Lecture on the various types of symmetric functions

E.J. Ditters

Preliminary , June 24, 2002, **concept**

Abstract

A short introduction[1] is given to the theory of symmetric functions, quasi-symmetric functions and noncommutative symmetric functions. The theorem of Radford is mentioned. An example is given that the monomial quasi-symmetric functions $M_{(3,6)}$ is a counterexample to the so called[2] *Ditters conjecture* A (short) proof is given, theorem 2.2 below, that the ring QSym of quasi-symmetric functions is a free polynomial algebra, generated freely by the set $\mathcal{W}$ of *Lyndon-Witt functions*. The set $\mathcal{W}$ is canonical in a sense, made precise in cor 2.4. These Lyndon-Witt functions were defined in [Di02a] and [Di02b].

Author's email adress is ejd@cs.vu.nl.

[1] based on an oral exposition

[2] but not by myself

1 Symmetric functions

1.1 Generalities

Let n be a positive natural number and put $B = \mathbb{Z}[x_1, \ldots, x_n]$. If $\mathcal{S}_n$ is the symmetric group of permutations of n obects, we may let act this group on B, by permutining the indices via

$$\sigma * (x_i) := x_{\sigma(i)}$$

and a polynomial $f \in B$ is called a *symmetric polynomial* if f does not change under permutations of these indices. For example $n = 2$ and $f = x_1 + x_2$ or $f = x_1 x_2$. Generic examples are

$$\prod_{i=1}^{n}(1 + x_i t) = \sum_{m=0}^{n} e_m t^m \equiv \exp\big(\sum_{m=1}^{n} \sigma_m \frac{t^m}{m}\big) \bmod t^{n+1} \tag{1}$$

and

$$\prod_{i=1}^{n} \frac{1}{(1 - x_i t)} = \sum_{m=0}^{n} h_m t^m \equiv \exp\big(\sum_{m=1}^{n} p_m \frac{t^m}{m}\big) \bmod t^{n+1}. \tag{2}$$

Here, the e_m are the *elementary symmetric functions*, the h_m are the *complete symmetric functions* and the p_m are the *power sums*, defined by

$$p_m = \sum_{i=1}^{n} x_i^m. \tag{3}$$

As usual, if $c = (1^{c_1}, 2^{c_2} \ldots, k^{c_k})$ is any partition and $v_i, (i \geq 1)$ is a set of (commuting variables), we let $v_c = v_1^{c_1} \cdots v_k^{c_k}$. Clearly, evry partition determinus a unique symmetric symmetric function, the *monomial symmetric function* denoted (c). function The main theorem on symmetric functions states: Every symmetric polynomial in B belongs to $\mathbb{Z}[e_1, \ldots, e_n] =: \Lambda^{(n)}$, and conversely, every polynomial in $\Lambda^{(n)}$ is symmetric. Making n arbitrarily large, we may as well consider the ring $\Lambda := \mathbb{Z}[e_i | i \geq 1]$, known as the *ring of symmetric functions*. This ring is very classical and has an astonishing rich structure, for which I only mention at the moment the following facts:

a. Due to the fact that the $\mathcal{S}_n$ is not a solvable group for $n \geq 5$, there is no possibility to express the inverse roots x_i of (2) algebraically in the elementary symmetric functions.

b. Let $\mathcal{R} = \{\chi_\lambda | \lambda \in \mathsf{Part}\}$ be the set of all irreducible representations of all symmetric groups $\mathcal{S}_n, (n \geq 1)$ and for every commutative unitary ring k let $k\mathcal{R} := \oplus_\chi k\chi$, thus the Grothendieck ring of the category of all representations over k of all symmetric groups $\mathcal{S}_n, (n \geq 1)$. The notion

of induced representation defines on $k\mathcal{R}$ the structure of commutative unitary ring. Define with Frobenius the *characteristic map*, taking $k = \mathbb{C}$: $\mathsf{ch} : \mathbb{C}\mathcal{R} \to \mathbb{C}[\Lambda]$, for $\chi \in \mathcal{S}_n$, denoting $\tau(\sigma)$ the cycle type of σ we set

$$\mathsf{ch}(\chi) := \frac{1}{n!} \sum_{w \in \mathcal{S}_n} \chi(w) p_{\tau(w)}.$$

