mathcal{B}_+$. Thus, in order to prove that $f_1 \circledast f_2 \in \mathcal{B}_{p+q}^\vee$, it suffices to show that $f_1 \circledast f_2$ is orthogonal to all these products.

So let $u \in \mathcal{B}_+^{p+q}$ and $v \in \mathcal{B}_+$. Then, we must prove that $\langle f_1 \circledast f_2 \mid uv \rangle = 0$. But we have

$$\langle f_1 \circledast f_2 \mid uv \rangle = \langle v \triangleright (f_1 \circledast f_2) \mid u \rangle. \tag{58}$$

Applying (57) to v instead of u, we get

$$v \triangleright (f_1 \circledast f_2) = (v \triangleright f_1) \circledast f_2 + f_1 \circledast (v \triangleright f_2) + \sum_{(v)} (v^{(1)} \triangleright f_1) \circledast (v^{(2)} \triangleright f_2) \tag{59}$$

with all $v^{(1)}$ and $v^{(2)}$ lying in $\mathcal{B}_+$. Thus, Lemma 5.10 yields $v \triangleright f_1 \in \mathcal{B}_{p-1}^\vee$ and $v \triangleright f_2 \in \mathcal{B}_{q-1}^\vee$ and $v^{(1)} \triangleright f_1 \in \mathcal{B}_{p-1}^\vee$ and $v^{(2)} \triangleright f_2 \in \mathcal{B}_{q-1}^\vee$. Thus, (59) becomes

$$\begin{aligned} v \triangleright (f_1 \circledast f_2) &= \underbrace{(v \triangleright f_1)}_{\in \mathcal{B}_{p-1}^\vee} \circledast \underbrace{f_2}_{\in \mathcal{B}_q^\vee} + \underbrace{f_1}_{\in \mathcal{B}_p^\vee} \circledast \underbrace{(v \triangleright f_2)}_{\in \mathcal{B}_{q-1}^\vee} + \sum_{(v)} \underbrace{(v^{(1)} \triangleright f_1)}_{\in \mathcal{B}_{p-1}^\vee} \circledast \underbrace{(v^{(2)} \triangleright f_2)}_{\in \mathcal{B}_{q-1}^\vee} \\ &\in \mathcal{B}_{p-1}^\vee \circledast \mathcal{B}_q^\vee + \mathcal{B}_p^\vee \circledast \mathcal{B}_{q-1}^\vee + \mathcal{B}_{p-1}^\vee \circledast \mathcal{B}_{q-1}^\vee \subseteq \mathcal{B}_{p+q-1}^\vee \end{aligned}$$

(by the induction hypothesis, applied three times). This entails $\langle v \triangleright (f_1 \circledast f_2) \mid u \rangle = 0$ by the definition of $\mathcal{B}_{p+q-1}^\vee$. Thus, (58) yields $\langle f_1 \circledast f_2 \mid uv \rangle = 0$. Thus, we have proved that $f_1 \circledast f_2 \in \mathcal{B}_{p+q}^\vee$. This completes the proof of $\mathcal{B}_p^\vee \circledast \mathcal{B}_q^\vee \subseteq \mathcal{B}_{p+q}^\vee$.

The fact that $\mathcal{B}_\infty^\vee$ is a subalgebra of the convolution algebra $\mathcal{B}^\vee$ follows from the preceding, since we also know that $\epsilon \in \mathcal{B}_0^\vee \subseteq \mathcal{B}_\infty^\vee$.

(b) We define the degree of an element $b \in \mathcal{B}_\infty^\vee$ to be the least index $d \geq -1$ such that $b \in \mathcal{B}_d^\vee$. We denote this index by $\deg(b)$. (Note that $\deg(0) = -1$.)

Recall that for $b \in \mathcal{B}_d^\vee$ and $u \in \mathcal{B}_+$, we have $u \triangleright b \in \mathcal{B}_{d-1}^\vee$ (by Lemma 5.10). Thus, for $b \in \mathcal{B}_\infty^\vee$ and $u \in \mathcal{B}_+$, we have $u \triangleright b \in \mathcal{B}_\infty^\vee$. In other words, $\mathcal{B}_+ \triangleright \mathcal{B}_\infty^\vee \subseteq \mathcal{B}_\infty^\vee$.

Let us consider non-trivial relations of the form

$$\sum_{g \in F} p_g \circledast g = 0 \tag{60}$$

with a finite subset F of $\Xi(\mathcal{B})^\times$ and with nonzero coefficients $p_g \in \mathcal{B}_\infty^\vee$. If there are no such relations with $F \neq \emptyset$, then we are done. Otherwise, we pick one such relation of type (60) with $|F| \neq 0$ minimal; among all such minimum-size relations, we pick one in which $\sum_{g \in F} \deg(p_g)$ is minimal. WLOG, we assume that $\epsilon \in F$ (otherwise, pick $g_0 \in F$ and multiply both sides of the equation (60) by $g_0^{\circledast -1}$).

It is impossible that $F = \{\epsilon\}$ (as $p_\epsilon \neq 0$); thus, we can choose $g_1 \in F \setminus \{\epsilon\}$. Having chosen this g_1, we observe that $g_1(\mathcal{B}_+) \neq 0$ (since $g_1(\mathcal{B}_+) = 0$ would imply $g_1 = \epsilon$ because of $g_1 \in \Xi(\mathcal{B})$); in other words, there exists some $u \in \mathcal{B}_+$ such that $\langle g_1 \mid u \rangle \neq 0$. Choose such a u.

It is easy to see (from the definition) that each character $g \in \Xi(\mathcal{B})$ and each $v \in \mathcal{B}_+$ satisfy

$$v \triangleright g = \langle g \mid v \rangle \, g. \tag{61}$$

Our plan is now to shift both sides of (60) by u, and rewrite the resulting equality again as an equality of the form (60) (with new values of p_g). To do so, we introduce a few notations.

