



Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation
ESA - CNRS 6090

Endomorphisms of the binomial coalgebra

M. Héraoua & A. Salinier

Rapport de recherche n° 2002-03

Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex
Tél. 05 55 45 73 23 - Fax. 05 55 45 73 22 - laco@unilim.fr

<http://www.unilim.fr/laco/>

Endomorphisms of the binomial coalgebra

M. Héraoua and A. Salinier

Abstract. The algebra of formal Hurwitz series has been recently investigated in view of potential applications to differential algebra. In the case where the ground ring is a reduced ring of prime characteristic, this paper describes continuous endomorphisms of the algebra of Hurwitz series - or equivalently endomorphisms of the binomial coalgebra. This is made by means of the investigation of the coradical filtration of this coalgebra and of components of linear maps between some graded modules that naturally arise in the problem. Our problem is tantamount to determine all polynomial sequences of binomial type. As such, it contains the study of sequences built by Carlitz in the context of his discovery of the Carlitz module.

Mathematics Subject Classification (2000): Primary 16W20, 16W30 ; secondary 05A40, 13A35, 13J99, 16W50.

Key words: coalgebra endomorphisms, binomial coalgebra, graded modules, coradical filtration, Hurwitz series, Carlitz module.

A close relative of the algebra of formal power series, namely the algebra of formal Hurwitz series has been studied recently by Keigher and Pritchard [9]. Its main interest lies in the fact that it provides formal solutions to homogeneous linear ordinary differential equations in any characteristic and so seems to have many potential applications to the study of differential algebra. Seeking to interpret the elements of this algebra as formal functions, Keigher and Pritchard have defined a composition of Hurwitz series. As in the realm of formal power series, this composition allows to build endomorphisms of the algebra by composition on the right with a fixed series that is without constant term. It is therefore natural to ask whether all endomorphisms of the algebra of formal Hurwitz series are of this kind, as it is indeed true for formal power series.

The main objective of this paper is to describe all continuous endomorphisms of the algebra of formal Hurwitz series in the case where the ground ring is a reduced ring of prime characteristic p . We shall see that other endomorphisms do exist that those arising from the composition of Hurwitz series.

The principal idea for our description stems from the umbral calculus. In the case where the ground ring is a field of characteristic 0, it has been shown indeed [12, 13] that umbral calculus can be traced back to the existence of a duality between polynomials and formal power series, leading to an interplay between the structure of the algebra of polynomials and the less apparent structure of coalgebra that is induced by this duality. Whatever characteristic has the ground ring, we observe in an analogous way that the dual of the algebra of formal Hurwitz series is, up to a topological isomorphism, nothing but the univariate binomial coalgebra \mathcal{B}_1 , as defined by Joni and Rota in [7]. Thus it is

clear that transposition maps bijectively the set of endomorphisms of the coalgebra \mathcal{B}_1 to the set of continuous endomorphisms of the algebra of formal Hurwitz series. Hence the problem to describe completely all continuous endomorphisms of the algebra of formal Hurwitz series is the same as to determine all endomorphisms of this binomial coalgebra.

This way to deal with the problem seems to make it more tractable, as we can use the tools of the coalgebra theory. In particular, the determination of the so-called “coradical filtration”, its interpretation as the filtration canonically associated to a very simple grading of \mathcal{B}_1 , the systematical use of the components of the linear maps between graded modules that naturally arise in our problem, are the foundations upon which our exposition rests. These results appear to be not directly translatable to properties of the dual algebra.

As it is well-known [7], the problem to determine the endomorphisms of the binomial coalgebra is tantamount to determine all polynomial sequences $(p_n)_n$ of binomial type, that is satisfying the binomial identity

$$p_n(x + y) = \sum_{\beta=0}^n \binom{n}{\beta} p_\beta(x) p_{n-\beta}(y) .$$

In the case where the ground ring is a field of characteristic zero, it has been observed that the automorphisms of this coalgebra, often called umbral operators, were in bijective correspondance with the polynomial sequences of binomial type [7, 12]. It means in particular that the degree of an element of the binomial coalgebra is invariant by every automorphism. In the case of prime characteristic, on the contrary, we shall see that there exist automorphisms of \mathcal{B}_1 that do not preserve the degree, as in our Example 4 (see Section 5). Precisely, we shall even show that every endomorphism of the submodule of primitive elements of \mathcal{B}_1 can be extended to an endomorphism of \mathcal{B}_1 .

In positive characteristic, an other method for building polynomial sequences of binomial type has been provided by Carlitz [2] in the context of his discovery of the object now known as the Carlitz module. His construction is described as follows. Let R be the ground ring, of which the characteristic is the prime number p . Given a sequence $(\psi_i)_{i \in \mathbb{N}}$ of additive polynomials, it suffices to set for each integer $k = \alpha_0 + \alpha_1 p + \dots + \alpha_s p^s$ where $0 \leq \alpha_i < p$:

$$G_k(t) = \psi_0(t)^{\alpha_0} \psi_1(t)^{\alpha_1} \dots \psi_s(t)^{\alpha_s} .$$

Then one can easily check, using the Lucas congruences, that the sequence $(G_k)_{k \in \mathbb{N}}$ is of binomial type. Hence by identifying \mathcal{B}_1 with $R[x]$, the R -linear map ϕ from $R[x]$ to $R[x]$ that sends x^k to $G_k(x)$ is an endomorphism of the R -coalgebra \mathcal{B}_1 . Still we shall see that not all the endomorphisms of the binomial coalgebra can be obtained by this process, as illustrated by our Example 4 (see Section 5).

Our paper is organized as follows. In Section 1, we first recall some facts about graded modules, graded maps and binomial coefficients. These results appear to be more or less known, but are resumed in order to supply a suitable reference for our work. Next Section 2 deals with the multi-integers and partitions and more particularly, we shall give some results concerning computation modulo p of multinomial coefficients. Then in Section 3 we shall introduce the main object of our paper, that is the binomial coalgebra, denoted by \mathcal{B}_1 after Joni and Rota, and examine a particular grading of this coalgebra which

allows us to characterize a coalgebra endomorphism by some of its components (Theorem 3.16). In order to reverse the process by building a coalgebra endomorphism from these particular components, we shall address in Section 4 the link between multi-integers and the coalgebraic structures, which will enable us to determine the wanted endomorphisms. Eventually, we shall examine a few examples in Section 5.

1 Basic notions

1.1 Graded modules

Let R be a fixed commutative ring, which will be called the *ground ring*. For every R -module M , let I_M denote the identity map of M .

Gradings

Let M be a R -module and Δ a non-empty set. Recall [1, chapitre II, page 164] that a *grading* of type Δ on M is the data, for each element δ in Δ , of a submodule M_δ of M , such that the family $(M_\delta)_{\delta \in \Delta}$ satisfies :

$$M = \bigoplus_{\delta \in \Delta} M_\delta .$$

Definition 1.1 *A graded module of type Δ , consists in a R -module M together with a grading of type Δ on M .*

Setting a graded R -module M of type Δ yields the maps $i_\delta : M_\delta \rightarrow M$ such that $i_\delta(x) = x$ for each x in M_δ . Besides, a unique map pr^δ from M to M_δ is defined by

$$\text{pr}^\delta \circ i_{\delta'} = \begin{cases} I_{M_\delta} & \text{if } \delta = \delta' ; \\ 0 & \text{if } \delta \neq \delta' . \end{cases} \quad (1)$$

Components of a linear map

Definition 1.2 *Let u a linear map of the graded R -module M of type Γ into the graded R -module N of type Δ . Fix $\gamma \in \Gamma$ and $\delta \in \Delta$. The (γ, δ) -component of u is defined to be the linear map u_γ^δ from M_γ to N_δ such that*

$$u_\gamma^\delta = \text{pr}^\delta \circ u \circ i_\gamma .$$

Notice that

$$u = \sum_{(\gamma, \delta) \in \Gamma \times \Delta} i_\delta \circ u_\gamma^\delta \circ \text{pr}^\gamma . \quad (2)$$

This makes sense since, for every x in M , the element $i_\delta \circ u_\gamma^\delta \circ \text{pr}^\gamma(x)$ is trivial except for a finite number of (γ, δ) .

Remark 1.3 Let M and N two graded R -modules of types respectively Γ and Δ . Two linear maps u and v from M to N are equal if and only if they have the same components, that is if and only if, for each element (γ, δ) in $\Gamma \times \Delta$, we have :

$$u_{\gamma}^{\delta} = v_{\gamma}^{\delta}.$$

Computation of components of the composition of two linear maps

Proposition 1.4 Let u be a linear map from a graded R -module M of type Γ to a graded R -module N of type Δ and let v be an other linear map from a graded R -module N of type Δ to a graded R -module P of type E . For every element $(\gamma, \delta, \varepsilon)$ in $\Gamma \times \Delta \times E$, the (γ, ε) -component of $v \circ u$ is

$$(v \circ u)_{\gamma}^{\varepsilon} = \sum_{\delta \in \Delta} v_{\delta}^{\varepsilon} \circ u_{\gamma}^{\delta}.$$

This sum makes sense since for a fixed x in M , the element $v_{\delta}^{\varepsilon} \circ u_{\gamma}^{\delta}(x)$ is zero except for finitely many δ .

Proof. Fix γ and ε in Γ and E respectively. The first step of the proof consists in applying Definition 1.2, getting

$$(v \circ u)_{\gamma}^{\varepsilon} = \text{pr}^{\varepsilon} \circ (v \circ u) \circ i_{\gamma};$$

by associativity of composition, this becomes

$$(v \circ u)_{\gamma}^{\varepsilon} = (\text{pr}^{\varepsilon} \circ v) \circ (u \circ i_{\gamma}); \quad (3)$$

but equality (2) yields :

$$v = \sum_{(\delta, \varepsilon') \in \Delta \times E} i_{\varepsilon'} \circ v_{\delta}^{\varepsilon'} \circ \text{pr}^{\delta} \quad \text{and} \quad u = \sum_{(\gamma', \delta') \in \Gamma \times \Delta} i_{\delta'} \circ u_{\gamma'}^{\delta'} \circ \text{pr}^{\gamma'}.$$

Substituting these expressions in equality (3) gives :

$$(v \circ u)_{\gamma}^{\varepsilon} = \sum_{(\delta, \varepsilon') \in \Delta \times E} \sum_{(\gamma', \delta') \in \Gamma \times \Delta} \text{pr}^{\varepsilon} \circ i_{\varepsilon'} \circ v_{\delta}^{\varepsilon'} \circ \text{pr}^{\delta} \circ i_{\delta'} \circ u_{\gamma'}^{\delta'} \circ \text{pr}^{\gamma'} \circ i_{\gamma}.$$

Finally, the result is deduced from relations (1).

Graded maps

Definition 1.5 Let M and N be two graded R -modules of the same type Δ . A R -linear map u from M to N is said to be graded when $u(M_{\delta}) \subseteq N_{\delta}$ for each δ in Δ .

We have just defined the category of graded modules of type Δ ; one can readily verify that it is an abelian category.

The map u is graded if and only if the component $u_{\delta}^{\delta'}$ is trivial whenever $\delta \neq \delta'$. In this case, equality (2) becomes :

$$u = \sum_{\delta \in \Delta} i_{\delta} \circ u_{\delta} \circ \text{pr}^{\delta} \quad (4)$$

where $u_\delta = u_\delta^\delta$.

Generally speaking, given a graded R -module M of type Γ , a graded R -module N of type Δ and a map ρ from Δ to Γ , we know [1, chapitre II, page 163, exemple 2] how to define the grading of N of type Γ deduced from $(N_\delta)_{\delta \in \Delta}$ by means of the map ρ . A R -linear map u from M to N is said to be ρ -graded when it is graded in the sense of Definition 1.5 for the gradings of type Γ given on M and thus defined on N . This is equivalent to the condition :

$$u(M_\gamma) \subseteq \bigoplus_{\rho(\delta)=\gamma} N_\delta$$

for each γ in Γ . The map u is ρ -graded if and only if the component u_γ^δ is trivial whenever $\rho(\delta) \neq \gamma$. Then equality (2) becomes :

$$u = \sum_{\delta \in \Delta} i_\delta \circ u_\delta \circ \text{pr}^{\rho(\delta)} \quad (5)$$

setting $u_\delta = u_{\rho(\delta)}^\delta$.

Tensor product of graded modules

Let M and N be two R -modules of type Γ and Δ respectively. The tensor product $M \otimes_R N$ is endowed with the product grading of type $\Gamma \times \Delta$, given by the decomposition in direct summands :

$$M \otimes_R N = \bigoplus_{(\gamma, \delta) \in \Gamma \times \Delta} (i_\gamma \otimes i_\delta)(M_\gamma \otimes_R N_\delta),$$

where $i_\gamma : M_\gamma \rightarrow M$ and $i_\delta : N_\delta \rightarrow N$ are the injections defined above.

When M and N are flat R -modules, so are their direct summands M_γ and N_δ . In this case, we shall systematically identify the R -module $M_\gamma \otimes_R N_\delta$ with its image by the injection $i_\gamma \otimes i_\delta$, thus writing :

$$M \otimes_R N = \bigoplus_{(\gamma, \delta) \in \Gamma \times \Delta} (M_\gamma \otimes_R N_\delta).$$

Components of the tensor product of two linear maps

Proposition 1.6 *Let M_1, M_2, N_1 and N_2 four flat graded R -modules of types $\Gamma_1, \Gamma_2, \Delta_1$ and Δ_2 respectively. Let u a linear map from M_1 to N_1 and v an other linear map from M_2 to N_2 . For each element $(\gamma_1, \gamma_2, \delta_1, \delta_2)$ in $\Gamma_1 \times \Gamma_2 \times \Delta_1 \times \Delta_2$ we have :*

$$(u \otimes v)_{(\gamma_1, \gamma_2)}^{(\delta_1, \delta_2)} = u_{\gamma_1}^{\delta_1} \otimes v_{\gamma_2}^{\delta_2}.$$

Proof. For every $(\gamma_1, \gamma_2, \delta_1, \delta_2)$ fixed in $\Gamma_1 \times \Gamma_2 \times \Delta_1 \times \Delta_2$, Definition 1.2 yields

$$(u \otimes v)_{(\gamma_1, \gamma_2)}^{(\delta_1, \delta_2)} = \text{pr}^{(\delta_1, \delta_2)} \circ (u \otimes v) \circ i_{(\gamma_1, \gamma_2)}.$$

Since M_1, M_2, N_1 and N_2 are flat R -modules, as already noticed, the tensor product of the homogenous components is identified with the homogenous component of the tensor product, which is expressed by the identities :

$$\text{pr}^{(\delta_1, \delta_2)} = \text{pr}^{\delta_1} \otimes \text{pr}^{\delta_2} \quad \text{and} \quad i_{(\gamma_1, \gamma_2)} = i_{\gamma_1} \otimes i_{\gamma_2}.$$

thus :

$$\begin{aligned}
(u \otimes v)_{(\gamma_1, \gamma_2)}^{(\delta_1, \delta_2)} &= (\text{pr}^{\delta_1} \otimes \text{pr}^{\delta_2}) \circ (u \otimes v) \circ (i_{\gamma_1} \otimes i_{\gamma_2}) \\
&= (\text{pr}^{\delta_1} \circ u \circ i_{\gamma_1}) \otimes (\text{pr}^{\delta_2} \circ v \circ i_{\gamma_2}) \\
&= u_{\gamma_1}^{\delta_1} \otimes v_{\gamma_2}^{\delta_2},
\end{aligned}$$

hence the result.