Here, $p_{\tau(w)}$ is the polynomial in the power sums as given by (3). A famous theorem is now, that the characteristic map of Frobenius induces an isometric ismorphism of commutative unitary rings ([McD79, thm I.7.3]):

$$\mathsf{ch} : \mathbb{Z}\mathcal{R} \to \Lambda.$$

The characteristic map gives in particular the mutually orthonormal symmetric polynomials s_χ, know as the *Schur functions*. An extended portion of the theory of symmetric functions relates determinants to symmetric functions, for instance, the Jacobi-Trudy formula [McD79, I.3, exm 8] for the product of two Schur functions. Another classical problem is the problem of substituting symmetric functions into symmetric functions, i.e. replace the x_i by symmetric expressions in the $x's$. The resulting theory is known as *plethysm*, c.f. [McD79, I.8].

1.2 Duality

In the sequel, CUR will be an abbreviation for a commutative unitary ring and $\mathbb{N}_+$ will be the set of positive natural numbers. We use freely the notations of [DS] with the exception that the Hopf algebra $\mathbb{Z}[e_i | i \geq 1]$ of the symmetric functions will be denoted Λ as in [McD79]. As usual, we attach weight n to e_n and $\Lambda(n)$ will be the abelian subgroup of all elements that are homogeneous of weight n. For general theory on Hopf algebras and their graded duals, see [**?**], [**?**], [**?**] or [**?**]. For Λ as a Hopf algebra, see [McD79, expl 25, p 91]. Let

$$\prod_{i \geq 1} (1 + x_i t) = \sum_{n=0}^{\infty} e_n t^n = \exp\left(\sum_{m=1}^{\infty} m^{-1} \sigma_m t^m \right) \tag{4}$$

be the generating function for Λ. Thus, e_n may be identified with the n^{th}-elementary symmetric function and the set $\{p_m := (-1)^{m+1}\sigma_m | m \geq 1\}$ is a $\mathbb{Z}$-module basis for the abelian Lie algebra $\mathcal{P}(\Lambda)$ of primitive elements in Λ. The sum $\sum_{n=0}^{\infty} e_n t^n$ is a curve in Λ, equivalently, $(e_n | n \geq 0)$ with $e_0 := 1$ is a sequence of divided powers in Λ. Differentiation (4) with respect to t gives the *Newton relations*

$$n e_n = \sum_{a+b=n} e_a \sigma_b, \qquad (n \geq 1, \sigma_0 = 0) \tag{5}$$

and explicit expansion gives

$$\sigma_n = \sum_{m=1}^{n} (-1)^{m+1} \sum_{\mathcal{B}_{m,n}} \frac{(m-1)!n}{a_1! \cdots a_m!} e_1^{a_1} \cdots e_m^{a_m} \equiv ne_n + (-1)^{n+1} e_1^n \bmod (e_2, \ldots, e_{n-1})\Lambda. \tag{6}$$

Here, $\mathcal{B}_{m,n}$ is the set of all nonnegative integer solutions $a_1 + \ldots + a_m = m$ and $a_1 + 2a_2 + \ldots + ma_m = n$. If Part_n is the set of partitions $(\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r)$ of the nonnegative integer n and if $e_\lambda = \prod_i e_{\lambda_i}$, then $\{e_\lambda | \lambda \in \mathsf{Part}_n\}$ is a $\mathbb{Z}$-module basis for the homogeneous component $\Lambda(n)$ of elements of weight n. Let $\Lambda^\star := \oplus_{n=0}^{\infty} (\Lambda(n)^\star)$ be the graded dual Hopf algebra with dual basis $\mathcal{C} := \{e^\lambda | \lambda \in \cup_n \mathsf{Part}_n\}$. If $\langle -, - \rangle : \Lambda \times \Lambda^\star \to \mathbb{Z}$ is the canonical evaluation map, then

$$\forall \lambda, \mu : \langle e_\mu, e^\lambda \rangle = \delta_{\lambda,\mu}.$$