Write $\Delta(u)$ as in (56), with $u^{(1)}, u^{(2)} \in \mathcal{B}_+$. For each $g \in F$, let us set

$$p'_g := u \triangleright p_g + \langle g \mid u \rangle p_g + \sum_{(u)} \langle g \mid u^{(2)} \rangle (u^{(1)} \triangleright p_g) \in \mathcal{B}^\vee.$$

Then, we have

$$u \triangleright (p_g \circledast g) = p'_g \circledast g \tag{62}$$

for each $g \in F$, because Lemma 5.9 yields

$$\begin{aligned}
&u \triangleright (p_g \circledast g) \\
&= (u \triangleright p_g) \circledast g + p_g \circledast (u \triangleright g) + \sum_{(u)} (u^{(1)} \triangleright p_g) \circledast (u^{(2)} \triangleright g) \\
&= (u \triangleright p_g) \circledast g + p_g \circledast (\langle g \mid u \rangle g) + \sum_{(u)} (u^{(1)} \triangleright p_g) \circledast \left(\langle g \mid u^{(2)} \rangle g \right) \qquad \text{(by (61))} \\
&= \underbrace{\left(u \triangleright p_g + \langle g \mid u \rangle p_g + \sum_{(u)} \langle g \mid u^{(2)} \rangle (u^{(1)} \triangleright p_g) \right)}_{= p'_g} \circledast g \\
&= p'_g \circledast g.
\end{aligned}$$

Thus, if we shift both sides of (60) by u, we find

$$u \triangleright \left(\sum_{g \in F} p_g \circledast g \right) = 0.$$

Hence,

$$0 = u \triangleright \left(\sum_{g \in F} p_g \circledast g \right) = \sum_{g \in F} u \triangleright (p_g \circledast g) = \sum_{g \in F} p'_g \circledast g \tag{63}$$

(by (62)).

For each $g \in F$, we have $p'_g \in \mathcal{B}_\infty^\vee$ (by the definition of p'_g, since $p_g \in \mathcal{B}_\infty^\vee$ and $\mathcal{B}_+ \triangleright \mathcal{B}_\infty^\vee \subseteq \mathcal{B}_\infty^\vee$).

It is easy to see that each $g \in F$ satisfies

$$\deg\left(p'_g\right) \leq \deg\left(p_g\right). \tag{64}$$

(Indeed, Lemma 5.10 shows that any nonzero $f \in \mathcal{B}_\infty^\vee$ satisfies $\deg(u \triangleright f) < \deg f$; for the same reason, $\deg\left(u^{(2)} \triangleright f\right) < \deg f$. Thus, the definition of p'_g represents

p'_g as a $\mathbf{k}$-linear combination of elements of $\mathcal{B}^\vee_\infty$ having the same degree as p_g or smaller degree. This proves (64).)

But the definition of p'_ϵ easily yields

$$p'_\epsilon = u \triangleright p_\epsilon \tag{65}$$

(since $u, u^{(2)} \in \mathcal{B}_+$ entail $u \triangleright p_\epsilon = 0$ and $u^{(2)} \triangleright p_\epsilon = 0$). Therefore, $\deg(p'_\epsilon) = \deg(u \triangleright p_\epsilon) < \deg(p_\epsilon)$ (since Lemma 5.10 shows that any nonzero $f \in \mathcal{B}^\vee_\infty$ satisfies $\deg(u \triangleright f) < \deg f$).

Now, recall the equality (63). This equality (once rewritten as $\sum_{g \in F} p'_g \circledast g = 0$) has the same structure as (60) (since $p'_g \in \mathcal{B}^\vee_\infty$ for each $g \in F$), and uses the same set F, but it satisfies $\sum_{g \in F} \deg\left(p'_g\right) < \sum_{g \in F} \deg\left(p_g\right)$ (because each $g \in F$ satisfies (64), but the specific character $g = \epsilon$ satisfies $\deg(p'_\epsilon) < \deg(p_\epsilon)$). Thus, if the coefficients p'_g in (63) are not all 0, then we obtain a contradiction to our choice of relation (which was to minimize $\sum_{g \in F} \deg\left(p_g\right)$). Hence, all coefficients p'_g must be 0. In particular, we must have $p'_{g_1} = 0$. Therefore,

$$0 = p'_{g_1} = u \triangleright p_{g_1} + \langle g_1 \mid u \rangle p_{g_1} + \sum_{(u)} \langle g_1 \mid u^{(2)} \rangle (u^{(1)} \triangleright p_{g_1})$$

(by the definition of p'_{g_1}), so that

$$\langle g_1 \mid u \rangle p_{g_1} = -u \triangleright p_{g_1} - \sum_{(u)} \langle g_1 \mid u^{(2)} \rangle (u^{(1)} \triangleright p_{g_1}) \in \mathcal{B}^\vee_{\deg\left(p_{g_1}\right)-1}$$

(by Lemma 5.10, since $u, u^{(2)} \in \mathcal{B}_+$ and $p_{g_1} \in \mathcal{B}^\vee_{\deg\left(p_{g_1}\right)}$). In other words, $\langle g_1 \mid u \rangle p_{g_1}$ is orthogonal to $\mathcal{B}_+^{\deg\left(p_{g_1}\right)}$. Since[20] $\langle g_1 \mid u \rangle \neq 0$, this entails that p_{g_1} is orthogonal to $\mathcal{B}_+^{\deg\left(p_{g_1}\right)}$ as well (since its target $\mathbf{k}$ is an integral domain). This means that $p_{g_1} \in \mathcal{B}^\vee_{\deg\left(p_{g_1}\right)-1}$, or, equivalently, $\deg\left(p_{g_1}\right) \leq \deg\left(p_{g_1}\right) - 1$. But this is absurd. This is the contradiction we were looking for. Thus, Theorem 5.8 **(b)** is proved. □

Remark 5.11. i) The invertible characters in $\Xi(\mathcal{B})^\times$ are also right $\mathcal{B}^\vee_\infty$-linearly independent. This can be proven similarly, using right shifts in the proof.

ii) The reader should beware of supposing that the standard decreasing filtration is necessarily Hausdorff[21] (i.e., satisfies $\bigcap_{n \geq 0} \mathcal{B}_+^n = \{0\}$). A counterexample can be obtained by taking the universal enveloping bialgebra of any simple Lie algebra (or, more generally, of any perfect Lie algebra); it will satisfy $\bigcap_{n \geq 0} \mathcal{B}_+^n = \mathcal{B}_+$.

[20] We recall that we have chosen $u \in \mathcal{B}_+$ such that $\langle g_1 \mid u \rangle \neq 0$.