Tensor algebra of a graded module

Let M be a flat graded R -module of type Γ and let $\widehat{\Gamma}$ stand for the disjoint union of the sets Γ^j where j runs over \mathbb{N} . The tensor algebra $T(M)$ of the R -module M is endowed with the grading of type $\widehat{\Gamma}$ that associates to every “multi-degree” $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_j) \in \Gamma^j$ the submodule $T_\gamma(M) = M_{\gamma_1} \otimes M_{\gamma_2} \otimes \dots \otimes M_{\gamma_j}$, so that $T(M) = \bigoplus_{\gamma \in \widehat{\Gamma}} T_\gamma(M)$. Further, the grading thus defined is compatible with the tensor product, in the sense that the tensor product of an element of $T_\gamma(M)$ by an element of $T_{\gamma'}(M)$ belongs to $T_{\gamma\gamma'}(M)$ where the product in Γ of γ and γ' is the concatenation product of words, that is, if $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_j)$ and $\gamma' = (\gamma_{j+1}, \gamma_{j+2}, \dots, \gamma_{j+h})$, then

$$\gamma\gamma' = (\gamma_1, \gamma_2, \dots, \gamma_j, \gamma_{j+1}, \dots, \gamma_{j+h}). \quad (6)$$

1.2 Binomial coefficients

Let p be a prime number, fixed throughout the paper.

An ordering of natural integers

Let a, b be two natural integers, let $\binom{b}{a}$ denote, as usual, the binomial coefficient defined by the identity

$$(1+x)^b = \sum_{a \geq 0} \binom{b}{a} x^a$$

between polynomials. In particular $\binom{b}{a} = 0$ when $a > b$.

Definition 1.7 Let \prec stand for the binary relation over \mathbb{N} such that

$$a \prec b \iff \binom{b}{a} \not\equiv 0 \pmod{p}.$$

Lemma 1.8 If $a \prec b$ then $a \leq b$.

Lemma 1.9 The relation \prec is an order relation over \mathbb{N} .

Proof. The reflexivity of \prec is straightforward, the antisymmetry results directly from Lemma 1.8 and the transitivity from the equality $\binom{c}{a} \binom{c-a}{c-b} = \binom{b}{a} \binom{c}{b}$.

Sum of digits function

Definition 1.10 *The sum of base p digits function is the function s_p from \mathbb{N} to itself defined by the induction formulas*

$$s_p(0) = 0 \quad \text{and} \quad s_p(qp + r) = s_p(q) + r \quad \text{if} \quad 0 \leq r < p.$$

When a is a natural integer, let $\mathbb{N}_{a,p}$ be the set of all natural integers n such that $s_p(n) = a$.

Recall that the p -adic valuation \mathcal{V}_p is the map from \mathbf{Q} to $\mathbb{Z} \cup \{+\infty\}$ defined by $\mathcal{V}_p(0) = +\infty$ and for $x \in \mathbf{Q}^*$, $\mathcal{V}_p(x) = r$ for $x = p^r \frac{a}{b}$ where a and b are integers coprime to p .

Lemma 1.11 *For every n in \mathbb{N} and every l in the set $\{0, 1, \dots, n\}$, the p -adic valuation of the binomial coefficient is given by the formula :*

$$\mathcal{V}_p \left(\binom{n}{l} \right) = \frac{s_p(l) + s_p(n-l) - s_p(n)}{p-1}.$$

Corollary 1.12 *Let a and b be two natural integers such that $a \leq b$; then $a \prec b$ is equivalent to $s_p(b-a) = s_p(b) - s_p(a)$.*

Proof. By definition, the relation $a \prec b$ is equivalent to the vanishing of the p -adic valuation of the binomial coefficient $\binom{b}{a}$, hence the result by Lemma 1.11.

Lemma 1.13 *Let a and b be two natural integers such that $a \neq b$. If $a \prec b$ then $s_p(a) < s_p(b)$.*

Proof. By corollary 1.12, $a \prec b$ imply that $s_p(b-a) = s_p(b) - s_p(a)$ therefore $s_p(a) < s_p(b)$.

Lemma 1.14 *Let n be a natural integer such that $n > 0$, there exists a natural integer l such that :*

$$l \prec n \quad \text{and} \quad s_p(l) = s_p(n) - 1.$$

Proof. We write the base p representation of n as $n = \sum_{\mu=0}^d \alpha_{\mu} p^{\mu}$; since $n > 0$, there exists some index $r \in \{0, 1, \dots, d\}$ such that $\alpha_{\mu_r} > 0$. Let us set then $l = n - p^{\mu_r}$, so that $s_p(l) = s_p(n) - 1$. It remains to prove that $l \prec n$; for this, it is sufficient to compute the p -adic valuation of $\binom{n}{l}$:

$$\mathcal{V}_p \left(\binom{n}{l} \right) = \frac{s_p(l) + s_p(n-l) - s_p(n)}{p-1}.$$

But $s_p(l) - s_p(n) = -1$ and $s_p(n-l) = s_p(p^{\mu_r}) = 1$ thus $\mathcal{V}_p \left(\binom{n}{l} \right) = 0$ and therefore $\binom{n}{l}$ is coprime to p , that is $l \prec n$.

2 Multi-integers and partitions

2.1 Multi-integers

Definitions and notations

A *multi-integer* \mathbf{a} of length j is a list $\mathbf{a} = (a_1, a_2, \dots, a_j) \in \mathbb{N}^j$ where the a_i for $1 \leq i \leq j$ are all natural integers. Let $\widehat{\mathbb{N}}$ denote the set $\bigcup_{j \in \mathbb{N}} \mathbb{N}^j$ of all multi-integers of any length. We provide then $\widehat{\mathbb{N}}$ with the concatenation operation defined by formula (6). For every multi-integer \mathbf{a} and for every natural integer n , we denote by $\mathbf{a}^{\times n}$ the n -th power of \mathbf{a} for this concatenation operation.

Let \mathbf{a} be a multi-integer, let $\mathbf{a}!$ stand for the natural integer $\mathbf{a}! = a_1!a_2!\dots a_j!$, called the *factorial* of \mathbf{a} . Moreover $|\mathbf{a}|$ is defined as the natural integer $|\mathbf{a}| = a_1 + a_2 + \dots + a_j$, that we call the *degree* of \mathbf{a} . For $\mathbf{a} = (a_1, a_2, \dots, a_j)$ a multi-integer of length j and p a prime number, let $\mathbb{N}_{\mathbf{a},p}$ stand for $\mathbb{N}_{a_1,p} \times \mathbb{N}_{a_2,p} \times \dots \times \mathbb{N}_{a_j,p}$.

We shall have to use the following interpretation of the base p representation of an integer n , where p is a fixed prime number. Let n be an integer, such that $s_p(n) = j$. We write $n = \alpha_0 + \alpha_1 p + \dots + \alpha_s p^s$, the base p representation of n , so that the integers α_i belong to $\{0, \dots, p-1\}$ for each $i \in \{0, \dots, s\}$ satisfy $\alpha_0 + \alpha_1 + \dots + \alpha_d = j$. Then one defines a map ω from $\mathbb{N}_{j,p}$ to $\mathbb{N}_{1 \times j, p}$ by setting

$$\omega(n) = 1^{\times \alpha_0} p^{\times \alpha_1} \dots p^{d \times \alpha_d}.$$

Lemma 2.1 *The map ω satisfy the identity*

$$|\omega(n)| = n$$

for every integer $n \in \mathbb{N}_{j,p}$.

This allows us to generalize Lemma 1.14 in the following way.

Lemma 2.2 *Let n be a natural integer such that $s_p(n) = j$ and let i be a natural integer such that $i < j$. Then there exists a natural integer l such that $l \prec n$ and $s_p(l) = i$.*

Proof. Let $\omega(n) = 1^{\times \alpha_0} p^{\times \alpha_1} \dots p^{d \times \alpha_d}$. As $\alpha_0 + \alpha_1 + \dots + \alpha_d = j$, there exist natural integers $\beta_0, \beta_1, \dots, \beta_d$ such that $0 \leq \beta_\nu \leq \alpha_\nu$ for each index $\nu \in \{0, \dots, d\}$ and satisfying the relation $\beta_0 + \dots + \beta_d = i$. The number $l = |1^{\times \beta_0} p^{\times \beta_1} \dots p^{d \times \beta_d}|$ answers our problem.

Multinomial coefficient

Let \mathbf{a} be a multi-integer of length j . The *multinomial coefficient* of the multi-integer \mathbf{a} is the natural integer $\mathfrak{M}(\mathbf{a})$ defined by :

$$\mathfrak{M}(\mathbf{a}) = \binom{a_1 + a_2 + \dots + a_j}{a_1, a_2, \dots, a_j} = \frac{|\mathbf{a}|!}{\mathbf{a}!}. \quad (7)$$

Lemma 2.3 *Let $\mathbf{a} = (a_1, a_2, \dots, a_j)$ and $\mathbf{a}' = (a_{j+1}, a_{j+2}, \dots, a_q)$ two multi-integers, then*

$$\mathfrak{M}(\mathbf{a}\mathbf{a}') = \binom{|\mathbf{a}| + |\mathbf{a}'|}{|\mathbf{a}|} \mathfrak{M}(\mathbf{a}) \mathfrak{M}(\mathbf{a}'). \quad (8)$$

Proof. By formula (7), we have the following equality :

$$\mathfrak{M}(\mathbf{a}\mathbf{a}') = \frac{|\mathbf{a}\mathbf{a}'|!}{(\mathbf{a}\mathbf{a}')!};$$

as $\mathbf{a}\mathbf{a}'$ is the concatenation product of words \mathbf{a} and \mathbf{a}' , we have :

$$|\mathbf{a}\mathbf{a}'| = |\mathbf{a}| + |\mathbf{a}'| \quad \text{and} \quad (\mathbf{a}\mathbf{a}')! = \mathbf{a}!\mathbf{a}'!,$$

from which formula (8) follows.

Action of symmetric group

Let S_j be the symmetric group on j symbols. We let S_j act on \mathbb{N}^j in a natural way, defining $\sigma\mathbf{a}$ for each $(\sigma, \mathbf{a}) \in S_j \times \mathbb{N}^j$ as $\sigma\mathbf{a} = (a_{\sigma^{-1}(1)}, a_{\sigma^{-1}(2)}, \dots, a_{\sigma^{-1}(j)})$ or in an equivalent way $(\sigma\mathbf{a})_\nu = a_{\sigma^{-1}(\nu)}$. It is obvious that $(\sigma\tau)\mathbf{a} = \sigma(\tau\mathbf{a})$.

Remark 2.4 *The multinomial coefficient $\mathfrak{M}(\mathbf{a})$ of a multi-integer \mathbf{a} is invariant by the symmetric group S_j , in the sense that for every permutation $\sigma \in S_j$ and for every multi-integer \mathbf{a} of length j , we have $\mathfrak{M}(\sigma\mathbf{a}) = \mathfrak{M}(\mathbf{a})$.*

Computation of multinomial coefficients modulo p

Lemma 2.5 *Let $\mathbf{a} = (a_1, a_2, \dots, a_j)$ be a multi-integer of length j such that at least p components are equal to the same power p^α of p . Then $\mathfrak{M}(\mathbf{a}) \equiv 0 \pmod{p}$.*

Proof. By hypothesis there exist p indices i_1, i_2, \dots, i_p in $\{1, 2, \dots, j\}$ such that for all $\nu \in \{1, 2, \dots, p\}$ we have :

$$a_{i_\nu} = p^\alpha.$$

By Remark 2.4, we can suppose that $i_1 = 1, i_2 = 2, \dots, i_p = p$. Now consider the multi-integer $\mathbf{b} = (p^\alpha)^{\times p}$ of length p . As $\mathbf{a} = \mathbf{b}\mathbf{c}$, where \mathbf{c} is a multi-integer of length $j - p$, Lemma 2.3 imply that it is sufficient to show $\mathfrak{M}(\mathbf{b}) \equiv 0 \pmod{p}$. Writing $\mathbf{b} = \mathbf{b}'\mathbf{b}''$, where $\mathbf{b}' = (p^\alpha)^{\times(p-1)}$ and $\mathbf{b}'' = (p^\alpha)^{\times 1}$, Lemma 2.3 gives

$$\mathfrak{M}(\mathbf{b}) = \binom{p^{\alpha+1}}{(p-1)p^\alpha} \mathfrak{M}(\mathbf{b}')\mathfrak{M}(\mathbf{b}'');$$

and lastly Lemma 1.11 yields

$$\binom{p^{\alpha+1}}{(p-1)p^\alpha} \equiv 0 \pmod{p},$$

hence the result.

Lemma 2.6 *Let $\mathbf{a} \in \mathbb{N}_{1 \times j, p}$ a multi-integer of length j , all the components of which are powers of p . Then $\mathfrak{M}(\mathbf{a}) \equiv \sharp \text{stab}(\mathbf{a}) \pmod{p}$, where $\sharp \text{stab}(\mathbf{a})$ is the order of the stabilizer $\text{stab}(\mathbf{a})$ of the multi-integer \mathbf{a} .*

Proof. Suppose that at least p components of \mathbf{a} are the same power of p . From Lemma 2.5 we infer that $\mathfrak{M}(\mathbf{a}) \equiv 0 \pmod{p}$. On the other hand $\#stab(\mathbf{a})$ contains at least the subgroup of S_j that permutes between them these p components ; thus $\#stab(\mathbf{a})$ is a multiple of $p!$, and then $\#stab(\mathbf{a}) \equiv 0 \pmod{p}$.