The special element e^λ corresponding to $\lambda = \underbrace{(1, \ldots, 1)}_{n}$, distribution on e_1^n, will be denoted ϵ_n. By duality one has, denoting for $\rho = (1^{r_1} \cdots m^{r_m})$ and $\sigma = (1^{s_1} \cdots m^{s_m})$ their union $\rho \cup \sigma := (1^{r_1 + s_1} \cdots m^{r_m + s_m})$:

$$\langle e_\pi \otimes e_\rho, \Delta(\epsilon_n) \rangle = \langle e_{\pi \cup \rho}, \epsilon_n \rangle,$$

making clear that

$$\Delta\big(\epsilon_n\big) = \sum_{a+b=n} \epsilon_a \otimes \epsilon_b.$$

Thus $\sum_{n=0}^{\infty} \epsilon_n t^n$ is a curve in $\Lambda^\star$. In the same way we have

$$\langle e_\pi \otimes e_\rho, \Delta\left(e^{(n)}\right) \rangle = \langle e_{\pi \cup \rho}, e^{(n)} \rangle,$$

making clear that

$$\Delta\left(e^{(n)}\right) = e^{(n)} \otimes 1 + 1 \otimes e^{(n)}.$$

Thus the $e^{(n)}$ are primitive elements. Summarizing: $\Phi : \Lambda \longrightarrow \Lambda^\star$, mapping e_n onto ϵ_n for all n, is a homomorphism of Hopf algebras. In fact, since for every n, the abelian group $\Lambda(n)$ is free of finite rank $\#\mathsf{Part}_n$, one even concludes that Φ is an isomorphism in the category Hopf. Thus we recover the well known fact $\Lambda^\star = \mathbb{Z}[\epsilon_n | n \geq 1]$. Next let $\mathcal{Z} = \mathbb{Z}\langle z_n | n \geq 1 \rangle \cong \mathbb{Z}\langle \mathbb{N}_+ \rangle$, be the Hopf algebra of the noncommutative symmetric functions, with the generic noncommutative curve

$$\sum_{n=0}^{\infty} z_n t^n = \exp\left(\sum_{m=0}^{\infty} m^{-1} x_m t^m \right), \tag{7}$$

equivalently

$$x_n = \sum_{c \in \mathsf{Comp}_n, l(c) = m} (-1)^{m+1} \frac{n}{m} z_c. \tag{8}$$

For the graded dual, we have the important fact: $\mathsf{QSym} \cong \mathcal{Z}^\star$, cf. [MR], [Gea] or [DS]. There is a diagram

(9)

Here, π is the canonical projection of $\mathcal{Z}$ onto its maximal commutative quotient and ζ is the canonical embedding of the Hopf algebra of symmetric functions into the Hopf algebra of quasisymmetric functions. By means of ζ we identify the element e^λ of $\Lambda^\star$ with the monomial symmetric function, defined by the partition λ. More precisely, let $c = (c_1, \ldots, c_n)$ be a composition of length n and $\mathcal{R}(c)$ be a set of representatives for the set of all permutations $\{(c_{w(1)}, \ldots, c_{w(n)}), w \in SS_n\}$ of the digits of c under the natural action of the symmetric group SS_n. Then, with the notations for monomial quasisymmetric functions of [**?**, (9.4.1), p 242]

$$\zeta(e^\lambda) = \sum_{d \in \mathcal{R}(\lambda)} M_d.$$

In particular $e^{(n)}$ corresponds to the "power sum" symmetric function $\sum x^n$, indexed by the symmetric composition (n) and ϵ_n corresponds to

$$M_{\underbrace{(1, \ldots, 1)}_{n}} = \sum_{x_1 < x_2 < \cdots < x_n} x_1 x_2 \cdots x_n.$$