[21] "Separated" in [Bourba72].

iii) The property (i.e., the linear independence) does not hold if we consider the set of all characters (that is, $\Xi(\mathcal{B})$) instead of $\Xi(\mathcal{B})^{\times}$. For example, let $\mathcal{B}$ be the univariate q-infiltration bialgebra $\left(\mathbf{k}[x], \Delta_{\uparrow_q}, \epsilon\right)$ from Example 2.3, and assume that $q \in \mathbf{k}$ is invertible. Define two $\mathbf{k}$-linear maps $f : \mathcal{B} \to \mathbf{k}$ and $g : \mathcal{B} \to \mathbf{k}$ by

$$f(x^n) = \delta_{n,1} \qquad \text{and} \qquad g(x^n) = \left(-\frac{1}{q}\right)^n \qquad \text{for all } n \in \mathbb{N}$$

(where the $\delta_{n,1}$ is a Kronecker delta). Note that g is a character of $\mathcal{B}$, while $f \in \mathcal{B}_1^{\vee} \subseteq \mathcal{B}_{\infty}^{\vee}$.

We claim that $f \circledast g = 0$. In fact, using (52), it is straightforward to see that $(f \circledast g)(x^m) = 0$ for each $m \in \mathbb{N}$; thus, $f \circledast g = 0$. Since f is nonzero, this shows that the set $\Xi(\mathcal{B})$ is not left $\mathcal{B}_{\infty}^{\vee}$-linearly independent.

Note that our above proof of Theorem 5.8 is somewhat similar to the standard (Artin) proof of the linear independence of characters in Galois theory ([Artin71, proof of Theorem 12]). Shifting by u in the former proof corresponds to replacing x by αx in the latter.

Corollary 5.12. *We suppose that $\mathcal{B}$ is cocommutative, and $\mathbf{k}$ is an integral domain. Let $(g_x)_{x \in X}$ be a family of elements of $\Xi(\mathcal{B})^{\times}$ (the set of invertible characters of $\mathcal{B}$), and let $\varphi_X : \mathbf{k}[X] \to (\mathcal{B}^{\vee}, \circledast, \epsilon)$ be the $\mathbf{k}$-algebra morphism that sends each $x \in X$ to g_x. In order for the family $(g_x)_{x \in X}$ (of elements of the commutative ring $(\mathcal{B}^{\vee}, \circledast, \epsilon)$) to be algebraically independent over the subring $(\mathcal{B}_{\infty}^{\vee}, \circledast, \epsilon)$, it is necessary and sufficient that the monomial map*

$$\begin{aligned} m : \mathbb{N}^{(X)} &\to (\mathcal{B}^{\vee}, \circledast, \epsilon), \\ \alpha &\mapsto \varphi_X(X^{\alpha}) = \prod_{x \in X} g_x^{\alpha_x} \end{aligned} \tag{66}$$

(where α_x means the x-th entry of α) be injective.

Proof. Indeed, as $\mathcal{B}$ is cocommutative (and $\mathbf{k}$ commutative), $(\mathcal{B}^{\vee}, \circledast, \epsilon)$ is a commutative algebra (see, e.g., [GriRei20, Exercise 1.5.5] or [Bourba89, Chapter III, §11.2, Proposition 2]). Thus, the algebraic independence of the family $(g_x)_{x \in X}$ is equivalent to the statement that the family $\left(\prod_{x \in X} g_x^{\alpha_x}\right)_{\alpha \in \mathbb{N}^{(X)}}$ be $\mathcal{B}_{\infty}^{\vee}$-linearly independent. In other words, it is equivalent to the claim that the family $(m(\alpha))_{\alpha \in \mathbb{N}^{(X)}}$ (with m as in (66)) be $\mathcal{B}_{\infty}^{\vee}$-linearly independent (since $m(\alpha) = \prod_{x \in X} g_x^{\alpha_x}$ for each $\alpha \in \mathbb{N}^{(X)}$). It suffices to remark that the elements $m(\alpha)$ are invertible characters (since they are products of invertible characters). Therefore, in view of Theorem 5.8 **(b)**, the $(m(\alpha))_{\alpha \in \mathbb{N}^{(X)}}$ are $\mathcal{B}_{\infty}^{\vee}$-linearly independent if they are distinct; but this amounts to saying that m is injective. $\square$

Example 5.13. i) Let $\mathbf{k}$ be an integral domain, and let us consider the bialgebra $\mathcal{B} = (\mathbf{k}[x], \Delta, \epsilon)$ from Example 2.2 (the standard univariate polynomial bialgebra). As it is a particular case of the situation of the free algebra[22], we will let $\sqcup\!\sqcup$ denote the convolution $\circledast$ on its dual $\mathbf{k}$-module $\mathcal{B}^\vee = \mathbf{k}[x]^\vee \cong \mathbf{k}[[x]]$; thus, $(\mathbf{k}[[x]], \sqcup\!\sqcup, 1)$ becomes a commutative $\mathbf{k}$-algebra.

For every $\alpha \in \mathbf{k}$, there exists only one character of $\mathbf{k}[x]$ sending x to α; we will denote this character by $(\alpha.x)^* \in \mathbf{k}[[x]]$ (see [1, DuMiNg19, DucTol09, DGM2-20] for motivations about this notation). Thus, $\Xi(\mathcal{B}) = \{(\alpha.x)^* \mid \alpha \in \mathbf{k}\}$. It is easy to check that $(\alpha.x)^* \sqcup\!\sqcup (\beta.x)^* = \big((\alpha+\beta).x\big)^*$ for any $\alpha, \beta \in \mathbf{k}$. Thus, any $c_1, c_2, \ldots, c_k \in \mathbf{k}$ and any $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ satisfy

$$\begin{aligned} &\big((c_1.x)^*\big)^{\sqcup\!\sqcup\,\alpha_1} \sqcup\!\sqcup \big((c_2.x)^*\big)^{\sqcup\!\sqcup\,\alpha_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup \big((c_k.x)^*\big)^{\sqcup\!\sqcup\,\alpha_k} \\ &= \big((\alpha_1 c_1 + \alpha_2 c_2 + \cdots + \alpha_k c_k).x\big)^* . \end{aligned} \tag{67}$$

The monoid $\Xi(\mathcal{B})$ is thus isomorphic to the abelian group $(\mathbf{k}, +, 0)$; in particular, it is a group, so that $\Xi(\mathcal{B})^\times = \Xi(\mathcal{B})$.