Therefore, we can suppose that each power of p appears at most $p-1$ times among the components of \mathbf{a} . At first, we tackle the case where $\mathbf{a} = (p^\alpha)^{\times j}$ with $j < p$. We proceed by induction on j . For $j = 1$, we have $\mathbf{a} = a_1 = p^\alpha$ and in this case, $\mathfrak{M}(\mathbf{a}) = 1 \equiv 1! \pmod{p}$. Suppose now that $\mathfrak{M}(p^{\alpha \times (j-1)}) \equiv (j-1)! \pmod{p}$. Let us set $\mathbf{a} = (p^\alpha)^{\times j}$ and compute $\mathfrak{M}(\mathbf{a})$:

$$\begin{aligned} \mathfrak{M}(\mathbf{a}) &= \mathfrak{M}((p^\alpha)^{\times j}) \\ &= \binom{j p^\alpha}{p^\alpha} \mathfrak{M}((p^\alpha)^{\times j-1}) \mathfrak{M}(p^\alpha) ; \end{aligned}$$

then using Lucas congruences [10, chapitre 23, page 418] results in

$$\mathfrak{M}((p^\alpha)^{\times j}) \equiv j(j-1)! \pmod{p} ,$$

that is to say

$$\mathfrak{M}((p^\alpha)^{\times j}) \equiv j! \pmod{p}. \tag{9}$$

We look now at the general case : we write, up to a permutation, letting unchanged $\mathfrak{M}(\mathbf{a})$, $\mathbf{a} = (p^{\alpha_1})^{\times j_1} \dots (p^{\alpha_h})^{\times j_h}$ where all the integers j_1, \dots, j_h are smaller than p . Then Lemma 2.3 allows to write :

$$\mathfrak{M}(\mathbf{a}) = \binom{j_1 p^{\alpha_1} + \dots + j_h p^{\alpha_h}}{j_1 p^{\alpha_1}} \mathfrak{M}[(p^{\alpha_1})^{\times j_1}] \mathfrak{M}[(p^{\alpha_2})^{\times j_2} \dots (p^{\alpha_h})^{\times j_h}] .$$

In this last formula, the binomial coefficient is $\equiv 1 \pmod{p}$ by Lucas congruences, and then we obtain :

$$\mathfrak{M}(\mathbf{a}) \equiv \mathfrak{M}[(p^{\alpha_1})^{\times j_1}] \mathfrak{M}[(p^{\alpha_2})^{\times j_2} \dots (p^{\alpha_h})^{\times j_h}] \pmod{p} ;$$

using an easy induction and formula (9) :

$$\mathfrak{M}(\mathbf{a}) \equiv j_1! \dots j_h! \pmod{p} ;$$

as $j_1! \dots j_h!$ is nothing but $\#stab(\mathbf{a})$ we deduce that :

$$\mathfrak{M}(\mathbf{a}) \equiv \#stab(\mathbf{a}) \pmod{p} .$$

2.2 Partitions

The multinomial coefficient of a partition

Let j be an integer ≥ 1 . We recall that a *partition* λ of an integer $n \in \mathbb{N}$ into j summands can be seen [3, chapitre II] as a non-increasing solution $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_j \geq 1$ in non-zero natural integers (called summands of the partition) of the equation :

$$\lambda_1 + \lambda_2 + \dots + \lambda_j = n ,$$

or as a solution in integers $a_i \geq 0$ (number of summands equal to i) of the system :

$$\begin{cases} a_1 + 2a_2 + \dots + na_n = n \\ a_1 + a_2 + \dots + a_n = j \end{cases} .$$

This second aspect allows to associate with a partition λ , the multi-integer of degree n defined as $1^{\times a_1} 2^{\times a_2} \dots n^{\times a_n}$. Thus the set of partitions of the integer n into j summands is identified to the set of orbits under the action of S_j of multi-integers of length j and degree n . We take advantage of this to define the *multinomial coefficient* of a partition $\lambda = (a_1, a_2, \dots, a_n)$ of n into j summands as $\mathfrak{M}(1^{\times a_1} 2^{\times a_2} \dots n^{\times a_n})$, that is $\mathfrak{M}(\lambda) = \frac{n!}{(1!)^{a_1} (2!)^{a_2} \dots (n!)^{a_n}}$.

A variant of multinomial coefficients

Let λ be a partition $(1^{a_1} 2^{a_2} \dots n^{a_n})$ of the integer n . We associate with λ a modified multinomial coefficient, that is the rational number $((\lambda)) = \frac{n!}{(1!)^{a_1} (2!)^{a_2} \dots (n!)^{a_n} a_1! a_2! \dots a_n!}$.

Lemma 2.7 *If λ is a partition of n , then the element $((\lambda))$ is an integer.*

This result was proved by Weill in 1880 [6, chapter 26, page 266]. The number $((\lambda))$ is called Faà di Bruno coefficient in [7].

A lemma

Let \mathbf{a} be a multi-integer of length j and n a non-zero natural integer. We suppose that $\mathbf{a} \neq 0^{\times j}$. We designate by $\mathbb{N}_{\mathbf{a}, p, n}$ the set of multi-integers in $\mathbb{N}_{\mathbf{a}, p}$ of degree equal to n . Let $Part_{\mathbf{a}}(n)$ denote the set of partitions of n into at most j summands (identified to non-increasing sequences of natural integers $y_1 \geq y_2 \geq \dots \geq y_j \geq 0$ such that $y_1 + y_2 + \dots + y_j = n$) satisfying the condition

$$\forall \nu \in \{1, \dots, j\} \quad s_p(y_\nu) = a_\nu.$$

Definition 2.8 *Let $\mathbf{a} \neq 0^{\times j}$ be an element of \mathbb{N}^j and $(\sigma, \lambda) \in \coprod_{\sigma \in S_j} Part_{\sigma \mathbf{a}}(n)$ that is an ordered pair (σ, λ) where $\sigma \in S_j$ and $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_j)$ is a non-increasing sequence of j natural integers such that $s_p(\lambda_\nu) = a_{\sigma^{-1}(\nu)}$ for every index $\nu \in \{1, \dots, j\}$ and $\lambda_1 + \lambda_2 + \dots + \lambda_j = n$. We set :*

$$\kappa(\sigma, \lambda) = (\lambda_{\sigma(1)}, \lambda_{\sigma(2)}, \dots, \lambda_{\sigma(j)}). \quad (10)$$

Lemma 2.9 *The equality (10) defines a map κ from the set $\coprod_{\sigma \in S_j} Part_{\sigma \mathbf{a}}(n)$ to $\mathbb{N}_{\mathbf{a}, p, n}$. For $\mathbf{z} \in \mathbb{N}_{\mathbf{a}, p, n}$, the cardinality of $\kappa^{-1}(\mathbf{z})$ is given by*

$$\text{card } \kappa^{-1}(\mathbf{z}) = \mathbf{b}! = \prod_{i=0}^n b_i!$$

where $b_i = \text{card } \{\nu \in \{1, \dots, j\} / z_\nu = i\}$. In particular, κ is surjective.

Proof. As $s_p(\lambda_\nu) = a_{\sigma^{-1}(\nu)}$, that is $s_p(\lambda_{\sigma(\nu)}) = a_\nu$, the multi-integer $\kappa(\sigma, \lambda)$ indeed belongs to $\mathbb{N}_{\mathbf{a}, p}$; moreover, since *ex hypothesi* $\lambda_1 + \lambda_2 + \dots + \lambda_j = n$, the sum $\lambda_{\sigma(1)} +$

$\lambda_{\sigma(2)} + \dots + \lambda_{\sigma(j)}$ is equal to n , so that κ defines a map from the set $\coprod_{\sigma \in S_j} Part_{\sigma a}(n)$ to the set $\mathbb{N}_{a,p,n}$.

For $\mathbf{z} \in \mathbb{N}_{a,p,n}$, we write $\mathbf{z} = (z_1, z_2, \dots, z_j)$; there obviously exists a permutation σ such that the sequence $\sigma \mathbf{z}$ is non-increasing. Set then $\lambda_\nu = z_{\sigma^{-1}(\nu)}$ for each index $\nu \in \{1, \dots, j\}$. It is readily verified that λ belongs to the set $Part_{\sigma a}(n)$. Thus (σ, λ) belongs to the set $\coprod_{\sigma \in S_j} Part_{\sigma a}(n)$ and its image by κ is \mathbf{z} . This shows already that the map κ is surjective.

Suppose now that two elements (σ, λ) and (σ', λ') in $\coprod_{\sigma \in S_j} Part_{\sigma a}(n)$ have the same image \mathbf{z} by κ . Since λ and λ' are non-increasing, necessarily $\lambda = \lambda'$. From this we infer that $\sigma \sigma'^{-1}$ belongs to the stabilizer under the action of the group S_j of the multi-integer \mathbf{z} . Therefore the set of antecedents of \mathbf{z} by the map κ is in bijection with the stabilizer of \mathbf{z} . Thus the result.

3 The binomial coalgebra

3.1 Definition

Here is the definition of the main subject of our paper [7, page 9].

Definition 3.1 *Let R be a commutative ring. The binomial R -coalgebra is defined as the triple $(\mathcal{B}_1, \Delta, \varepsilon)$ where :*

-the R -module \mathcal{B}_1 is the free R -module with denumerable basis $(e_n)_{n \in \mathbb{N}}$;

-the comultiplication Δ is the R -linear map from \mathcal{B}_1 to $\mathcal{B}_1 \otimes_R \mathcal{B}_1$ such that :

$$\Delta(e_n) = \sum_{k=0}^n \binom{n}{k} e_k \otimes e_{n-k} .$$

-the counit is the R -linear map $\varepsilon : \mathcal{B}_1 \longrightarrow R$ such that :

$$\varepsilon(e_n) = \begin{cases} 0 & \text{if } n \neq 0 \\ 1 & \text{if } n = 0 \end{cases} .$$

In the case where R is a ring the characteristic of which is a prime number p , since by definition $k \prec n$ is equivalent to $\binom{n}{k} \not\equiv 0 \pmod{p}$, the comultiplication Δ can be expressed by :

$$\Delta(e_n) = \sum_{k \prec n} \binom{n}{k} e_k \otimes e_{n-k} . \tag{11}$$

Remark 3.2 The coalgebra \mathcal{B}_1 can be provided with a filtered structure. Indeed by setting $C_0 = Re_0$, $C_1 = Re_0 + Re_1, \dots$, $C_j = Re_0 + Re_1 + \dots + Re_j, \dots$ we get a non-decreasing filtration of the R -module \mathcal{B}_1 by sub-coalgebras C_n , with $\bigcup_{n \in \mathbb{N}} C_n = \mathcal{B}_1$. We say that \mathcal{B}_1 is a filtered R -coalgebra ; this allows to define the degree $\deg(b)$ of an element b of \mathcal{B}_1 by setting $\deg(b) = \min\{k \in \mathbb{N}; b \in C_k\}$.

We denote by HR the Hurwitz algebra defined by Keigher in [8] provided with its natural topology [9, page 293]. Let provide the dual algebra \mathcal{B}_1^* of the coalgebra \mathcal{B}_1 with

the weak topology, which by definition is the weakest topology that makes continuous the maps $i_b : \mathcal{B}_1^* \rightarrow R$ defined by $i_b(b^*) = \langle b^*, b \rangle$ for each $b \in \mathcal{B}_1$, R being provided with the discrete topology.

Lemma 3.3 *The map :*

$$\Omega : \mathcal{B}_1^* \rightarrow HR$$

that with an element b^ in \mathcal{B}_1^* associates the element $\Omega(b^*) = (b^*(e_n))_n$ is an isomorphism of topological algebras.*

Proof. It is clear that Ω is a bijection, because we can immediately explicit Ω^{-1} . Indeed, it is defined as the map from HR to \mathcal{B}_1^* that with an element $(a_n)_n$ of HR associates the element b^* of \mathcal{B}_1^* such that $\langle b^*, e_n \rangle = a_n$. One easily proves that Ω is a morphism of algebras. Lastly, we have to prove that Ω and Ω^{-1} are continuous. For this, we observe that \mathcal{B}_1^* is provided with the weak topology, which is the weakest topology that makes continuous the maps $i_b : \mathcal{B}_1^* \rightarrow R$, and that HR is provided with its natural topology as defined by [9, page 293], that is the weakest topology that makes continuous for all $n \in \mathbb{N}$ the maps $\pi_n : HR \rightarrow R$. (Recall that π_n is defined by [9] as the map that sends a formal Hurwitz series $(a_n)_n$ to a_n). Therefore it is sufficient to prove that the maps $\pi_n \circ \Omega : \mathcal{B}_1^* \rightarrow R$ and $i_b \circ \Omega^{-1} : HR \rightarrow R$ are continuous for all natural integers n and for all elements b in \mathcal{B}_1 . We observe that $\pi_n \circ \Omega = i_{e_n}$ which is continuous on \mathcal{B}_1^* , and we also remark that $i_b \circ \Omega^{-1}$ is a locally constant map, hence a continuous map, so Ω and Ω^{-1} are continuous, which ends the proof of Lemma 3.3.

By Lemma 3.3, we can build continuous endomorphisms of the algebra HR by transposition of coalgebra endomorphisms of \mathcal{B}_1 . When R is a field of characteristic zero, we know that HR is topologically isomorphic to the algebra $R[[t]]$ of univariate power series with coefficients in R and that every continuous endomorphism of this algebra can be described as a composition on the right by a fixed series without constant term. This description of coalgebra endomorphisms explains the link between polynomial sequences of binomial type and formal power series that lies at the core of umbral calculus. Now our objective is to describe the coalgebra maps of \mathcal{B}_1 in positive characteristic. In the sequel we intend, at least in the case where R is a reduced ring, to determine the group-like elements of the binomial coalgebra and to study the coradical filtration of this coalgebra.

3.2 Group-like elements

Recall the definition of *group-like* elements of a coalgebra as given in [11, page 57].