In the sequel we shall write the monomial quasisymmetric function M_c as c and write $z_c = z_{c_1} \cdots z_{c_n}$. The evaluation map $\langle -, - \rangle$ in (9) then has the simple form

$$\forall c, d \in \mathsf{Comp} : \langle c, z_d \rangle = \delta_{c,d}. \tag{10}$$

Now apply $\Phi, \forall n : e_n \mapsto \epsilon_n$ to (4). Since Φ is weight preserving, $\Phi(\sigma_m) = \pm(m)$, thus write $\Phi(\sigma_m = (-1)^{r_m} \sigma_m$. It follows

$$\sum_{n=0}^{\infty} \epsilon_n t^n = \exp\left(\sum_{m=1}^{\infty} m^{-1} \Phi(\sigma_m) t^m \right) \equiv \sum_{m=1}^{\infty} (-1)^{r_m} (-1)^{m+1} \epsilon_1^{m+1} \bmod (\epsilon_2, \ldots, \epsilon_m) \Lambda^\star.$$

The left side assumes the value $+1$ in e_1^n, hence the right side must do the same. Evaluating the coefficient of e_1^n shows

Lemma 1.1

$$\sum_{n=0}^{\infty} \epsilon_n t^n = \exp\left(\sum_{m=1}^{\infty} m^{-1} (-1)^{m+1} (m) t^m \right). \tag{11}$$

More in particular: if we take the $\{\epsilon_n | n \geq 1\}$ as set of elementary symmetric functions, then the set $\{(m) | m \geq 1\}$ is the set of power sums.

Corollary 1.2 *From the lemma we see that* not *the set of primitive elements* $\{(n)|n \geq 1\} \subset \Lambda^\star \subset \mathsf{QSym}$ *generates the free polynomial ring* $\Lambda^\star$ *over the integers, (it generates freely* $\Lambda^\star_{\mathbb{Q}}$*), but rather the set of partitions* $\underbrace{(1,\ldots,1)}_{n}$ conjugate to (n) *is a set of free polynomial generators of* $\Lambda^\star$ *over* $\mathbb{Z}$.

1.3 A result from fomal group theory

Our proof for finding explicit polynomial generators for QSym over the ring of integers uses the following results of formal group theory. Let F be an n-parameter formal group law over a commutative unitary basis ring k, short: $F \in \mathsf{FGL}_{n,k}$, with contaravariant bialgebra $\theta(F) = k[[x_1, \ldots, x_n]]$, equipped with the x-adic topology, (discrete topology on k). If $\mathsf{MI}(n)$ is the set of n-multi-indices over $\mathbb{N}$, we let $\{\epsilon_\alpha|\alpha \in \mathsf{MI}(n)\}$ be the basis for the covariant bialgebra $U(F) = \oplus_\alpha k\epsilon_\alpha$, dual to the basis of monomials $\{x^\alpha|\alpha \in \mathsf{MI}(n)\}$ of $\theta(F)$. A *formal curve* in F is by definition a continuous homomorphism of k-algebras $\phi : \theta(F) \longrightarrow k[[t]]$, commuting with the augmentation on the (topological) Hopf algebra $\theta(F)$ and the map $t \mapsto 0$ on $k[[t]]$. Writing

$$\phi(x) = \sum_{i=0}^{\infty} \phi_i(x)t^i = \left(\sum_{i=0}^{\infty} \phi_i t^i\right)(x), \qquad x \in \theta(F),$$