The decreasing filtration of $\mathcal{B}$ is given by $\mathcal{B}_+^n = \mathbf{k}[x]_{\geq n}$ (the ideal of polynomials of degree $\geq n$). Hence, the reader may check easily that $\mathcal{B}_n^\vee = \mathbf{k}[x]_{\leq n}$ (the module of polynomials of degree $\leq n$), whence $\mathcal{B}_\infty^\vee = \mathbf{k}[x]$.

Now, let $((c_i.x)^*)_{i\in I}$ be a family of elements of $\Xi(\mathcal{B})^\times$. Taking $X = I$ and $g_i = c_i.x$ for each $i \in I$, we can then apply Corollary 5.12, and we conclude that the family $((c_i.x)^*)_{i\in I}$ of elements of the power series ring $\mathbf{k}[[x]]$ is algebraically independent over the subring $(\mathcal{B}_\infty^\vee, \circledast, \epsilon) = \mathbf{k}[x]$ if and only if the monomial map (66) is injective.

But (67) shows that the monomial map (66) is injective if and only if the family $(c_i)_{i\in I}$ is $\mathbb{Z}$-linearly independent in $\mathbf{k}$.

To illustrate this, take $\mathbf{k} = \overline{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) and $c_n = \sqrt{p_n} \in \mathbb{N}$, where p_n is the n-th prime number. What precedes shows that the family of series $\big((\sqrt{p_n}x)^*\big)_{n\geq 1}$ is algebraically independent over the polynomials (i.e., over $\overline{\mathbb{Q}}[x]$) within the commutative $\overline{\mathbb{Q}}$-algebra $\big(\overline{\mathbb{Q}}[[x]], \sqcup\!\sqcup, 1\big)$. This example can be double-checked using partial fractions decompositions as, in fact, $(\sqrt{p_n}x)^* = \dfrac{1}{1-\sqrt{p_n}x}$ (this time, the inverse is taken within the ordinary product in $\mathbf{k}[[x]]$) and

$$\Big(\frac{1}{1-\sqrt{p_n}x}\Big)^{\sqcup\!\sqcup\, n} = \frac{1}{1-n\sqrt{p_n}x}.$$

ii) The preceding example can be generalized as follows: Let $\mathbf{k}$ still be an integral domain; let V be a $\mathbf{k}$-module, and let $\mathcal{B} = \Big(T(V), \mathrm{conc}, 1_{T(V)}, \Delta_{\boxtimes}, \epsilon\Big)$ be the

[22] See [GriRei20, Proposition 1.6.7] and [Reuten93, Section 1.4].

standard tensor conc-bialgebra[23] For every linear form $\varphi \in V^\vee$, there is an unique character φ^* of $\left(T(V), \mathrm{conc}, 1_{T(V)}\right)$ such that all $u \in V$ satisfy

$$\langle \varphi^* \mid u \rangle = \langle \varphi \mid u \rangle. \tag{68}$$

Again, it is easy to check[24] that $(\varphi_1)^* \sqcup\!\sqcup (\varphi_2)^* = \left(\varphi_1 + \varphi_2\right)^*$ for any $\varphi_1, \varphi_2 \in V^\vee$, because, from Lemma 4.10, both sides are characters of $\left(T(V), \mathrm{conc}, 1_{T(V)}\right)$ so that the equality has only to be checked on V. Again, from this, any $\varphi_1, \varphi_2, \ldots, \varphi_k \in V^\vee$ and any $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ satisfy

$$\begin{aligned} &\left((\varphi_1)^*\right)^{\sqcup\!\sqcup \alpha_1} \sqcup\!\sqcup \left((\varphi_2)^*\right)^{\sqcup\!\sqcup \alpha_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup \left((\varphi_k)^*\right)^{\sqcup\!\sqcup \alpha_k} \\ &= \left(\alpha_1\varphi_1 + \alpha_2\varphi_2 + \cdots + \alpha_k\varphi_k\right)^*. \end{aligned} \tag{69}$$

The decreasing filtration of $\mathcal{B}$ is given by $\mathcal{B}_+^n = \bigoplus_{k \geq n} T_k(V)$ (the ideal of tensors of degree $\geq n$) and the reader may check easily that, in this case, $\mathcal{B}_\infty^\vee$ is the shuffle algebra of finitely supported linear forms – i.e., for each $\Phi \in \mathcal{B}^\vee$, we have the equivalence

$$\Phi \in \mathcal{B}_\infty^\vee \Longleftrightarrow (\exists N \in \mathbb{N})(\forall k \geq N)(\Phi(T_k(V)) = \{0\}).$$

Then, Corollary 5.12 shows that $(\varphi_i^*)_{i \in I}$ are $\mathcal{B}_\infty^\vee$-algebraically independent within $(T(V)^\vee, \sqcup\!\sqcup, \epsilon)$ if the corresponding monomial map is injective, and (69) shows that it is so iff the family $(\varphi_i)_{i \in I}$ of linear forms is $\mathbb{Z}$-linearly independent in $V^\vee$.

5.4. Appendix: Remarks on the dual of a tensor product

In Subsection 5.1, we have mentioned the difficulties of defining the dual coalgebra of a $\mathbf{k}$-algebra in the general case when $\mathbf{k}$ is not necessarily a field. As we said, these difficulties stem from the fact that the canonical map $M^\vee \otimes N^\vee \to (M \otimes N)^\vee$ (for two $\mathbf{k}$-modules M and N) is not generally an isomorphism, and may fail to be injective even if $\mathbf{k}$ is an integral domain. Even worse, the $\mathbf{k}$-module $M^\vee \otimes N^\vee$ may fail to be torsionfree (which automatically precludes any $\mathbf{k}$-linear map $M^\vee \otimes N^\vee \to (M \otimes N)^\vee$, not just the canonical one, from being injective). We shall soon give an example where this happens (Example 5.15). First, let us prove a positive result:

Proposition 5.14. *Let* $\mathbf{k}$ *be an integral domain. Let* M *and* N *be two* $\mathbf{k}$*-modules. Consider the canonical* $\mathbf{k}$*-linear map*

$$\Phi : M^\vee \otimes_{\mathbf{k}} N^\vee \longrightarrow (M \otimes_{\mathbf{k}} N)^\vee \tag{70}$$

[23] The one defined by

$$\Delta_{\boxtimes}(1) = 1 \otimes 1 \text{ and } \Delta_{\boxtimes}(u) = u \otimes 1 + 1 \otimes u \; ; \; \epsilon(u) = 0 \text{ for all } u \in V.$$

[24] For this bialgebra $\sqcup\!\sqcup$ stands for $\circledast$ on the space $\mathrm{Hom}(\mathcal{B}, \mathbf{k})$.

defined by

$$(\Phi(f \otimes g))(u \otimes v) = f(u)g(v) \qquad \text{for all } f \in M^\vee,\ g \in N^\vee,\ u \in M \text{ and } v \in N.$$

Then, the following are equivalent:

1. *The* $\mathbf{k}$*-module* $M^\vee \otimes_{\mathbf{k}} N^\vee$ *is torsionfree.*
2. *The map* Φ *is injective.*

First proof of Proposition 5.14. 1. $\Longrightarrow$ 2.) Assume that statement 1. holds. Thus, the $\mathbf{k}$-module $M^\vee \otimes_{\mathbf{k}} N^\vee$ is torsionfree.