Definition 3.4 *We call x a group-like element of a R -coalgebra (C, Δ, ε) , when x is an element of C satisfying the relation :*

$$\Delta(x) = x \otimes x.$$

Proposition 3.5 *Let R be a reduced ring. The group-like elements of the binomial coalgebra \mathcal{B}_1 are exactly these of the form re_0 , where r is an idempotent of R .*

Proof. It is clear that elements of \mathcal{B}_1 of the form re_0 , with $r^2 = r$, are group-like. Examine the reciprocal : let $x = \sum_{i=0}^N r_i e_i$ a group-like with $r_N \neq 0$, let us show that

$r_1 = r_2 = \dots = r_N = 0$ and $r_0^2 = r_0$. As x is group-like, the equality $\Delta(x) = x \otimes x$ is true. On the one hand we can compute :

$$\Delta(x) = \sum_{i=0}^N \sum_{j=0}^i r_i \binom{i}{j} e_j \otimes e_{i-j}$$

and on the other hand

$$x \otimes x = \sum_{i=0}^N \sum_{j=0}^N r_i r_j e_i \otimes e_j.$$

By identification, we get that for each ordered pair (i, j) of integers such that $i + j \leq N$ the equality :

$$r_i r_j = r_{i+j} \binom{i+j}{i}$$

is true, and that if $i + j > N$ then $r_i r_j = 0$. We see that for $i = j = 0$ $r_0^2 = r_0$ and consequently r_0 is idempotent. When $N \neq 0$, by putting $i = j = N$, this gives $r_N^2 = 0$ which imply inevitably that r_N is zero because R is a reduced ring. Hence the result.

Remark 3.6 For all element r of R , the element $e_0 + r e_1$ is group-like if and only if $r^2 = 0$. Thus previous proposition is no longer valid when R is not reduced.

3.3 The coradical filtration

Definition 3.7 We define by induction a sequence $(E_k)_{k \in \mathbb{N}}$ of submodules of \mathcal{B}_1 by setting $E_0 = R e_0$ and, for every integer $k \geq 1$

$$E_k = \ker((\pi_{k-1} \otimes \pi_0) \circ \Delta)$$

where, for each natural integer j , π_j is the canonical surjection from \mathcal{B}_1 to \mathcal{B}_1/E_j .

Remark 3.8 In the case where R is a field, E_k is the $(k+1)$ -th power of E_0 for the “wedge” operation defined by [11, page 179]. $(E_k)_{k \in \mathbb{N}}$ is the coradical filtration defined by [11, page 185].

As a first step in our investigation of the coalgebra \mathcal{B}_1 , we have to determine the submodules E_k . This will be made under the supplementary assumption that R has characteristic p , a prime number.

Let \mathcal{P}_j be the R -submodule of \mathcal{B}_1 spanned by the subset $\{e_n; n \in \mathbb{N}_{j,p}\}$. The data of $(\mathcal{P}_j)_{j \in \mathbb{N}}$ is a grading of type \mathbb{N} on \mathcal{B}_1 . We shall show that the filtration canonically associated with this grading is nothing but the coradical filtration. In other words, we have the following.

Proposition 3.9 If R is a ring of characteristic the prime number $p > 0$, then :

$$E_k = \bigoplus_{j=0}^k \mathcal{P}_j .$$

Proof. We proceed by induction on the natural integer k . When $k = 0$, it obvious that $\mathcal{P}_0 = Re_0 = E_0$. Let us suppose that $E_{k-1} = \bigoplus_{j=0}^{k-1} \mathcal{P}_j$ and infer from this that $E_k = \bigoplus_{j=0}^k \mathcal{P}_j$.

To prove the inclusion $E_k \supseteq \bigoplus_{j=0}^k \mathcal{P}_j$, it is sufficient to show that e_m belongs to E_k as soon as $s_p(m) \leq k$. Accordingly we fix a natural integer m such that $s_p(m) \leq k$; let us show that $\Delta(e_m)$ belongs to the kernel of $\pi_{k-1} \otimes \pi_0$. By formula (11), we have :

$$(\pi_{k-1} \otimes \pi_0)\Delta(e_m) = \sum_{l < m} \binom{m}{l} \pi_{k-1}(e_l) \otimes \pi_0(e_{m-l}).$$

By our induction hypothesis, it is known that $\pi_{k-1}(e_l) = 0$ when $s_p(l) < k$. Moreover we have $\pi_0(e_0) = 0$. So we can write :

$$(\pi_{k-1} \otimes \pi_0)\Delta(e_m) = \sum_{l < m, l \neq m, s_p(l) \geq k} \binom{m}{l} \pi_{k-1}(e_l) \otimes \pi_0(e_{m-l}).$$

This last sum is restricted to indices l such that $s_p(l) \geq k$. On the other hand *ex hypothesis* $s_p(m) \leq k$, hence $s_p(l) \geq s_p(m)$. Then Lemma 1.13 imply that $m \not\equiv l \pmod{p}$. Therefore $(\pi_{k-1} \otimes \pi_0)\Delta(e_m) = 0$, and this means that e_m indeed belongs to the kernel of $(\pi_{k-1} \otimes \pi_0) \circ \Delta$, as to be shown.

In order to show the reciprocal inclusion $E_k \subseteq \bigoplus_{j=0}^k \mathcal{P}_j$, let us fix an element y in E_k . As $(e_n)_{n \in \mathbb{N}}$ is a basis of the R -module \mathcal{B}_1 , we can write $y = \sum_{n=0}^d r_n e_n$ where $r_n \in R$ for each integer n , so that :

$$\Delta(y) = \sum_{n=0}^d r_n \sum_{l < n} \binom{n}{l} e_l \otimes e_{n-l}. \quad (12)$$

Applying the map $(\pi_{k-1} \otimes \pi_0)$ to the two sides of the preceding equality (12) and using the fact that $y \in E_k$, we obtain :

$$0 = (\pi_{k-1} \otimes \pi_0)\Delta(y) = \sum_{n=0}^d r_n \sum_{l < n, l \neq n, s_p(l) \geq k} \binom{n}{l} \pi_{k-1}(e_l) \otimes \pi_0(e_{n-l}). \quad (13)$$

Let F_{k-1} be the R -submodule of \mathcal{B}_1 spanned by the elements e_n , where $n \notin \mathbb{N}_{0,p} \cup \mathbb{N}_{1,p} \cup \dots \cup \mathbb{N}_{k-1,p}$. By our induction hypothesis $E_{k-1} = \bigoplus_{j=0}^{k-1} \mathcal{P}_j$, we know that the submodules E_{k-1} and F_{k-1} of \mathcal{B}_1 are supplementary. Thus the restriction of π_{k-1} to F_{k-1} is an isomorphism from F_{k-1} on \mathcal{B}_1/E_{k-1} . Then we can define a morphism

$$\phi_{k-1} : \mathcal{B}_1/E_{k-1} \longrightarrow \mathcal{B}_1$$

as the composition of the natural injection from F_{k-1} to \mathcal{B}_1 with $(\pi_{k-1} |_{F_{k-1}})^{-1}$. In the same way, we define $\phi_0 : \mathcal{B}_1/E_0 \longrightarrow \mathcal{B}_1$ as the composition of the natural injection from F_0 to \mathcal{B}_1 with $(\pi_0 |_{F_0})^{-1}$. Then we can apply $\phi_{k-1} \otimes \phi_0$ to the two sides of the equality (13), getting :

$$\sum_{n=0}^d \sum_{l < n, s_p(l) \geq k, l \neq n} \binom{n}{l} r_n e_l \otimes e_{n-l} = 0.$$

As the subset $\{e_l \otimes e_m : (l, m) \in \mathbb{N}^2\}$ of $\mathcal{B}_1 \otimes \mathcal{B}_1$ is R -linearly independent, we see that, for every $n \in \{0, \dots, d\}$ and for every $l \prec n$ such that $l \neq n$, the relation $s_p(l) \geq k$ imply that $\binom{n}{l} r_n = 0$. Let $n \in \{0, \dots, d\}$ be such that $s_p(n) > k > 0$, Lemma 1.14 shows the existence of a natural integer l with $l \prec n$ and $s_p(l) = s_p(n) - 1$, so that $\binom{n}{l}$ is coprime to p and therefore $r_n = 0$ for each n such that $s_p(n) > k$. Thus y indeed belongs to $\bigoplus_{j=0}^k \mathcal{P}_j$.

Observe that, since E_k is a free R -module, $E_k \otimes E_k$ is identified with a submodule of $\mathcal{B}_1 \otimes \mathcal{B}_1$.

Corollary 3.10 *The R -module E_k is a direct summand of \mathcal{B}_1 . Moreover E_k is a subcoalgebra of \mathcal{B}_1 , in the sense that $\Delta(E_k) \subseteq E_k \otimes E_k$.*

Proof. The module E_k has a basis formed by elements (e_n) where n describe the set $\bigcup_{j=0}^k \mathbb{N}_{j,p}$. It is sufficient to show that, for such an integer n , $\Delta(e_n)$ belongs to $E_k \otimes E_k$. Thus let n be a natural integer such that $s_p(n) \leq k$. By Lemma 1.13, if $s_p(l) > s_p(n)$ then $l \not\prec n$. So if $l \prec n$, then $s_p(l) \leq s_p(n)$ and therefore $e_l \in E_k$. As $\binom{n}{n-l} = \binom{n}{l}$, we observe that $l \prec n$ if and only if $n-l \prec n$. So when $l \prec n$ we have, in the same way as before, $e_{n-l} \in E_k$. By the equality (11), this proves the wanted inclusion $\Delta(E_k) \subseteq E_k \otimes E_k$.

Lemma 3.11 *For each integer $k \geq 1$, we have*

$$E_k = \Delta^{-1}(E_{k-1} \otimes \mathcal{B}_1 + \mathcal{B}_1 \otimes E_0).$$

Proof. This is a straightforward consequence of the fact that E_{k-1} and E_0 are direct summands of \mathcal{B}_1 .

Proposition 3.12 *Let R be a reduced ring of characteristic equal to p . Then the submodule E_k is stable by every endomorphism ϕ of the coalgebra \mathcal{B}_1 .*

Proof. Let ϕ be an endomorphism of the coalgebra \mathcal{B}_1 . Let us prove by induction on k that $\phi(E_k) \subseteq E_k$. For $k = 0$, by Proposition 3.5 we have $\phi(e_0) = r e_0$ with r an idempotent of R , so that $\phi(E_0) \subseteq E_0$. Let us suppose now that $\phi(E_{k-1}) \subseteq E_{k-1}$ and let β be an element in E_k . By lemma 3.11, we have

$$\Delta \circ \phi(\beta) = (\phi \otimes \phi) \circ \Delta(\beta) \in (\phi \otimes \phi)(E_{k-1} \otimes \mathcal{B}_1 + \mathcal{B}_1 \otimes E_0) ;$$

hence the desired result $\phi(\beta) \in E_k$ by our induction hypothesis.

3.4 The components of the comultiplication

We provide \mathcal{B}_1 with its grading by the submodules \mathcal{P}_j , with $j \in \mathbb{N}$. Let ρ be the mapping from $\mathbb{N} \times \mathbb{N}$ to \mathbb{N} such that $\rho(\mu, \nu) = \mu + \nu$. We remark that Δ is ρ -graded from \mathcal{B}_1 to $\mathcal{B}_1 \otimes \mathcal{B}_1$; indeed, by formula (11), we have $\Delta(\mathcal{P}_j) \subseteq \bigoplus_{\rho(\mu, \nu)=j} \mathcal{P}_\mu \otimes \mathcal{P}_\nu$. As seen in section 1, we have then

$$\Delta = \sum_{\mu, \nu \geq 0} (i_\mu \otimes i_\nu) \circ \Delta_{\mu, \nu} \circ \text{pr}^{\mu+\nu} ,$$

where

$$\Delta_{\mu, \nu} = (\text{pr}^\mu \otimes \text{pr}^\nu) \circ \Delta \circ i_{\mu+\nu}.$$

Lemma 3.13 *The map $\Delta_{l,m}$ from \mathcal{P}_{l+m} to $\mathcal{P}_l \otimes \mathcal{P}_m$ is injective.*

Proof. In order to show that $\Delta_{l,m}$ is injective, it is sufficient to find a R -linear map $f_{l,m}$ from $\mathcal{P}_l \otimes \mathcal{P}_m$ to \mathcal{P}_{l+m} such that $f_{l,m} \circ \Delta_{l,m} = I_{\mathcal{P}_{l+m}}$. Such an application is determined in a unique way by the images of the elements $e_\mu \otimes e_\nu$ where $(\mu, \nu) \in \mathbb{N}_{l,p} \times \mathbb{N}_{m,p}$. Indeed these elements make up a basis for the submodule $\mathcal{P}_l \otimes \mathcal{P}_m$ of $\mathcal{B}_1 \otimes \mathcal{B}_1$.

For a natural integer $n \in \mathbb{N}_{l+m,p}$, we build the set D_n of natural integers defined as :

$$D_n = \{j \in \mathbb{N}_{l,p} ; j \prec n\}.$$

By Lemma 2.2, the set D_n is non-empty. We set $d(n) = \min D_n$. Let (μ, ν) be an element of $\mathbb{N}_{l,p} \times \mathbb{N}_{m,p}$. We put :

$$f_{l,m}(e_\mu \otimes e_\nu) = \begin{cases} 0 & \text{if } \binom{\mu+\nu}{\mu} \equiv 0 \pmod{p} (\Leftrightarrow \mu \not\prec \mu + \nu) \\ 0 & \text{if } \mu \prec \mu + \nu \text{ and if } \mu \neq d(\mu + \nu) \\ \binom{\mu+\nu}{\mu}^{-1} e_{\mu+\nu} & \text{if } \mu = d(\mu + \nu) \prec \mu + \nu \end{cases}$$

Let us verify that $f_{l,m} \circ \Delta_{l,m} = I_{\mathcal{P}_{l+m}}$. For $n \in \mathbb{N}_{l+m,p}$, we compute :

$$\Delta_{l,m}(e_n) = \sum_{(j,k) \in \mathbb{N}_{l,p} \times \mathbb{N}_{m,p}, j+k=n} \binom{n}{j} e_j \otimes e_k.$$

Hence

$$\begin{aligned} f_{l,m} \circ \Delta_{l,m}(e_n) &= \sum_{(j,k) \in \mathbb{N}_{l,p} \times \mathbb{N}_{m,p}, j+k=n} \binom{n}{j} f_{l,m}(e_j \otimes e_k) \\ &= \binom{n}{d(n)} \binom{n}{d(n)}^{-1} e_n \\ &= e_n. \end{aligned}$$

Indeed, on the one hand $f_{l,m}(e_j \otimes e_k)$ is zero except for $j = d(n)$, and on the other hand the ordered pair $(d(n), n - d(n))$ belongs to the set $\{(j, k) \in \mathbb{N}_{l,p} \times \mathbb{N}_{m,p}, j + k = n\}$. In this way we see that $\Delta_{l,m}$ is an injective map.