gives the criterion: ϕ is a formal curve if and only if the set $(\phi_i|i \geq 0)$ is a sequence of divided powers in the Hopf algebra $U(F)$. The terminology "formal curve" is based on the identification of the set of continuous algebra homomorphisms $\theta(F) \to k[[t]]$ with the set of morphisms of formal spectra $\mathsf{Spf}(k[[t]]) \to \mathsf{Spf}(\theta(F))$. Returning to the given formal group law, the special curves defined by $\phi_{F,i}(x_j) = \delta_{i,j}t, (1 \leq i \leq n)$ are called the *canonical curves*. Let $\phi_{F,i} = \sum_j \phi_{F,i,j}t^j$. Then with $\delta_{F,i} := \phi_{F,i,1}$ the set $\{\delta_{F,i}|1 \leq i \leq n\}$ is a basis for the Lie algebra of primitive elements $\mathcal{P}(F) \subset U(F)$. Since the covariant bialgebra $U(F)$ is pointed irreducible, we have the coradical filtration on $U(F) = \cup_n U(F)_n$ and define for $u \in U(F)$ its *height* $h(u) := \min_n\{U(F)_n|u \in U(F)_n\}$ cf. [**?**, th 9.2.2, p 193]. Since $U(F)_iU(F)_j \subset U(F)_{i+j}$, we have $h(uv) = h(u) + h(v)$. If $J = \mathrm{Ker}\,(\epsilon : \theta(F) \to k)$, then $u \in U(F)_n \Leftrightarrow \langle u, J^{n+1}\rangle = 0$ by [**?**, prop 11.0.5b, p 220].

Theorem 1.3 *Let* $k \in \mathsf{CUR}$ *and let* $\theta(F) = k[[x_{F,i}|1 \leq i \leq n]]$ *be the contravariant bialgebra of an* n*-parameter formal group law over* k*. Let* $\phi_{F,i}, (1 \leq i \leq n)$ *be the set of canonical curves on these generators of* $\theta(F)$*, thus* $\forall i, j : \phi_{F,i}(x_{F,j}) = \delta_{i,j}t$*. Then the set of all ordered products*

$$\mathcal{B} = \{\phi_{F,\alpha} := \phi_{F,i_1,\alpha_1} \cdots \phi_{F,i_k,\alpha_k}|k \geq 0, i_1 < \ldots < i_k, \text{ all } \alpha_1, \ldots \alpha_k \geq 0\} \tag{12}$$

is a k-module basis for the dual $U(F)$*. It is a* structural basis *in the sense of Dieudonné, namely*

$$\forall \alpha \in \mathsf{MI}(n) : \Delta_{U(F)}(\phi_{F,\alpha}) = \sum_{\{u,v \in \mathsf{MI}(n) | u+v=\alpha\}} \phi_{F,u} \otimes \phi_{F,v}. \tag{13}$$

The set $\{\delta_{F,i} := \phi_{F,i,1} | 1 \leq i \leq n\}$ *is a k-module basis for the k-Lie algebra* $\mathcal{P}(F)$ *of primitives of* $U(F)$*. Finally, one has*

$$\forall \alpha \in \mathsf{MI}(n) : h(\phi_\alpha) = |\alpha|. \tag{14}$$

Proof. Since the formal group law will remain fixed, we omit the index "F". For any multi-index $\alpha = (\alpha_1, \ldots, \alpha_n)$ we define its *norm* $|\alpha|$ to be $|\alpha| := \sum_i \alpha_i$. We intend to prove

$$\forall \alpha, \beta \in \mathsf{MI}(n) : |\alpha| \leq |\beta| \Rightarrow \langle \phi_\alpha, x^\beta \rangle = \delta_{\alpha,\beta}. \tag{15}$$