We must prove that the map Φ is injective. Assume the contrary. Thus, $\ker \Phi \neq 0$. Therefore, there exists some nonzero $t \in M^\vee \otimes N^\vee$ such that $\Phi(t) = 0$. Consider this t. Consider all choices of nonzero $m \in \mathbf{k}$ and of elements $u_1, u_2, \ldots, u_r \in M^\vee$ and $v_1, v_2, \ldots, v_r \in N^\vee$ such that

$$mt = \sum_{i=1}^{r} u_i \otimes v_i. \tag{71}$$

Among all such choices, choose one for which r is minimum.

From the fact that r is minimum, we conclude that the elements $v_1, v_2, \ldots, v_r$ of $N^\vee$ are $\mathbf{k}$-linearly independent[25]. But the map Φ is $\mathbf{k}$-linear; hence, $\Phi(mt) = m\Phi(t) = 0$ (since $\Phi(t) = 0$). Thus, $0 = \Phi(mt) = \sum_{i=1}^{r} \Phi(u_i \otimes v_i)$ (by (71)). Hence, for all $x \in M$ and $y \in N$, we have

$$0 = \left(\sum_{i=1}^{r} \Phi(u_i \otimes v_i) \right)(x \otimes y) = \sum_{i=1}^{r} u_i(x) v_i(y) \tag{72}$$

[25]Here is the *proof* in detail: Assume the contrary. Thus, $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_r v_r = 0$ for some scalars $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbf{k}$, not all of which are zero. Consider these scalars, and assume WLOG that $\lambda_r \neq 0$. Hence, $\lambda_r m \neq 0$ (since $\mathbf{k}$ is an integral domain) and $\lambda_r v_r = -\sum_{i=1}^{r-1} \lambda_i v_i$ (since $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_r v_r = 0$). Now, multiplying the equality (71) with λ_r, we obtain

$$\begin{aligned}
\lambda_r mt &= \lambda_r \sum_{i=1}^{r} u_i \otimes v_i = \sum_{i=1}^{r} u_i \otimes \lambda_r v_i = \sum_{i=1}^{r-1} \underbrace{u_i \otimes \lambda_r v_i}_{=\lambda_r u_i \otimes v_i} + u_r \otimes \underbrace{\lambda_r v_r}_{=-\sum_{i=1}^{r-1} \lambda_i v_i} \\
&= \sum_{i=1}^{r-1} \lambda_r u_i \otimes v_i + u_r \otimes \left(-\sum_{i=1}^{r-1} \lambda_i v_i \right) = \sum_{i=1}^{r-1} \lambda_r u_i \otimes v_i - \sum_{i=1}^{r-1} \lambda_i u_r \otimes v_i \\
&= \sum_{i=1}^{r-1} (\lambda_r u_i - \lambda_i u_r) \otimes v_i.
\end{aligned}$$

This is an equality of the same shape as (71), but with $r-1$ instead of r (since $\lambda_r m \neq 0$). Hence, it contradicts the minimality of r. This contradiction completes our proof.

(by the definition of Φ). This can be rewritten as

$$0 = \sum_{i=1}^{r} u_i(x) v_i \text{ in } N^\vee \qquad \text{for all } x \in M. \tag{73}$$

But this entails that $u_i(x) = 0$ for all $1 \leq i \leq r$ (since $v_1, v_2, \ldots, v_r$ are $\mathbf{k}$-linearly independent). Since this holds for all $x \in M$, we thus find that $u_i = 0$ for all $1 \leq i \leq r$. Hence, (71) shows that $mt = 0$, so that $t = 0$ (since $M^\vee \otimes N^\vee$ is torsionfree). This contradicts $t \neq 0$. This contradiction completes the proof of 1. $\Longrightarrow$ 2.

2. $\Longrightarrow$ 1.) The $\mathbf{k}$-module $\left(M \otimes_{\mathbf{k}} N\right)^\vee$ is torsionfree, since the dual of any $\mathbf{k}$-module is torsionfree. Hence, if Φ is injective, then $M^\vee \otimes_{\mathbf{k}} N^\vee$ is torsionfree (since a submodule of a torsionfree $\mathbf{k}$-module is always torsionfree). □

Second proof of Proposition 5.14 (sketched). 1. $\Longrightarrow$ 2.) Assume that statement 1. holds. Thus, the $\mathbf{k}$-module $M^\vee \otimes_{\mathbf{k}} N^\vee$ is torsionfree.

We must prove that the map Φ is injective.

Let $\mathbf{F}$ be the fraction field of $\mathbf{k}$. For any $\mathbf{k}$-module P, we let $P_{\mathbf{F}}$ denote the $\mathbf{F}$-vector space $\mathbf{F} \otimes P$ (which can also be defined as the localization of P with respect to the multiplicatively closed subset $\mathbf{k} \setminus \{0\}$ of $\mathbf{k}$), and we let ι_P denote the canonical $\mathbf{k}$-linear map $P \to P_{\mathbf{F}}$. We note that ι_P is injective when P is torsionfree.

If V is an $\mathbf{F}$-vector space, then we shall write V^* for the dual space $\operatorname{Hom}_{\mathbf{F}}(V, \mathbf{F})$ of V. This should be distinguished from the $\mathbf{k}$-module dual of V, which we denote by $V^\vee$.