3.5 The components of a coalgebra endomorphism

We denote by ϕ_ν^μ the (ν, μ) -component of ϕ (see Definition 1.2). As in Section 1, for each endomorphism ϕ of the R -module \mathcal{B}_1 , we have :

$$\phi = \sum_{\mu, \nu \geq 0} i_\mu \circ \phi_\nu^\mu \circ \text{pr}^\nu.$$

Proposition 3.14 *Let ϕ be an endomorphism of the R -module \mathcal{B}_1 . The identity $\Delta \circ \phi = (\phi \otimes \phi) \circ \Delta$ is true if and only if, for every natural integers l, m, ρ , we have the following equality :*

$$\Delta_{l,m} \circ \phi_\rho^{l+m} = \sum_{\mu+\nu=\rho} (\phi_\mu^l \otimes \phi_\nu^m) \circ \Delta_{\mu,\nu}.$$

Proof. Firstly we remark that the data of the submodules \mathcal{P}_μ provide the R -module \mathcal{B}_1 with a grading of type \mathbb{N} and consequently $\mathcal{B}_1 \otimes \mathcal{B}_1$ with a grading of type $\mathbb{N} \times \mathbb{N}$. Let us compute the $(\gamma, (l, m))$ -component of $\Delta \circ \phi$. By Proposition 1.4, for γ and (l, m) fixed respectively in \mathbb{N} and $\mathbb{N} \times \mathbb{N}$, we have :

$$(\Delta \circ \phi)_\gamma^{(l, m)} = \sum_{\delta \in \mathbb{N}} \Delta_\delta^{(l, m)} \circ \phi_\gamma^\delta. \quad (14)$$

It is known that Δ is ρ -graded, where ρ is the map from $\mathbb{N} \times \mathbb{N}$ to \mathbb{N} such that $\rho(l, m) = l + m$. Thus $\Delta_\delta^{(l, m)} = 0$ when $\delta \neq l + m$. Therefore the sum in the right-hand side of formula (14) is restricted to a single term with $\delta = l + m$, hence :

$$(\Delta \circ \phi)_\gamma^{(l, m)} = \Delta_{l+m}^{(l, m)} \circ \phi_\gamma^{l+m}.$$

But, as we let $\Delta_{l, m}$ denote $\Delta_{l+m}^{(l, m)}$, the $(\gamma, (l, m))$ -component of $\Delta \circ \phi$ is :

$$(\Delta \circ \phi)_\gamma^{(l, m)} = \Delta_{l, m} \circ \phi_\gamma^{l+m}.$$

Now let us compute the $(\gamma, (l, m))$ -component of $(\phi \otimes \phi) \circ \Delta$. By Proposition 1.4, for γ and (l, m) fixed respectively in \mathbb{N} and $\mathbb{N} \times \mathbb{N}$, we have :

$$[(\phi \otimes \phi) \circ \Delta]_\gamma^{(l, m)} = \sum_{(\mu, \nu) \in \mathbb{N} \times \mathbb{N}} (\phi \otimes \phi)_{(\mu, \nu)}^{(l, m)} \circ \Delta_\gamma^{(\mu, \nu)}. \quad (15)$$

As \mathcal{B}_1 is free as a R -module, it is flat and consequently $\mathcal{B}_1 \otimes \mathcal{B}_1$ is flat. So Proposition 1.6 allows to write :

$$(\phi \otimes \phi)_{(\mu, \nu)}^{(l, m)} = \phi_\mu^l \otimes \phi_\nu^m.$$

Substituting this equality in formula (15), we get :

$$[(\phi \otimes \phi) \circ \Delta]_\gamma^{(l, m)} = \sum_{(\mu, \nu) \in \mathbb{N} \times \mathbb{N}} (\phi_\mu^l \otimes \phi_\nu^m) \circ \Delta_\gamma^{(\mu, \nu)}. \quad (16)$$

As Δ is ρ -graded, we have $\Delta_\gamma^{(\mu, \nu)} = 0$ if $\mu + \nu \neq \gamma$ and therefore the sum in the right-hand side of formula (16) is restricted to a sum of terms such that $\mu + \nu = \gamma$; hence the $(\gamma, (l, m))$ -component of $(\phi \otimes \phi) \circ \Delta$ is :

$$[(\phi \otimes \phi) \circ \Delta]_\gamma^{(l, m)} = \sum_{\mu + \nu = \gamma} (\phi_\mu^l \otimes \phi_\nu^m) \circ \Delta_{\mu, \nu}.$$

Lastly, remark 1.3 gives the wished equivalence.

Lemma 3.15 *Suppose that R is a reduced ring of characteristic p . Let ϕ be an endomorphism of the R -coalgebra \mathcal{B}_1 . The $(\mu, 0)$ -component and the $(0, \nu)$ -component of ϕ are zero for all non-zero natural integers μ and ν . The $(0, 0)$ -component of ϕ is nothing but $I_{\mathcal{P}_0}$.*

Proof. The map ϕ is an endomorphism of the R -coalgebra \mathcal{B}_1 , so that $\varepsilon \circ \phi = \varepsilon$. Provide R with its unique grading of type $\{0\}$. For μ a natural integer, let ε_μ denote the

$(\mu, 0)$ -component of ε . Let us compute the $(\mu, 0)$ -component of $\varepsilon \circ \phi$. By Proposition 1.4, we have :

$$(\varepsilon \circ \phi)_\mu^0 = \sum_{\nu \in \mathbb{N}} \varepsilon_\nu \circ \phi_\mu^\nu. \quad (17)$$

Now $\varepsilon_\mu = 0$ when $\mu \neq 0$. Therefore the sum, in the right-hand side of equality (17) is restricted to a single terme, hence :

$$(\varepsilon \circ \phi)_\mu^0 = \varepsilon_0 \circ \phi_\mu^0.$$

By Remark 1.3, we can write :

$$\varepsilon_\mu = \varepsilon_0 \circ \phi_\mu^0. \quad (18)$$

Moreover, it can be observed that ε_0 is the linear map from the rank 1 free R -module \mathcal{P}_0 to R that maps $e_0 \in \mathcal{P}_0$ to $1 \in R$. Therefore ε_0 is bijective. We are in one of the following cases :

If $\mu = 0$, the equality (18) gives $\varepsilon_0 = \varepsilon_0 \circ \phi_0^0$. As ε_0 is bijective, we deduce $\phi_0^0 = I_{\mathcal{P}_0}$.

If $\mu \neq 0$, the equality (18) becomes $0 = \varepsilon_0 \circ \phi_\mu^0$, so $\phi_\mu^0 = 0$ for $\mu > 0$.

Lastly Proposition 3.12 shows that for $\mu > \nu$ we have $\phi_\nu^\mu = 0$. Hence $\phi_0^\mu = 0$ for $\mu > 0$.

3.6 Characterization of coalgebra endomorphisms

We define the map Θ from the set of R -coalgebra endomorphisms of \mathcal{B}_1 to the product $\prod_{j \geq 1} \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$ by the formula :

$$\Theta(\phi) = (\phi_j^1)_{j \geq 1}. \quad (19)$$

The following theorem shows that ϕ is completely characterized by $\Theta(\phi)$.

Theorem 3.16 *If R is a reduced ring of characteristic p , then the map Θ defined by (19) is injective.*

Proof. Let ϕ and ϕ' two endomorphisms of the R -coalgebra \mathcal{B}_1 such that $\Theta(\phi) = \Theta(\phi')$. We have only to verify that the (μ, ν) -components ϕ_ν^μ and ϕ'_ν^μ agree for all natural integers μ and ν . We prove this by induction on μ . Lemma 3.15 shows that this is true for $\mu = 0$. Fix now a natural integer $\mu \geq 0$ and suppose that $\phi_\nu^\mu = \phi'_\nu^\mu$ for all $\nu \geq 0$; let us show that $\phi_\nu^{\mu+1} = \phi'_\nu^{\mu+1}$ for all $\nu \geq 0$. By Proposition 3.14, we have :

$$\begin{aligned} \Delta_{\mu,1} \circ \phi_\nu^{\mu+1} &= \sum_{\alpha+\beta=\nu} (\phi_\alpha^\mu \otimes \phi_\beta^1) \circ \Delta_{\alpha,\beta} \\ &= \sum_{\alpha+\beta=\nu} (\phi'_\alpha^\mu \otimes \phi'_\beta^1) \circ \Delta_{\alpha,\beta} \\ &= \Delta_{\mu,1} \circ \phi'_\nu^{\mu+1}. \end{aligned}$$

Now, by Lemma 3.13, the map $\Delta_{\mu,1}$ is injective, thus $\phi_\nu^{\mu+1} = \phi'_\nu^{\mu+1}$ for each natural integer ν , as to be shown.

As a matter of fact, we shall prove in the sequel the following result.

Theorem 3.17 *If R is a reduced ring of characteristic p , then the map Θ is bijective.*

In order to show this theorem, we need some preliminary results about coalgebras. This will be examined in the next Section.

4 Multi-integers and coalgebras

Throughout this section, the ground ring R is supposed to be a reduced ring of characteristic p .

4.1 Notations

Definition 4.1 *The diagonal map of order j is the R -linear map $\Delta^{(j)}$ of \mathcal{B}_1 to $\mathcal{B}_1^{\otimes j}$ defined by induction on j by setting :*

$\Delta^{(0)}$ is the counit ε of \mathcal{B}_1 , $\Delta^{(1)} = I_{\mathcal{B}_1}$ and $\Delta^{(j+1)} = (\Delta^{(j)} \otimes I_{\mathcal{B}_1}) \circ \Delta$ for each natural integer $j \geq 1$.

Remark 4.2 *As Δ is ρ -graded, we easily verify that the map $\Delta^{(j)}$ is ρ_j -graded where ρ_j is the map from \mathbb{N}^j to \mathbb{N} that sends a multi-integer \mathbf{a} of length j to the integer $|\mathbf{a}|$.*

For every multi-integer $\mathbf{a} = (a_1, \dots, a_j)$ of length j , we denote by $\mathcal{P}_{\mathbf{a}}$ the R -module $\otimes_{i=1}^j \mathcal{P}_{a_i}$ (denoted by $T_{\mathbf{a}}(P)$ in Section 1) so that we have $\mathcal{B}_1^{\otimes j} \simeq \bigoplus_{\mathbf{a} \in \mathbb{N}^j} \mathcal{P}_{\mathbf{a}}$. For a multi-integer \mathbf{a} of length j , we denote by $e_{\mathbf{a}}$ the tensor product $\otimes_{i=1}^j e_{a_i}$, by $i_{|\mathbf{a}|}$ the injection from $\mathcal{P}_{|\mathbf{a}|}$ to \mathcal{B}_1 , by $\text{pr}^{\mathbf{a}} = \otimes_{i=1}^j \text{pr}^{a_i}$ the projection from $\mathcal{B}_1^{\otimes j}$ to $\mathcal{P}_{\mathbf{a}}$.

4.2 The components of the diagonal map of order j

Let \mathbf{a} be a multi-integer of length j . Let $\Delta_{\mathbf{a}}^{(j)}$ denote the $(|\mathbf{a}|, \mathbf{a})$ -component of $\Delta^{(j)}$ that is :

$$\Delta_{\mathbf{a}}^{(j)} = \text{pr}^{\mathbf{a}} \circ \Delta^{(j)} \circ i_{|\mathbf{a}|}.$$

the map $\Delta_{\mathbf{a}}^{(j)}$ is a R -linear map from $\mathcal{P}_{|\mathbf{a}|}$ to $\mathcal{P}_{\mathbf{a}}$.

Proposition 4.3 *Let \mathbf{b} and \mathbf{c} be two multi-integers of length respectively i and j . We have the following formula :*

$$\Delta_{\mathbf{bc}}^{(i+j)} = (\Delta_{\mathbf{b}}^{(i)} \otimes \Delta_{\mathbf{c}}^{(j)}) \circ \Delta_{|\mathbf{b}|, |\mathbf{c}|}.$$

Proof. The coassociativity of Δ gives the following equality :

$$\Delta^{(i+j)} = (\Delta^{(i)} \otimes \Delta^{(j)}) \circ \Delta.$$

Fix two multi-integers \mathbf{b} and \mathbf{c} respectively in \mathbb{N}^i and \mathbb{N}^j . Considering $(|\mathbf{bc}|, \mathbf{bc})$ - components in the two sides of the preceding equality, Proposition 1.4 implies

$$\Delta_{\mathbf{bc}}^{(i+j)} = \sum_{(\mu, \nu) \in \mathbb{N} \times \mathbb{N}} (\Delta^{(i)} \otimes \Delta^{(j)})_{(\mu, \nu)}^{\mathbf{bc}} \circ \Delta_{|\mathbf{bc}|}^{(\mu, \nu)}. \quad (20)$$

Now Proposition 1.6 gives :

$$(\Delta^{(i)} \otimes \Delta^{(j)})_{(\mu, \nu)}^{\mathbf{bc}} = (\Delta^{(i)})_{\mu}^{\mathbf{b}} \otimes (\Delta^{(j)})_{\nu}^{\mathbf{c}};$$

by Remark 4.2, we have $(\Delta^{(i)})_{\mu}^b = 0$ if $\mu \neq |\mathbf{b}|$ and $(\Delta^{(j)})_{\nu}^c = 0$ if $\nu \neq |\mathbf{c}|$; moreover for $\mu = |\mathbf{b}|$ and $\nu = |\mathbf{c}|$, we have :

$$\begin{aligned} (\Delta^{(i)} \otimes \Delta^{(j)})_{(\mu,\nu)}^{bc} &= (\Delta^{(i)})_{|\mathbf{b}|}^b \otimes (\Delta^{(j)})_{|\mathbf{c}|}^c \\ &= \Delta_{\mathbf{b}}^{(i)} \otimes \Delta_{\mathbf{c}}^{(j)}. \end{aligned}$$

Substituting this last expression in equality (20), we get :

$$\Delta_{bc}^{(i+j)} = (\Delta_{\mathbf{b}}^{(i)} \otimes \Delta_{\mathbf{c}}^{(j)}) \circ \Delta_{|\mathbf{bc}|}^{|\mathbf{b}|,|\mathbf{c}|},$$

that is the desired identity.