Now, if $|\alpha| = 0$, corresponding to $k = 0$ in (12), we have $\phi_0 = \epsilon : \theta(F) \longrightarrow k$, the canonical augmentation. It is well known that this augmentation is the neutral element for multiplication in $U(F)$. It then is clear that for all β we have $\langle \phi_0, x^\beta \rangle = \delta_{0,\beta}$. More generally, let $N := |\beta|$ and $|\beta| > |\alpha|$. Applying Δ^{N-1} we have

$$\sum_{u_1 + \ldots + u_N = \alpha} \langle \phi_{u_1} \otimes \cdots \otimes \phi_{u_N}, x_1^{\otimes \beta_1} \otimes \cdots \otimes x_n^{\otimes \beta_n} \rangle = 0. \tag{16}$$

Indeed, since $|\alpha| < |\beta|$, there must be some u_j with $\phi_{u_j} = \phi_0 = \epsilon$, while the corresponding x-factor belongs to the augmentation ideal Ker (ϵ).

By the very definition of canonical curves, $\alpha| = |\beta| = 1$ implies that relation (15) is true. Thus assume (15) to be true for $|\alpha| = |\beta| = N$, for some $N \geq 1$ and let $|\alpha| = N + 1$. In view of (16), we may restrict to the case $|\beta| = N + 1$ Write $\beta =: \mu + \nu$ with some fixed $|\mu| \neq 0$ and $|\nu| \neq 0$, then

$$\langle \phi_\alpha, x^\beta \rangle = \sum_{u+v=\alpha} \langle \phi_u, x^\mu \rangle \langle \phi_v, x^\nu \rangle.$$

By induction, the right side can be nonzero if and only if there are multi-indices u and v with sum α such that $u = \mu$ and $v = \nu$. Since $\mu + \nu = \beta$, we thus must have $\beta = \alpha$. This proves (15). The verification of (13) is easy. By (15) we immediately see For each $\alpha \mathsf{MI}(n)$ we have $h(\phi_\alpha) = |\alpha|$. □

Remark It is not an essential complication, to consider formal group laws in a denumerably infinite set of (weighted) parameters.

1.4 Canonical curves for $\Lambda^\star$

We use foregoing theorem in order to find canonical curves for the completion of $\Lambda^\star$. Let $\Lambda^{\star\hat{}} = \mathbb{Z}[[\epsilon_n | n \geq 1]]$ be the completion of $\Lambda^\star$ and consider the set of canonical curves, denoted $\{\phi_a | a \geq 1\}$ and determined by

$$\phi_a(\epsilon_b) := \delta_{a,b} t.$$

The "trick of Cartier" relates ϕ_a to the Frobenius operators of formal group theory: let ζ_a be any primitive a^{th}-root of 1 and consider

$$\Phi_a := \prod_{i=0}^{a-1} [\zeta_a^i] e = \prod_{i=0}^{a-1} \exp\left(\sum_{m=1}^{\infty} m^{-1} \sigma_m \zeta_a^{mi} t^m\right) = \exp\left(\sum_{m=1}^{\infty} m^{-1} \sigma_m \sum_{i=0}^{a-1} (\zeta_a^{mi}) t^m\right). \tag{17}$$

Here, the operator $[\lambda]$ on formal curves, denotes the homothety $([\lambda]\phi)(t) = \phi(\lambda t)$ for $\lambda \in k$ and curves $\phi = \phi(t)$.

$$\sum_{i=0}^{a-1} \zeta_a^{mi} = \begin{cases} a & \text{if } a | m \\ 0 & \text{otherwise} \end{cases}.$$

Replacing m by aN and substituting afterwards n by m, it follows that (17) reduces to

$$\prod_{i=0}^{a-1} [\zeta_a^i] e = \exp\left(\sum_{m=1}^{\infty} m^{-1} \sigma_{am} t^{am}\right) = V_a \exp\left(\sum_{m=1}^{\infty} m^{-1} \sigma_{am} t^m\right). \tag{18}$$