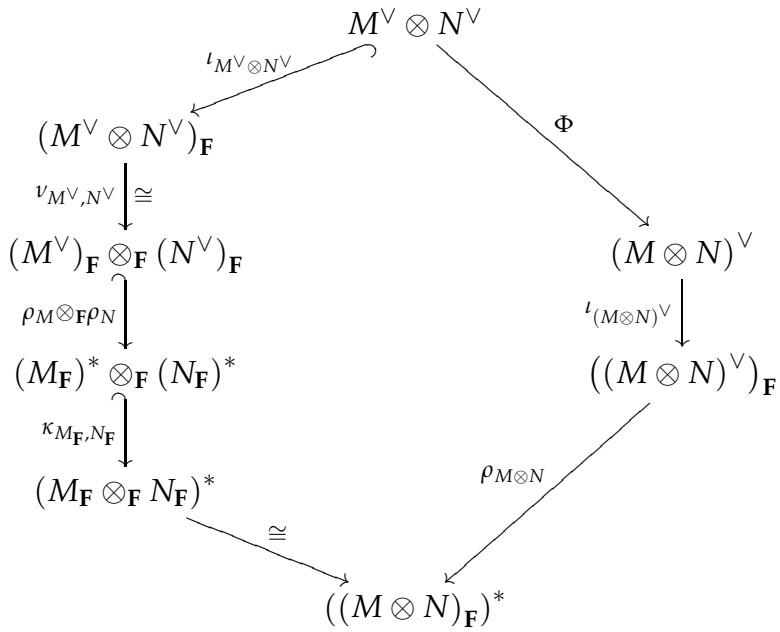
For any $\mathbf{k}$-module P, the canonical $\mathbf{F}$-linear map $\rho_P : (P^\vee)_{\mathbf{F}} \to (P_{\mathbf{F}})^*$ (which sends each $f \in P^\vee$ to the unique $\mathbf{F}$-linear map $P_{\mathbf{F}} \to \mathbf{F}$ that extends f) is injective. (This is easily checked by hand, using the fact that the map $\mathbf{k} \to \mathbf{F}$ is injective.) Hence, we obtain two injective $\mathbf{F}$-linear maps $\rho_M : (M^\vee)_{\mathbf{F}} \to (M_{\mathbf{F}})^*$ and $\rho_N : (N^\vee)_{\mathbf{F}} \to (N_{\mathbf{F}})^*$. Their tensor product is an injective $\mathbf{F}$-linear map $\rho_M \otimes_{\mathbf{F}} \rho_N : (M^\vee)_{\mathbf{F}} \otimes_{\mathbf{F}} (N^\vee)_{\mathbf{F}} \to (M_{\mathbf{F}})^* \otimes_{\mathbf{F}} (N_{\mathbf{F}})^*$ (since the tensor product of two injective $\mathbf{F}$-linear maps over $\mathbf{F}$ is injective, because $\mathbf{F}$ is a field).

For any $\mathbf{k}$-modules M and N, there is a canonical isomorphism $\nu_{M,N} : (M \otimes N)_{\mathbf{F}} \to M_{\mathbf{F}} \otimes_{\mathbf{F}} N_{\mathbf{F}}$. (This is a general property of base change.) Hence, $M_{\mathbf{F}} \otimes_{\mathbf{F}} N_{\mathbf{F}} \cong (M \otimes N)_{\mathbf{F}}$, so that $\left(M_{\mathbf{F}} \otimes_{\mathbf{F}} N_{\mathbf{F}}\right)^* \cong \left((M \otimes N)_{\mathbf{F}}\right)^*$.

Also, it is known from linear algebra that the canonical map $\kappa_{V,W} : V^* \otimes_{\mathbf{F}} W^* \to (V \otimes_{\mathbf{F}} W)^*$ is injective whenever V and W are two $\mathbf{F}$-vector spaces.

We assumed that $M^\vee \otimes N^\vee$ is torsionfree. Thus, the map $\iota_{M^\vee \otimes N^\vee}$ is injective. We

have the following commutative diagram of **k**-modules:



(74)

All maps along the left boundary of this diagram are injective; thus, their composition is injective as well. But this composition equals the composition of the maps along the right boundary of the diagram. Hence, the latter composition is injective. Thus, Φ (being the initial map in this composition) must be injective. This proves 1. $\Longrightarrow$ 2.

2. $\Longrightarrow$ 1.) As in the First proof above. $\square$

We can now give an example (communicated to us by Jeremy Rickard) where $M^\vee \otimes N^\vee$ fails to be torsionfree:

Example 5.15. Let **k** be a field, I and J infinite sets, and A the **k**-subalgebra of

$$\mathbf{k}(t)[x_i, y_j : i \in I, j \in J]$$

generated by

$$\{x_i, y_j, tx_i, t^{-1}y_j : i \in I \text{ and } j \in J\}.$$

Then, A is an integral domain. In this example, all duals are taken with respect to A (not with respect to **k**); that is, $M^\vee$ means $\mathrm{Hom}_A(M, A)$.

The free A-modules $A^{(I)}$, $A^{(J)}$ and $A^{(I\times J)}$ satisfy $\left(A^{(I)}\right)^\vee \cong A^I$, $\left(A^{(J)}\right)^\vee \cong A^J$, $\left(A^{(I\times J)}\right)^\vee \cong A^{I\times J}$, and $A^{(I\times J)} \cong A^{(I)} \otimes_A A^{(J)}$. Moreover, there is a natural A-linear map

$$\Psi : A^I \otimes_A A^J \to A^{I\times J},$$
$$(a_i)_{i\in I} \otimes_A (b_j)_{j\in J} \mapsto (a_i b_j)_{(i,j)\in I\times J}$$

that forms a commutative diagram

$$\begin{array}{ccc} A^I \otimes_A A^J & \xrightarrow{\Psi} & A^{I\times J} \\ \cong\downarrow & & \cong\downarrow \\ \left(A^{(I)}\right)^\vee \otimes_A \left(A^{(J)}\right)^\vee & \xrightarrow[\Phi]{} & \left(A^{(I\times J)}\right)^\vee \end{array} \tag{75}$$

with the canonical map $\Phi : \left(A^{(I)}\right)^\vee \otimes_A \left(A^{(J)}\right)^\vee \to \left(A^{(I\times J)}\right)^\vee$ defined as in Proposition 5.14.