The following lemma makes explicit the images by the map $\Delta_{\mathbf{a}}^{(j)}$ of the elements of the basis $(e_n)_{n \in \mathbb{N}_{|\mathbf{a}|,p}}$ of $\mathcal{P}_{|\mathbf{a}|}$.

Lemma 4.4 *Let \mathbf{a} be a multi-integer of length $j \geq 1$. For $n \in \mathbb{N}_{|\mathbf{a}|,p}$, we have :*

$$\Delta_{\mathbf{a}}^{(j)}(e_n) = \sum_{|\mathbf{k}|=n, \mathbf{k} \in \mathbb{N}_{\mathbf{a},p}} \mathfrak{M}(\mathbf{k}) e_{\mathbf{k}}.$$

Proof. This is straightforward by induction on j , by means of Proposition 4.3 and Lemma 2.3.

4.3 A map linked to the diagonal map of order j

Definition 4.5 *Let \mathbf{a} be a multi-integer of length j such that $\mathbf{a} \neq 0^{\times j}$. We define the map $\Gamma_{\mathbf{a}}^{(j)}$ of $\mathcal{P}_{|\mathbf{a}|}$ to $\mathcal{P}_{\mathbf{a}}$ such that, for $n \in \mathbb{N}_{|\mathbf{a}|,p}$*

$$\Gamma_{\mathbf{a}}^{(j)}(e_n) = \sum_{\lambda \in \text{Part}_{\mathbf{a}}(n)} ((\lambda)) e_{\lambda}; \quad (21)$$

where $e_{\lambda} = e_{\lambda_1} \otimes e_{\lambda_2} \otimes \dots \otimes e_{\lambda_j}$, if λ is the partition $n = \lambda_1 + \dots + \lambda_j$ with $\lambda_1 \geq \dots \geq \lambda_j \geq 1$.

Definition 4.6 *Let σ belongs to the set S_j . We define the map $\tau_{\sigma^{-1}, \mathbf{a}}$ from $\mathcal{P}_{\sigma \mathbf{a}}$ to $\mathcal{P}_{\mathbf{a}}$, that with an element $(b_1 \otimes b_2 \otimes \dots \otimes b_j) \in \mathcal{P}_{\sigma \mathbf{a}}$ associates the element $(b_{\sigma(1)} \otimes b_{\sigma(2)} \otimes \dots \otimes b_{\sigma(j)}) \in \mathcal{P}_{\mathbf{a}}$.*

Lemma 4.7 *Let \mathbf{a} and \mathbf{b} be two multi-integers of length j and j R -linear maps ψ_1, \dots, ψ_j such that ψ_i maps $\mathcal{P}_{\mathbf{a}_i}$ to $\mathcal{P}_{\mathbf{b}_i}$. Then we have*

$$\left[\bigotimes_{\nu=1}^j \psi_{\nu} \right] \circ \tau_{\sigma^{-1}, \mathbf{a}} = \tau_{\sigma^{-1}, \mathbf{b}} \circ \left[\bigotimes_{\nu=1}^j \psi_{\sigma^{-1}\nu} \right].$$

Proof. The proof is direct.

Lemma 4.8 *Let \mathbf{a} be a multi-integer of length j such that $\mathbf{a} \neq 0^{\times j}$ and $\tau_{\sigma^{-1}, \mathbf{a}}$ as in Definition 4.6. We have :*

$$\Delta_{\mathbf{a}}^{(j)} = \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, \mathbf{a}} \circ \Gamma_{\sigma \mathbf{a}}^{(j)}.$$

Proof. Let n be an element of $\mathbb{N}_{|a|,p}$; equality (21) and Definition 4.6 give :

$$\sum_{\sigma \in S_j} \tau_{\sigma^{-1},a} \circ \Gamma_{\sigma a}^{(j)}(e_n) = \sum_{\sigma \in S_j} \sum_{\lambda \in \text{Part}_{\sigma a}(n)} ((\lambda)) \tau_{\sigma^{-1},a}(e_\lambda).$$

A direct computation gives :

$$\tau_{\sigma^{-1},a}(e_\lambda) = e_{\sigma^{-1}(\lambda)}.$$

Now $\sigma^{-1}(\lambda)$ belongs to the set $\mathbb{N}_{a,p}$ and satisfies the equality $|\sigma^{-1}(\lambda)| = n$. Setting $\mathbf{k} = \kappa(\sigma, \lambda)$ - with the notation of Definition 2.8, we get :

$$\sum_{\sigma \in S_j} \tau_{\sigma^{-1},a} \circ \Gamma_{\sigma a}^{(j)}(e_n) = \sum_{k \in \mathbb{N}_{a,p,n}} \sum_{(\sigma, \lambda) \in \kappa^{-1}(k)} ((\lambda)) e_k.$$

It remains to prove that $\sum_{(\sigma, \lambda) \in \kappa^{-1}(k)} ((\lambda)) = \mathfrak{M}(\mathbf{k})$. By Lemma 2.9, we know that the cardinality of $\kappa^{-1}(\mathbf{k})$ is $\mathbf{a}!$ and then $\mathfrak{M}(\kappa(\sigma, \lambda)) = \mathbf{a}!((\lambda)) = \mathfrak{M}(\mathbf{k})$, hence the result by Lemma 4.4.

4.4 The map f_j

We set $f_0 = \varepsilon_0$. Given a natural integer $j \geq 1$, let f_j denote the map from \mathcal{P}_j to $\mathcal{P}_1^{\otimes j}$ defined by :

$$f_j = (f_{j-1} \otimes I_{\mathcal{P}_1}) \circ \Delta_{j-1,1}.$$

We can identify f_1 with $I_{\mathcal{P}_1}$ by means of the canonical isomorphism of $R \otimes \mathcal{P}_1$ with \mathcal{P}_1 .

Lemma 4.9 *The map f_j is injective.*

Proof. This follows easily by induction on j from the flatness of the R -module \mathcal{P}_1 and from Lemma 3.13.

Proposition 4.10 *The map f_j is equal to the $(j, 1^{\times j})$ -component of the diagonal map of order j , where $1^{\times j} = (1, 1, \dots, 1) \in \mathbb{N}^j$.*

Proof. We proceed by induction on the natural integer $j \geq 1$. For $j = 1$, we have $f_1 = I_{\mathcal{P}_1} = \Delta_{1^{\times 1}}^{(1)}$. Suppose now that $f_{j-1} = \Delta_{1^{\times j-1}}^{(j-1)}$ and let us prove that $f_j = \Delta_{1^{\times j}}^{(j)}$. By Proposition 4.3, we have by setting $\mathbf{b} = 1^{\times(j-1)}$ and $\mathbf{c} = 1^{\times 1}$, the following equality :

$$\Delta_{1^{\times j}}^{(j)} = (\Delta_{1^{\times j-1}}^{(j-1)} \otimes \Delta_{1^{\times 1}}^{(1)}) \circ \Delta_{j-1,1}. \quad (22)$$

But $f_{j-1} = \Delta_{1^{\times j-1}}^{(j-1)}$ (induction hypothesis) and $\Delta_{1^{\times 1}}^{(1)} = I_{\mathcal{P}_1}$, thus by substituting in equality (22), we have :

$$\Delta_{1^{\times j}}^{(j)} = (f_{j-1} \otimes I_{\mathcal{P}_1}) \circ \Delta_{j-1,1},$$

which is nothing but f_j .

Lemma 4.11 *Let n be a natural integer such that $s_p(n) = j$. We have :*

$$f_j(e_n) = \sum_{\sigma \in S_j} e_{\sigma a};$$

where \mathbf{a} is the multi-integer $\mathbf{a} = \omega(n)$ defined before Lemma 2.1.

Proof. Let us set $\mathbf{a} = \omega(n)$ we have then $|\mathbf{a}| = n$. By Proposition 4.10, $f_j(e_n) = \Delta_{1 \times j}^{(j)}(e_n)$ and Lemma 4.4 gives the following equality :

$$\Delta_{1 \times j}^{(j)}(e_n) = \sum_{|k|=n, k \in \mathbf{N}_{1 \times j, p}} \mathfrak{M}(\mathbf{k}) e_k .$$

By the fact that R is of characteristic p , using the uniqueness of the base p representation of n , Lemma 2.5 imply

$$f_j(e_n) = \sum_{k \in S_{j\mathbf{a}}} \mathfrak{M}(\mathbf{k}) e_k ;$$

Lemma 2.6 allows to write :

$$f_j(e_n) = \sum_{k \in S_{j\mathbf{a}}} \#stab(\mathbf{k}) e_k ;$$

and since the order of the stabilizer is constant over the orbit of \mathbf{a} , it results that :

$$f_j(e_n) = \#stab(\mathbf{a}) \sum_{k \in S_{j\mathbf{a}}} e_k .$$

On the other hand

$$\sum_{\sigma \in S_j} e_{\sigma\mathbf{a}} = \sum_{\sigma \in \mathcal{R}} \sum_{\tau \in stab(\mathbf{a})} e_{\sigma\tau\mathbf{a}} ;$$

where \mathcal{R} is a set of class representatives for the left cosets of $stab(\mathbf{a})$ in S_j . We deduce :

$$\sum_{\sigma \in S_j} e_{\sigma\mathbf{a}} = \sum_{\sigma \in \mathcal{R}} \#stab(\mathbf{a}) e_{\sigma\mathbf{a}} ,$$

hence the result.

4.5 The map Tr_j

Let j be a non-zero natural integer and σ a permutation in S_j , we have already defined (Definition 4.6) the endomorphism $\tau_{\sigma^{-1}, 1 \times j}$ of $\mathcal{P}_1^{\otimes j}$ that with an element $(x_1 \otimes x_2 \otimes \dots \otimes x_j)$, associates the element $(x_{\sigma(1)} \otimes x_{\sigma(2)} \otimes \dots \otimes x_{\sigma(j)})$. The map Tr_j from $\mathcal{P}_1^{\otimes j}$ to $\mathcal{P}_1^{\otimes j}$ is then defined by :

$$Tr_j \left(\bigotimes_{i=1}^j x_i \right) = \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, 1 \times j} \left(\bigotimes_{i=1}^j x_i \right).$$

that is

$$Tr_j \left(\bigotimes_{i=1}^j x_i \right) = \sum_{\sigma \in S_j} \left(\bigotimes_{i=1}^j x_{\sigma(i)} \right). \quad (23)$$

Lemma 4.12 *The submodules $Im(f_j)$ and $Im(Tr_j)$ of $\mathcal{P}_1^{\otimes j}$ are equal.*

Proof. Let \mathbf{a} be a multi-integer in $\mathbb{N}_{1 \times j, p}$. The definition of the map Tr_j gives :

$$Tr_j(e_{\mathbf{a}}) = \sum_{\sigma \in S_j} e_{\sigma \mathbf{a}} ;$$

By Lemma 4.11, it is obvious that $Im(f_j) \subseteq Im(Tr_j)$; now, let us show the reciprocal inclusion. Still by Lemma 4.11, $\sum_{\sigma \in S_j} e_{\sigma \mathbf{a}} = f_j(e_n)$ where $n = \sum_{i=1}^j p^{a_i}$ thus $Tr_j(e_{\mathbf{a}}) = f_j(e_n)$ and hence $Im(Tr_j) \subseteq Im(f_j)$.

4.6 Proof of Theorem 3.17

Let $(\psi_j)_{j \geq 1}$ an element in the set $\prod_{j \geq 1} \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$. We write $\psi_0 = 0$ for the sake of convenience. We look for an endomorphism ϕ of the R -coalgebra \mathcal{B}_1 such that $\phi_j^1 = \psi_j$ for each natural integer $j \geq 1$. By formula (2), it is sufficient to define its components ϕ_μ^ν .

Definition 4.13 *Let ρ and j be two natural integers. We define the map $h_{\rho, j}$ from \mathcal{P}_ρ to $\mathcal{P}_1^{\otimes j}$, by :*

$$h_{\rho, j} = \sum_{\mathbf{b} \in \mathbb{N}^j, |\mathbf{b}| = \rho} \left[\bigotimes_{\nu=1}^j \psi_{b_\nu} \right] \circ \Delta_{\mathbf{b}}^{(j)}.$$

In particular we remark that $h_{0,0} = \varepsilon_0$, $h_{\rho,0} = 0$ for $\rho > 0$ and $h_{\rho,1} = \psi_\rho$. Given two natural integers ρ and j , we look for a R -linear map ϕ_ρ^j from \mathcal{P}_ρ to \mathcal{P}_j such that :

$$f_j \circ \phi_\rho^j = h_{\rho, j}. \quad (24)$$

In order to find ϕ_ρ^j satisfying the equality (24), as the sub- R -modules \mathcal{P}_ρ are free, it is sufficient to show that $Im(h_{\rho, j}) \subseteq Im(f_j)$; but by Lemma 4.12, the submodules $Im(f_j)$ and $Im(Tr_j)$ are equal, and accordingly we have only to show that $Im(h_{\rho, j}) \subseteq Im(Tr_j)$.