Recalling the Verschiebung $(V_a\phi)(t) = \phi(t^a)$, we see that V_a is injective. The exponential defines a curve $F_a e$ with components in $\Lambda_{\mathbb{Q}}$, while the left side defines a curve with coefficients in $\Lambda[\zeta_a]$. The curve thus has coefficients in Λ and can be written in the form

$$F_a e = \prod_{i=1}^{\infty} (1 + x_i^a t) = \sum_{n=0}^{\infty} e_{a,n} t^n = \exp\left(\sum_{m=1}^{\infty} m^{-1} \sigma_{am} t^m\right). \tag{19}$$

This curve is called the a^{th} *commutative Frobenius curve*. One easily sees from (19) that $e_{a,n}$ is the monomial symmetric function, belonging to the partition $\underbrace{(a, a, \ldots, a)}_{n}$ of weight an. Working modulo the ideal in Λ, generated by the $e_i, (i \geq 2)$, one sees that

$$F_a e \equiv \exp\left(\sum_{m=1}^{\infty} m^{-1} (-e_1)^{am+1} t^m\right) \equiv 1 - (-e_1)^a t.$$

Considered as a morphism $F_a e : \Lambda^{\star\hat{}} \longrightarrow \mathbb{Z}[[t]]$, it follows from this formula that $F_a e$ contains from all powers of e_1 only $-(-1e_1)^a = (-1)^{a+1} e_1^a$ and thus is canonical on the generator $(-1)^{a+1}\epsilon_a$ and assumes the value 1. Thus,

Corollary 1.4 *modulo sign, the Frobenius curves are canonical curves on the free polynomial generators ϵ_a of $\Lambda^\star$.*

1.5 Lyndon-Witt functions

We put in formula (11):

$$(m) := \sum_{d|m} d w_d^{m/d}, m \geq 1. \tag{20}$$

Taking into account that we consider the ϵ_n as elementary symmetric functions in, for example, the quantities $x_d, (d \in \mathbb{N}_+)$, we may write in view of lemma 1.1

$$\begin{aligned}
\prod_{d=1}^{\infty}(1+x_d t) = \sum_{n=0}^{\infty}\epsilon_n t^n \quad &= \quad \exp\left(\sum_{m=1}^{\infty} m^{-1}(-1)^{m+1}\sum_{d|m} d w_d^{m/d} t^m\right) \\
&\overset{m=ad}{=} \quad \exp\left(-\sum_{a,d=1}^{\infty} a^{-1} w_d^a (-t^d)^a\right) \\
&= \quad \exp\circ\log\left(\prod_{d=1}^{\infty}(1-w_d(-t)^d\right) \\
&= \quad \prod_{d=1}^{\infty}\left(1-w_d(-t)^d\right)
\end{aligned} \tag{21}$$

This computation has as immediate consequence:

Corollary 1.5 a. *We have*

$$\epsilon_n = \sum_{\lambda \in \mathsf{Part}_n^{dp}} (-1)^{l(\lambda+n} w_\lambda,$$

in particular

b.

$$\Lambda^\star = \mathbb{Z}[\epsilon_n | n \geq 1] = \mathbb{Z}[w_d | d \geq 1].$$

c. *The comultiplication Δ on the free generators w_d is determined by the formula*

$$\prod_{d=1}^{\infty}(1-)\Delta(w_d)(-t)^d) = \prod_{d=1}^{\infty}(1-)(w_d \otimes 1)(-t)^d) \cdot \prod_{d=1}^{\infty}(1-)(1 \otimes w_d)(-t)^d).$$