Now, we define an element

$$\xi = (tx_i)_{i\in I} \otimes_A (t^{-1}y_j)_{j\in J} - (x_i)_{i\in I} \otimes_A (y_j)_{j\in J} \in A^I \otimes_A A^J.$$

It is clear by computation that $\Psi(\xi) = 0$. We shall now show that $\xi \neq 0$.

Indeed, assume the contrary. Thus, $\xi = 0$. Hence, ξ can be "shown to be zero using only finitely many elements of A" – i.e., there exists a finitely generated $\mathbf{k}$-subalgebra B of A such that

$$(tx_i)_{i\in I} \otimes_B (t^{-1}y_j)_{j\in J} - (x_i)_{i\in I} \otimes_B (y_j)_{j\in J} = 0 \qquad \text{in } A^I \otimes_B A^J. \tag{76}$$

(Indeed, $A^I \otimes_A A^J$ can be viewed as a quotient of $A^I \otimes_{\mathbb{Z}} A^J$ modulo the $\mathbb{Z}$-submodule spanned by all the differences $ua \otimes_{\mathbb{Z}} v - u \otimes_{\mathbb{Z}} av$ for $u \in A^I$, $v \in A^J$ and $a \in A$. Thus, $\xi = 0$ means that the element $(tx_i)_{i\in I} \otimes_{\mathbb{Z}} (t^{-1}y_j)_{j\in J} - (x_i)_{i\in I} \otimes_{\mathbb{Z}} (y_j)_{j\in J}$ of $A^I \otimes_{\mathbb{Z}} A^J$ is a $\mathbb{Z}$-linear combination of finitely many such differences. Now take the (finitely many) a's involved in these differences, and define B to be the $\mathbf{k}$-subalgebra of A generated by these finitely many a's. Then, (76) holds, as desired.)

Consider this B. Choose $r \in I$ and $s \in J$ so that

$$B \subseteq \mathbf{k}(t)[x_i, y_j : i \neq r \text{ and } j \neq s].$$

(Such r and s exist, since B is finitely generated.)

If m is a monomial in the variables $\{x_i, y_j : i \in I, j \in J\}$, then $\deg_x m$ shall denote the total degree of m in the variables x_i, while $\deg_y$ shall denote the total degree of m in the variables y_j. A good monomial shall mean a product of the form $t^l m$, where m is a monomial in the variables $\{x_i, y_j : i \in I, j \in J\}$ and $l \in \mathbb{Z}$ satisfies $-\deg_y m \leq l \leq \deg_x m$. As a $\mathbf{k}$-vector space, A has a basis consisting of all good monomials.

A good monomial $t^l m$ will be called strict if m is just a power of x_r or just a power of y_s. (In particular, the monomial 1 is strict.) The non-strict good monomials span a proper ideal of A. Let $\bar{A}$ be the corresponding quotient algebra of A; then the image $\bar{B}$ of B in $\bar{A}$ is just (a copy of) $\mathbf{k}$ (since every element of B is a $\mathbf{k}$-linear combination of non-strict good monomials and of the monomial 1). For any $f \in A$, we let $\overline{f}$ denote the canonical projection of f on the quotient ring $\bar{A}$.

Now, we have a $\mathbf{k}$-linear map obtained by composing

$$A^I \otimes_B A^J \to \bar{A}^I \otimes_{\bar{B}} \bar{A}^J \xrightarrow{\cong} \bar{A}^I \otimes_{\mathbf{k}} \bar{A}^J \to \bar{A} \otimes_{\mathbf{k}} \bar{A},$$

where

- the first arrow sends each tensor $u \otimes_B v \in A^I \otimes_B A^J$ to the tensor $\overline{u} \otimes_{\bar{B}} \overline{v} \in \bar{A}^I \otimes_{\bar{B}} \bar{A}^J$ (with $\overline{u}$ denoting the projection of $u \in A^I$ to $\bar{A}^I$, and with $\overline{v}$ defined similarly);
- the second arrow is due to $\bar{B}$ being (a copy of) $\mathbf{k}$;
- the third arrow is obtained by tensoring

$$\begin{aligned} &\text{the canonical projection } \bar{A}^I \to \bar{A},\ (a_i)_{i\in I} \mapsto a_r \\ \text{with } &\text{the canonical projection } \bar{A}^J \to \bar{A},\ \left(b_j\right)_{j\in J} \mapsto b_s. \end{aligned}$$

Applying this $\mathbf{k}$-linear map to both sides of the equation (76), we obtain

$$\overline{tx_r} \otimes_{\mathbf{k}} \overline{t^{-1}y_s} - \overline{x_r} \otimes_{\mathbf{k}} \overline{y_s} = 0 \qquad \text{in } \bar{A} \otimes_{\mathbf{k}} \bar{A}.$$

But this contradicts the fact that the four basis elements $\overline{tx_r}, \overline{t^{-1}y_s}, \overline{x_r}, \overline{y_s}$ of $\bar{A}$ are $\mathbf{k}$-linearly independent.

Hence, our assumption ($\xi = 0$) was false. Thus, $\xi \neq 0$. In view of $\Psi(\xi) = 0$, this shows that Ψ is not injective. Due to the commutative diagram (75), this means that Φ is not injective. Hence, Proposition 5.14 shows that the A-module $\left(A^{(I)}\right)^\vee \otimes_A \left(A^{(J)}\right)^\vee$ is not torsionfree. In view of (75), this means in turn that the A-module $A^I \otimes_A A^J$ is not torsionfree (despite being the tensor product of the two torsionfree, and even torsionless, A-modules A^I and A^J).

The presence of torsion in $A^I \otimes_A A^J$ can also be seen directly using the element ξ from the above argument: For any $s \in I$, we have

$$x_s \xi = x_s \left((tx_i)_{i\in I} \otimes_A (t^{-1}y_j)_{j\in J} - (x_i)_{i\in I} \otimes_A (y_j)_{j\in J} \right) = 0,$$

since

$$\begin{aligned} x_s \left((tx_i)_{i\in I} \otimes_A (t^{-1}y_j)_{j\in J} \right) &= (tx_s x_i)_{i\in I} \otimes_A (t^{-1}y_j)_{j\in J} \\ &= (x_i)_{i\in I} \otimes_A (x_s y_j)_{j\in J} \\ &= x_s \left((x_i)_{i\in I} \otimes_A (y_j)_{j\in J} \right). \end{aligned}$$

Another example of a non-injective canonical map $A^I \otimes_A A^J \to A^{I\times J}$ (and thus, of a tensor product of the form $M^\vee \otimes_A N^\vee$ having torsion) can be found in the last two paragraphs of [Goodea72].