Lemma 4.14 *For two natural integers j and ρ such that $j > 0$ and $\rho \geq 0$, the image $Im(h_{\rho, j})$ is a submodule of $Im(Tr_j)$.*

Proof. Definition 4.13 gives :

$$h_{\rho, j} = \sum_{\mathbf{b} \in \mathbb{N}^j, |\mathbf{b}| = \rho} \left[\bigotimes_{\nu=1}^j \psi_{b_\nu} \right] \circ \Delta_{\mathbf{b}}^{(j)}. \quad (25)$$

Now, for each multi-integer \mathbf{b} of length $j > 0$, Lemma 4.8 gives :

$$\Delta_{\mathbf{b}}^{(j)} = \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, \mathbf{b}} \circ \Gamma_{\sigma \mathbf{b}}^{(j)} ;$$

substituting this last relation in identity (25), we obtain :

$$h_{\rho, j} = \sum_{\mathbf{b} \in \mathbb{N}^j, |\mathbf{b}| = \rho} \left[\bigotimes_{\nu=1}^j \psi_{b_\nu} \right] \circ \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, \mathbf{b}} \circ \Gamma_{\sigma \mathbf{b}}^{(j)} ;$$

then using Lemma 4.7, we obtain :

$$h_{\rho,j} = \sum_{b \in \mathbb{N}^j, |b|=\rho} \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, 1 \times j} \circ \left[\bigotimes_{\nu=1}^j \psi_{(\sigma b)_\nu} \right] \circ \Gamma_{\sigma b}^{(j)} ;$$

inverting the summations, we get :

$$h_{\rho,j} = \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, 1 \times j} \circ \sum_{b \in \mathbb{N}^j, |b|=\rho} \left[\bigotimes_{\nu=1}^j \psi_{(\sigma b)_\nu} \right] \circ \Gamma_{\sigma b}^{(j)} ;$$

in this last sum, we replace the index (σ, \mathbf{b}) by (σ, \mathbf{c}) with $\mathbf{c} = \sigma \mathbf{b}$; we find

$$h_{\rho,j} = \sum_{\sigma \in S_j} \tau_{\sigma^{-1}, 1 \times j} \circ \sum_{c \in \mathbb{N}^j, |c|=\rho} \left[\bigotimes_{\nu=1}^j \psi_{c_\nu} \right] \circ \Gamma_c^{(j)} ;$$

hence

$$h_{\rho,j} = Tr_j \circ \left(\sum_{c \in \mathbb{N}^j, |c|=\rho} \left[\bigotimes_{\nu=1}^j \psi_{c_\nu} \right] \circ \Gamma_c^{(j)} \right) .$$

The proof of the lemma is complete.

So (24) allows us to find ϕ_ρ^j for all natural integers j and ρ . It remains only to verify that the endomorphism ϕ of \mathcal{B}_1 that has as ϕ_ρ^j as (ρ, j) -component is a coalgebra endomorphism . Since f_0 is bijective, the relation (24) proves that

$$\phi_\rho^0 = 0 \quad \text{if } \rho > 0 ;$$

and

$$\phi_0^0 = I_{\mathcal{P}_0} \quad \text{if } \rho = 0 .$$

It results that $\varepsilon \circ \phi = \varepsilon$. It remains to prove the identity $\Delta \circ \phi = (\phi \otimes \phi) \circ \Delta$. By Proposition 3.14, this is equivalent to prove that, for every natural integers l, m, ρ , we have

$$\Delta_{l,m} \circ \phi_\rho^{l+m} = \sum_{\mu+\nu=\rho} (\phi_\mu^l \otimes \phi_\nu^m) \circ \Delta_{\mu,\nu} . \quad (26)$$

Now, by Lemma 4.9 the map f_j is injective and as the submodules \mathcal{P}_j are flat, we infer that $f_l \otimes f_m$ is injective. Thus equality (26) is equivalent to the equality given by composition on the left with $\Delta_{1 \times l}^{(l)} \otimes \Delta_{1 \times m}^{(m)} = f_l \otimes f_m$. By Proposition 4.3, we are reduced to prove

$$\Delta_{1 \times (l+m)}^{(l+m)} \circ \phi_\rho^{l+m} = \sum_{\mu+\nu=\rho} (\Delta_{1 \times l}^{(l)} \circ \phi_\mu^l) \otimes (\Delta_{1 \times m}^{(m)} \circ \phi_\nu^m) \circ \Delta_{\mu,\nu} ,$$

that is :

$$f_{l+m} \circ \phi_\rho^{l+m} = \sum_{\mu+\nu=\rho} (f_l \circ \phi_\mu^l) \otimes (f_m \circ \phi_\nu^m) \circ \Delta_{\mu,\nu} ;$$

and using the formula (24), we see that is sufficient to prove that :

$$h_{\rho, l+m} = \sum_{\mu+\nu=\rho} (h_{\mu, l} \otimes h_{\nu, m}) \circ \Delta_{\mu, \nu} .$$

We compute the right-hand sum :

$$\begin{aligned} \sum_{\mu+\nu=\rho} (h_{\mu, l} \otimes h_{\nu, m}) \circ \Delta_{\mu, \nu} = & \sum_{\substack{\mu + \nu = \rho, \\ \mathbf{b} \in \mathbb{N}^l, |\mathbf{b}| = \mu, \\ \mathbf{c} \in \mathbb{N}^m, |\mathbf{c}| = \nu}} \left(\bigotimes_{v=1}^l \psi_{b_v} \right) \otimes \left(\bigotimes_{v=1}^m \psi_{c_v} \right) \circ [(\Delta_{\mathbf{b}}^{(l)} \otimes \Delta_{\mathbf{c}}^{(m)}) \circ \Delta_{\mu, \nu}]. \end{aligned}$$

But, by Proposition 4.3, $(\Delta_{\mathbf{b}}^{(l)} \otimes \Delta_{\mathbf{c}}^{(m)}) \circ \Delta_{\mu, \nu} = (\Delta_{\mathbf{b}}^{(l)} \otimes \Delta_{\mathbf{c}}^{(m)}) \circ \Delta_{|\mathbf{b}|, |\mathbf{c}|} = \Delta_{\mathbf{bc}}^{(l+m)}$, thus :

$$\sum_{\mu+\nu=\rho} (h_{\mu, l} \otimes h_{\nu, m}) \circ \Delta_{\mu, \nu} = \sum_{\mu+\nu=\rho, \mathbf{b} \in \mathbb{N}^l, |\mathbf{b}|=\mu, \mathbf{c} \in \mathbb{N}^m, |\mathbf{c}|=\nu} \left(\bigotimes_{v=1}^l \psi_{b_v} \right) \otimes \left(\bigotimes_{v=1}^m \psi_{c_v} \right) \circ \Delta_{\mathbf{bc}}^{(l+m)} ;$$

and by setting $\mathbf{bc} = \mathbf{a}$ with $\mathbf{a} \in \mathbb{N}^{l+m}$, the last equality becomes :

$$\begin{aligned} \sum_{\mu+\nu=\rho} (h_{\mu, l} \otimes h_{\nu, m}) \circ \Delta_{\mu, \nu} &= \sum_{\mathbf{a} \in \mathbb{N}^{l+m}, |\mathbf{a}|=\rho} \left[\bigotimes_{v=1}^{l+m} \psi_{a_v} \right] \circ \Delta_{\mathbf{a}}^{(l+m)} \\ &= h_{\rho, l+m} ; \end{aligned}$$

hence the result. Thus ϕ is a R -coalgebra endomorphism of \mathcal{B}_1 such that $\Theta(\phi) = (\phi_j^1)_{j \geq 1}$, and so Θ is bijective.

Corollary 4.15 *A coalgebra endomorphism ϕ of \mathcal{B}_1 is bijective if and only if ϕ_1^1 is an automorphism of \mathcal{P}_1 .*

Proof. Let ϕ be a R -coalgebra endomorphism of \mathcal{B}_1 . Let us show that if ϕ is bijective, then the component ϕ_1^1 is too. Set $\psi = \phi^{-1}$, so that ψ is a R -coalgebra endomorphism of \mathcal{B}_1 such that $\phi \circ \psi = I_{\mathcal{B}_1}$ and $\psi \circ \phi = I_{\mathcal{B}_1}$. Let us compute the (γ, ρ) -component of the compositions $\psi \circ \phi$ and $\phi \circ \psi$. We obtain by means of Proposition 1.4 :

$$(\psi \circ \phi)_\gamma^\rho = \sum_{\delta \in \mathbb{N}} \psi_\delta^\rho \circ \phi_\gamma^\delta \quad \text{and} \quad (\phi \circ \psi)_\gamma^\rho = \sum_{\delta \in \mathbb{N}} \phi_\delta^\rho \circ \psi_\gamma^\delta .$$

As $\psi \circ \phi = I_{\mathcal{B}_1}$ and $\phi \circ \psi = I_{\mathcal{B}_1}$, using Proposition 3.12 and Lemma 3.15, we get :

$$\psi_1^1 \circ \phi_1^1 = I_{\mathcal{P}_1} \quad \text{and} \quad \phi_1^1 \circ \psi_1^1 = I_{\mathcal{P}_1} ;$$

which means that ϕ_1^1 is an automorphism of \mathcal{P}_1 .

Reciprocally, let ϕ be a R -coalgebra endomorphism of \mathcal{B}_1 such that ϕ_1^1 is an automorphism of \mathcal{P}_1 ; let us show that ϕ is bijective. We use the two following lemmas.

Lemma 4.15a

Let ϕ be an endomorphism of \mathcal{B}_1 ; if ϕ_1^1 is an automorphism of \mathcal{P}_1 then, for every natural integer j , ϕ_j^j is an automorphism of \mathcal{P}_j .

Proof. For $j = 0$, $\phi_0^0 = I_{\mathcal{P}_0}$ and for $j = 1$, ϕ_1^1 is *ex hypothesi* an automorphism of \mathcal{P}_1 . Let us show that for every natural integer $j \geq 2$, ϕ_j^j is an automorphism of \mathcal{P}_j . By equality (24) we have :

$$f_j \circ \phi_j^j = \phi_1^{1 \otimes j} \circ f_j . \quad (27)$$

As f_j is known to be injective (Lemma 4.9) this shows that ϕ_j^j is injective too. Having in mind to show that ϕ_j^j is surjective, we first observe that the automorphism $\phi_1^{1 \otimes j}$ of $\mathcal{P}_1^{\otimes j}$ maps the submodule $Im(Tr_j)$ into itself and so induces an automorphism of this submodule. Let y be an element of \mathcal{P}_j ; by Lemma 4.12, there exists an element z in $\mathcal{P}_1^{\otimes j}$ such that $f_j(y) = Tr_j(z)$; we have remarked that $\phi_1^{1 \otimes j}$ induces an automorphism of the submodule $Im(Tr_j)$ hence we can write

$$f_j(y) = \phi_1^{1 \otimes j}(z') ; \quad (28)$$

for an element z' in $Im(Tr_j) = Im(f_j)$, so that there exists x belonging to \mathcal{P}_j satisfying $z' = f_j(x)$. Thus

$$f_j(y) = \phi_1^{1 \otimes j}(f_j(x)) ;$$

formula (27) gives then $f_j(y) = f_j(\phi_j^j(x))$; as f_j is injective, we deduce that $y = \phi_j^j(x)$, which ends the proof of our lemma.

Lemma 4.15b

Let ϕ be an endomorphism of \mathcal{B}_1 ; if ϕ_1^1 is an automorphism of \mathcal{P}_1 then ϕ is surjective.

Proof. We know that the data of the $(\mathcal{P}_\delta)_{\delta \in \mathbb{N}}$ is a grading of type \mathbb{N} on \mathcal{B}_1 . Let y be an element in \mathcal{P}_δ , let us show by induction on δ that y belongs to $Im(\phi)$. For $\delta = 0$, $y \in \mathcal{P}_0$, thus $y = \phi(y)$ because by Lemma 3.15, $\phi_0^0 = I_{\mathcal{P}_0}$. Suppose that for $\delta < j$, we have $\mathcal{P}_\delta \subseteq Im(\phi)$ and let $y \in \mathcal{P}_j$; by Lemma 4.15a, there exists x belonging to \mathcal{P}_j such that $y = \phi_j^j(x)$. Now let us compute $\phi(x) - y$; formula (2) gives :

$$\phi(x) = \sum_{\delta=1}^j i_\delta \circ \phi_j^\delta \circ pr^j(x) = \sum_{\delta=1}^j \phi_j^\delta(x) ; \quad (29)$$

then $\phi(x) - y = \sum_{\delta=1}^{j-1} \phi_j^\delta(x)$; as $\phi_j^\delta(x) \in \mathcal{P}_\delta$ for $\delta < j$, by induction hypothesis we have $\phi_j^\delta(x) \in Im(\phi)$ for $\delta < j$ then $\phi_j^\delta(x) = \phi(x_\delta)$ for some x_δ in \mathcal{B}_1 thus $\phi(x) - y = \sum_{\delta=1}^{j-1} \phi(x_\delta)$. Hence $y = \phi(x) - \sum_{\delta=1}^{j-1} \phi(x_\delta)$ which proves that $y \in Im(\phi)$; thus ϕ is surjective.

Now we are ready to prove Corollary 4.15. Let ϕ be a R -coalgebra endomorphism of \mathcal{B}_1 such that ϕ_1^1 is an automorphism of \mathcal{P}_1 , we are going to build an element $(\chi_j^1)_{j \geq 1}$ in

$\prod_{j \geq 1} \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$. Using Lemma 4.15a, we begin by setting $\chi_i^i = (\phi_i^i)^{-1}$ for every integer $i \in \{1, \dots, j\}$. For $j > 1$ we define by induction :

$$\chi_j^1 = - \sum_{\delta=1}^{j-1} \chi_\delta^1 \circ \phi_j^\delta \circ \chi_j^j ; \quad (30)$$

where $\chi_j^1 \in \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$. By Theorem 3.17, there exists a unique R -coalgebra endomorphism χ of \mathcal{B}_1 such that $\Theta(\chi) = (\chi_j^1)_{j \geq 1}$. Consider the R -coalgebra endomorphism $\chi \circ \phi$ of \mathcal{B}_1 and let us compute $\Theta(\chi \circ \phi) = [(\chi \circ \phi)_j^1]_{j \geq 1}$. Proposition 1.4 implies the equality

$$(\chi \circ \phi)_j^1 = \sum_{\delta \in \mathbb{N}} \chi_\delta^1 \circ \phi_j^\delta ; \quad (31)$$

and using the fact that $\phi_j^\delta = 0$ when $\delta > j$, formula (31) gives :

$$(\chi \circ \phi)_j^1 = \chi_j^1 \circ \phi_j^j + \sum_{\delta=1}^{j-1} \chi_\delta^1 \circ \phi_j^\delta ;$$

for $j > 1$, substituting for χ_j^1 its value given by formula (30), we obtain :

$$(\chi \circ \phi)_j^1 = - \sum_{\delta=1}^{j-1} \chi_\delta^1 \circ \phi_j^\delta \circ \chi_j^j \circ \phi_j^j + \sum_{\delta=1}^{j-1} \chi_\delta^1 \circ \phi_j^\delta ;$$

but $\chi_j^j \circ \phi_j^j = I_{\mathcal{P}_j}$ thus

$$(\chi \circ \phi)_j^1 = - \sum_{\delta=1}^{j-1} \chi_\delta^1 \circ \phi_j^\delta + \sum_{\delta=1}^{j-1} \chi_\delta^1 \circ \phi_j^\delta = 0.$$

We see that $(\chi \circ \phi)_j^1 = 0$ for $j > 1$; for $j = 1$, $(\chi \circ \phi)_1^1 = \chi_1^1 \circ \phi_1^1 = I_{\mathcal{P}_1}$; so we have $\Theta(\chi \circ \phi) = \Theta(I_{\mathcal{B}_1})$. As, by Theorem 3.17, Θ is bijective, we have $\chi \circ \phi = I_{\mathcal{B}_1}$. It remains only to prove that $\phi \circ \chi = I_{\mathcal{B}_1}$. Let y be an element in \mathcal{B}_1 , we want to prove that $\phi \circ \chi(y) = y$; as ϕ is surjective by Lemma 4.15b, there exists an element x in \mathcal{B}_1 such that $y = \phi(x)$ and then $\phi(\chi(y)) = \phi(\chi(\phi(x)))$ but $\chi(\phi(x)) = x$ and hence $\phi(\chi(y)) = \phi(x) = y$.

5 Examples

In this last Section, we present some examples of endomorphisms of the binomial coalgebra. We fix a reduced ring R the characteristic of which is a prime number p . In Examples 1 and 2, we consider endomorphisms defined very directly by means of our Theorem 3.17. These examples can also be built by Carlitz's method. Both preserve the degree as defined in Remark 3.2. Example 3 is the Carlitz's original example. Example 4 cannot be got by Carlitz's method. It does not preserve the degree. Eventually, we show that our Example 1 cannot be built by means of the method of Keigher and Pritchard that we have described at the beginning of our paper.

5.1 Example 1

Let λ be an element in R ; we consider the element $(\psi_j)_{j \geq 1}$ in $\prod_{j \geq 1} \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$ such that $\psi_j = 0$ if $j \neq 1$ and $\psi_1 : \mathcal{P}_1 \rightarrow \mathcal{P}_1$ is defined by $\psi_1(x) = \lambda x$. By Theorem 3.17, we define in a unique way the endomorphism ϕ_λ of \mathcal{B}_1 by the condition :

$$\Theta(\phi_\lambda) = (\psi_j)_{j \geq 1} ,$$

where Θ is the same map as in formula (19). It is easy to verify by formula (24) that :

$$\forall n \in \mathbb{N}; \phi_\lambda(e_n) = \lambda^{s_p(n)} e_n .$$

This example fall into the class of endomorphisms liable to be built by the method of Carlitz explained at the beginning of our paper. Indeed, let us set $\Psi_\nu(t) = \lambda t^{p^\nu}$, so that

$$\Psi_\nu(t+u) = \Psi_\nu(t) + \Psi_\nu(u) . \quad (32)$$

From this, the Carlitz's method build a polynomial sequence $(G_k)_k$ of binomial type such that

$$G_k(t) = \Psi_0(t)^{\alpha_0} \Psi_1(t)^{\alpha_1} \dots \Psi_s(t)^{\alpha_s} ,$$

where $k = \alpha_0 + \alpha_1 p + \dots + \alpha_s p^s$ is the base p representation of k . An easy computation gives

$$G_k(t) = \lambda^{s_p(k)} t^k .$$

As $(G_k)_k$ is of binomial type (that is it verifies the binomial formula

$$G_k(t+u) = \sum_{\beta=0}^k \binom{k}{\beta} G_\beta(t) G_{k-\beta}(u) ,$$

by identifying \mathcal{B}_1 with $R[x]$, the R -linear map ϕ from $R[x]$ to $R[x]$ that sends x^n to $G_n(x) = \lambda^{s_p(n)} x^n$ is identified to the R -coalgebra endomorphism ϕ_λ of \mathcal{B}_1 .

5.2 Example 2

Let γ be an element fixed in R ; for $j > 1$, let Υ_j denote the zero morphism from \mathcal{P}_j to \mathcal{P}_1 and define Υ_1 as the endomorphism of the R -module \mathcal{P}_1 such that $\Upsilon_1(e_n) = \gamma^n e_n$ for $n \in \mathbb{N}_{1,p}$. Consider the element $(\Upsilon_j)_{j \geq 1}$ in the product $\prod_{j \geq 1} \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$ and let Θ be the map defined by the formula (19). By Theorem 3.17, we define in a unique way the endomorphism ϕ'_γ of \mathcal{B}_1 by setting :

$$\Theta(\phi'_\gamma) = (\Upsilon_j)_{j \geq 1} .$$

Using formula (24), we find easily :

$$\forall n \in \mathbb{N}; \phi'_\gamma(e_n) = \gamma^n e_n .$$

This example is also obtainable by Carlitz's method. Indeed, let us set $\Psi_\nu(t) = \gamma^{p^\nu} t^{p^\nu}$. This sequence Ψ_ν satisfy the equality (32) and if $k = \alpha_0 + \alpha_1 p + \dots + \alpha_s p^s$ is the base p

representation of k , the Carlitz's method built a polynomial sequence $(G_k)_k$ of binomial type such that :

$$\begin{aligned} G_k(t) &= \Psi_0(t)^{\alpha_0} \Psi_1(t)^{\alpha_1} \dots \Psi_s(t)^{\alpha_s} \\ &= \lambda^k t^k. \end{aligned}$$

As $(G_k)_{k \in \mathbb{N}}$ is of binomial type, by identifying \mathcal{B}_1 with $R[x]$, the R -linear map ϕ' from $R[x]$ to $R[x]$ that sends x^n to $G_n(x) = \gamma^n x^n$ is identified to the R -coalgebra endomorphism ϕ'_γ of \mathcal{B}_1 .

5.3 Example 3

By taking up the original example of Carlitz as described by Diarra in [5], we can get another endomorphism of the coalgebra \mathcal{B}_1 . Let us describe it.

The Carlitz module defined in [4] leads us to the introduction of two important series, namely the Carlitz exponential series and the Carlitz logarithm. For x an element belonging to $\mathbb{F}_p((T^{-1}))$, we define $e_c(x)$ (the Carlitz exponential series) by :

$$e_c(x) = \sum_{i=0}^{\infty} \frac{x^{p^i}}{D_i},$$

where D_i is the product of all monic polynomials of degree i in $\mathbb{F}_p[T]$. Putting $C_T(x) = x^p + Tx$, we arrive to the functional equation :

$$e_c(Tx) = C_T(e_c(x));$$

the Carlitz logarithm Log_c is the reciprocal series of e_c and it is shown that :

$$Log_c x = \sum_{i=0}^{\infty} \frac{x^{p^i}}{L_i},$$

with $L_i = \prod_{l=1}^i [l]$ with $[l] = T^{p^l} - T$. It is not difficult to see that :

$$e_c(z Log_c x) = \sum_{j=0}^{\infty} E_j(z) x^{p^j},$$

with $E_j(z) = \sum_{l=0}^j (-1)^{j-l} \frac{z^{p^l}}{L_{j-l}^{p^l} D_l}$. Now we study the sequence of polynomials (E_j) ; we remark that

$$E_j(u + v) = E_j(u) + E_j(v)$$

in $\mathbb{F}_p[u, v]$, so that by setting $\Psi_\nu = E_{p^\nu}$, the sequence Ψ_ν satisfy the relation (32). Let j be a natural integer, we write $j = j_0 + j_1 p + \dots + j_s p^s$ with $0 \leq j_i < p$. Carlitz's construction gives us here a new example of a coalgebra endomorphism of \mathcal{B}_1 , indeed the sequence h_j defined by :

$$h_j = E_{p^0}^{j_0} E_{p^1}^{j_1} \dots E_{p^s}^{j_s};$$

is a polynomial sequence of binomial type and hence by identifying \mathcal{B}_1 with $R[z]$, the R -linear map ϕ from $R[z]$ to $R[z]$ that sends z^j to $h_j(z) = \prod_{\nu=0}^s E_{q^\nu}^{j_\nu}(z)$ defines a R -coalgebra endomorphism ϕ_c of \mathcal{B}_1 .

5.4 Example 4

We give now an example of a R -coalgebra endomorphism of \mathcal{B}_1 which cannot be built by the Carlitz's method. We suppose that $p \neq 2$.

We consider the element $(\psi_j)_{j \geq 1}$ in the product $\prod_{j \geq 1} \text{Hom}(\mathcal{P}_j, \mathcal{P}_1)$ such that $\psi_j = I_{\mathcal{P}_j}$ when $j = 1$, ψ_2 is the map from \mathcal{P}_2 to \mathcal{P}_1 defined by $\psi_2(e_{p^\alpha+p^\beta}) = e_{p^{\alpha+\beta}}$ for all natural integers α and β and $\psi_j = 0$ when $j \geq 3$. By Theorem 3.17, we define in a unique way the endomorphism ϕ of \mathcal{B}_1 by setting :

$$\Theta(\phi) = (\psi_j)_{j \geq 1} .$$

By formulas (2) and (24), it is easily verified that :

$$\phi(e_{p^\alpha+p^\beta}) = e_{p^{\alpha+\beta}} + e_{p^\alpha+p^\beta} .$$

If this example can be built by means of Carlitz's method, we should have, identifying \mathcal{B}_1 with $R[x]$, the following identities :

$$\begin{aligned} x^{p^\alpha+p^\beta} + x^{p^{\alpha+\beta}} &= G_{p^\alpha+p^\beta}(x) \\ &= \Psi_\alpha(x)\Psi_\beta(x) \end{aligned}$$

with $\Psi_\alpha(x) = x^{p^\alpha}$, and that is not true.

5.5 An example of an endomorphism not described by the method of Hurwitz series

In the case of positive characteristic, Keigher and Pritchard have defined on HR an operation of composition that generalizes the composition of power series. This makes us think to build endomorphisms of \mathcal{B}_1 by transposition of endomorphisms of HR given as composition on the right by an element of HR without constant term. We are now going to show that the endomorphism ϕ_λ of example 5.1 defined by :

$$\forall n \in \mathbb{N} \quad ; \quad \phi_\lambda(e_n) = \lambda^{s_p(n)} e_n$$

cannot be obtained in this process, as soon as λ is an element of the ring R such that $\lambda^p \neq \lambda$. Such a λ exist in R when for example R is a field that is not reduced to the prime subfield.

From Lemma 3.3, the transpose $\phi_\lambda^* \in \mathcal{B}_1^*$ can be seen as a continuous endomorphism, still denoted by ϕ_λ^* , of the topological algebra HR such that :

$$\phi_\lambda^*(x^{[n]}) = \lambda^{s_p(n)} x^{[n]} ,$$

where $x^{[n]}$ is, in accordance with the notation of Keigher and Pritchard [9, page 293], the n -th divided power of $x = (0, 1, 0, 0, \dots)$ in HR .

Let search for an element f in H_0R such that :

$$\phi_\lambda^*(x^{[n]}) = \lambda^{s_p(n)} x^{[n]} = x^{[n]} \circ f ;$$

if true, we necessarily have $f = \lambda x^{[1]}$. As, for each natural integer n , the n -th divided power of f is given [9, page 295] by $f^{[n]} = x^{[n]} \circ f$, we are reduced to look for a formal Hurwitz series without constant term f such that :

$$\forall n \in \mathbb{N} \quad f^{[n]} = \lambda^{s_p(n)} x^{[n]}. \quad (33)$$

As $f = \lambda x^{[1]}$ and by [9, page 293], we have $f^{[n]} = \lambda^n x^{[n]}$, and the very existence of f would give us the equality :

$$\forall n \in \mathbb{N} \quad \lambda^n x^{[n]} = \lambda^{s_p(n)} x^{[n]}; .$$

In particular, for $n = p$, we obtain

$$\lambda^p = \lambda ;$$

but we have supposed that $\lambda^p \neq \lambda$, which is a contradiction and hence, it cannot exist $f \in HR$ without constant term such that

$$\phi_\lambda^*(x^{[n]}) = x^{[n]} \circ f ;$$

and so ϕ_λ cannot be an endomorphism of the binomial coalgebra obtained by the composition method described above.

References

- [1] **Nicolas Bourbaki**, *Éléments de mathématique, Algèbre, Chapitres 1 à 3*, Hermann, Paris 1970.
- [2] **L. Carlitz**, *A set of polynomials*, Duke Math. Jour. 6, 1940.486-504.
- [3] **Louis Comtet**, *Analyse combinatoire*, tome premier, Collection Sup “Le Mathématicien”, 4, Presses Universitaires de France, Paris, 1970.
- [4] **D. Goss**, *Basic Structures of Function Field Arithmetic*, Ergeb. Math. u. i. Grenz. 35, Springer-Verlag, Berlin-Heidelberg-New York, 1998.
- [5] **Bertin Diarra**, *The Hopf algebra $\mathcal{C}(\mathbb{F}_q[[T]], K); \mathbb{F}_q((T)) \subset K$* , preprint, 2002.
- [6] **Leonard Eugene Dickson**, *History of the theory of numbers, volume I : Divisibility and Primality*, reprint, Chelsea Publishing Company, New York, 1971.
- [7] **S. A. Joni and G.-C. Rota**, *Coalgebras and Bialgebras in Combinatorics*, Contemporary Mathematics, Volume 6 (1982), 1-47.
- [8] **William F. Keigher**, *On the ring of Hurwitz series*, Comm. Algebra 25 (1997), no. 6, 1845-1859.
- [9] **William F. Keigher and F. Leon Pritchard**, *Hurwitz series as formal functions*, J. Pure Appl. Algebra 146 (2000), no. 3, 291-304.

- [10] **Édouard Lucas**, *Théorie des nombres*, nouveau tirage, Librairie scientifique et technique Albert Blanchard, Paris, 1958.
- [11] **Moss E. Sweedler**, *Hopf algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York 1969.
- [12] **Steven Roman**, The umbral calculus, chapter 16 in *Advanced linear algebra*, Graduate Texts in Mathematics, 135, Springer-Verlag, New York, 1992.
- [13] **Steven Roman and Gian-Carlo Rota**, *The umbral calculus*, Advances in Math, 27 (1978), no. 2, 95-188.

LACO (UMR 6090 CNRS)
Département de Mathématiques
Faculté des Sciences
123, avenue Albert Thomas
87060 LIMOGES Cedex
FRANCE.