Note that such examples can only exist when A is not Noetherian. Indeed, it has been shown in [AbGoWi99, Proposition 1.2] that if A is a Noetherian ring, then the canonical map $A^I \otimes_A A^J \to A^{I\times J}$ for any two sets I and J is injective.

References

[Abe80] Eiichi Abe, *Hopf algebras*, Cambridge Tracts in Mathematics **74**. Cambridge University Press, Cambridge-New York, 1980.

[AbGoWi99] J. Y. Abuhlail, J. Gómez-Torrecillas, R. Wisbauer, *Dual coalgebras of algebras over commutative rings*, Journal of Pure and Applied Algebra **153** (2000), pp. 107–120.

[Artin71] Emil Artin, *Galois Theory*, Notre Dame Mathematical Lectures **2**, University of Notre Dame Press, 1971. `https://projecteuclid.org/euclid.ndml/1175197041`

[BeRe88] J. Berstel, C. Reutenauer, *Rational series and their languages*, Springer-Verlag, 1988.

[GoF04] G. Duchamp, K.A. Penson, A.I. Solomon, A. Horzela and P. Blasiak, *One-Parameter Groups and Combinatorial Physics*, Scientific World Publishing (2004).
`arXiv:quant-ph/0401126`.

[Bourba89] N. Bourbaki, *Algebra I (Chapters 1-3)*, Springer 1989.

[Bourba98] N. Bourbaki, *Lie groups and Lie algebras (Chapters 1-3)*, Springer 1998.

[Bourba72] N. Bourbaki, *Commutative Algebra*, Hermann 1972.

[Bui12] V. C. Bui, *Hopf algebras of shuffles and quasi-shuffles. Constructions of dual bases*, Master dissertation (2012).

[BDMKT16] V. C. Bui, G. H. E. Duchamp, Hoang Ngoc Minh, L. Kane, C. Tollu, *Dual bases for noncommutative symmetric and quasi-symmetric functions via monoidal factorization*, Journal of Symbolic Computation **75** (2016), pp. 56–73.

[Car07] Pierre Cartier.– *A primer of Hopf algebras*, in: Cartier P., Moussa P., Julia B., Vanhove P. (eds), Frontiers in Number Theory, Physics, and Geometry II, (2007).

[CaFo69] P. Cartier, D. Foata, *Commutation and Rearrangements*, An electronic reedition of the monograph *Problèmes combinatoires decommutation et réarrangements*, Lect. Notes in Math. **85** Springer-Verlag (1969), with three new appendices by D. Foata, B. Lassand Ch. Krattenthaler (2006)

[ChFoLy58] K.T. Chen, R.H. Fox, R.C. Lyndon, *Free differential calculus, IV: The quotient groups of the lower central series*, Ann. of Math. (2) **68** (1958), pp. 163–178.

[DGM2-20] Gérard H. E. Duchamp, Darij Grinberg, Hoang Ngoc Minh, *Kleene stars in shuffle bialgebras*, forthcoming.

[Duc97] G. Duchamp, C. Reutenauer, *Un critère de rationalité provenant de la géométrie noncommutative*, Inventiones Mathematicae, **128** (1997), pp. 613–622.

[DuKr93] G. Duchamp, D.Krob, *Free partially commutative structures*, Journal of Algebra, 156 , 318-359 (1993)

[DucTol09] Gérard H. E. Duchamp, Christophe Tollu, *Sweedler's duals and Schützenberger's calculus*, In K. Ebrahimi-Fard, M. Marcolli and W. van Suijlekom (eds), Combinatorics and Physics, pp. 67–78, Amer. Math. Soc. (Contemporary Mathematics, vol. 539), 2011. arXiv:0712.0125v3.

[DMTCN14] Gérard H. E. Duchamp, Vincel Hoang Ngoc Minh, Christophe Tollu, Bùi van Chiên, Nguyen Hoang Nghia, *Combinatorics of ϕ-deformed stuffle Hopf algebras*, arXiv:1302.5391v7.

[DuMiNg19] G.H.E. Duchamp, V. Hoang Ngoc Minh, Q.H. Ngo, *Kleene stars of the plane, polylogarithms and symmetries*, Theoretical Computer Science **800** (2019), pp. 52–72, arXiv:1811.09091v2.

[Ducham15] Gérard H. E. Duchamp, *MathOverflow answer #216201: Important formulas in combinatorics*, https://mathoverflow.net/a/216201

[Ducham01] G. Duchamp, M. Flouret, É. Laugerotte, J.-G. Luque, *Direct and dual laws for automata with multiplicities*, Theoretical Computer Science **267** (2001), pp. 105–120, arXiv:math/0607412v1.

[1] S. Eilenberg, *Automata, languages and machines, vol A*. Acad. Press, New-York, 1974.

[Goodea72] K. R. Goodearl, *Distributing Tensor Product over Direct Product*, Pacific Journal of Mathematics **43**, no. 1 (1972), pp. 107–110.

[Grinbe17] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019, arXiv:2008.09862v1.

[GriRei20] Darij Grinberg, Victor Reiner, *Hopf algebras in Combinatorics*, version of 27 July 2020, arXiv:1409.8356v7.
See also http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf for a version that gets updated.

[MM65] J.W. Milnor and J.C. Moore, *On the structure of Hopf algebras*, Ann. of Math. (2) **81** (1965), pp. 211–264.

[PatReu02] Frédéric Patras, Christophe Reutenauer, *On Dynkin and Klyachko Idempotents in Graded Bialgebras*, Advances in Applied Mathematics **28** (2002), pp. 560–579.

[Radfor12] David E. Radford, *Hopf algebras*, Series on Knots and Everything **49**. World Scientific, 2012.

[Reuten93] Christophe Reutenauer, *Free Lie Algebras*, London Math. Soc. Monographs, 1993.

[RodTaf05] Suemi Rodríguez-Romo, Earl J. Taft, *A left quantum group*, Journal of Algebra **286** (2005), pp. 154–160.

[Schütz61] Marcel-Paul Schützenberger, *On the definition of a family of automata*, Information and Control, **4** (1961), pp. 245–270.

[Sweedl69] Moss E. Sweedler, *Hopf algebras*, W.A. Benjamin, New York, 1969.