Proof. The first assertion is a direct consequence of

$$\epsilon_n = \sum (-w_1)(-w_2)\cdots(-w_k)(-t)^{d_1+d_2+\cdots+d_k},$$

where the sum is taken over all partitions $(d_1, d_2, \cdots, d_k)$ of n into *different parts*. Observing, that

$$\sum_n \Delta(\epsilon_n) = \sum_n \sum_{a+b=n} \epsilon_a \otimes \epsilon_b = \sum_n (\epsilon_n \otimes 1)) \cdot \sum_n (1 \otimes \epsilon_n),$$

the remaining assertion is clear. □

Application to QSym Define for every $a \in \mathbb{N}_+$ and every composition $c = (c_1, \ldots, c_k)$, the composition $a\#c := (ac_1, \ldots, ac_k)$. This definition gives rise to an endomorphism of abelian groups $\#a : \mathsf{QSym} \to \mathsf{QSym}$. This definition implies

Lemma 1.6 a. *The transpose of $a\#$ on $\mathcal{Z}$ is the Verschiebung, determined by*

$$v_a(z_n) = \begin{cases} z_{n/a} & \text{if } a|n \\ 0 & \text{otherwise} \end{cases}.$$

In particular, the endomorphisms $\#a$ are Hopf algebra endomorphisms of QSym.

b. For all $a, b \in \mathbb{N}_+$ one has $a\# \circ b\# = (ab)\#$.

Next let $l = (l_1, \ldots, l_k) \in \mathcal{L}$ be a reduced Lyndon word, i.e. $\gcd(l) = \gcd\{l_1, \ldots, l_k\} = 1$ and define

$$m\#l =: \sum_{d|m} d w_{d\#l}^{m/d}, m \geq 1. \tag{22}$$

We denote $\mathcal{L}_{red}$ the set of all reduced Lyndon words. Then

$$\mathcal{W} := \{w_{m\#l} | l \in \mathcal{L}_{\text{red}}, m \geq 1\} = \{w_\lambda | \lambda \in \mathcal{L}\}$$

Elements of the set $\mathcal{W}$ will be called *Lyndon-Witt functions*. The term comes from the theory of (global) Witt vectors as follows: for $k \in \mathsf{CUR}$, let $W(k)$ be the set of all *Witt vectors* $\underline{x} = (x_1, x_2, \ldots, x_m, \ldots)$ with components $x_m \in k$.

$$w_m(\underline{x}) := \sum_{d|m} d x_d^{m/d}, m \geq 1.$$

$W(k)$ then is itself a commutative unitary ring by means of the generic condition

$$w_m(\underline{x}) * w_m(\underline{y}) =: w_m(\underline{x * y}), m \geq 1,$$

where $* \in \{+, \cdot, -\}$. In this optic, the Witt vector $\underline{w_l}$ with the Lyndon-Witt quasisymmetric functions $w_{m\#l}$ as components, has the Lyndon compositions $m\#l$ as ghost components. We will soon see that this Witt vector

actually lies in $W(\mathsf{QSym})$, (as opposed to $W(\mathsf{QSym}\otimes\mathbb{Q}$. In fact, let $l\in\mathcal{L}$ be a Lyndon word, not necessarily reduced. Replace x_d by $x_{d,l}$, ϵ_n by $\epsilon_{n,l}$ and w_d by $w_{d,l}$ in formula (21) in order to have the relation

$$\prod_{d=1}^{\infty}(1+x_{d,l}t)=\sum_{n=0}^{\infty}\epsilon_{n,l}t^n=\exp\left(\sum_{m=1}^{\infty}m^{-1}(-1)^{m+1}(m\#l)t^m\right)=\prod_{d=1}^{\infty}\left(1-w_{d,l}(-t)^d\right). \tag{23}$$

It is convenient to use again the "trick of Cartier": replace t in (23) by $\zeta_a^i t$ and multiply over $0\le i\le a-1$. The result may be written in the form

$$\begin{aligned}\prod_{d=1}^{\infty}\prod_{i=0}^{a-1}(1+x_{d,l}\zeta_a^i t) &= \prod_{i=0}^{a-1}\sum_{n=0}^{\infty}\epsilon_{n,l}(\zeta_a^i t)^n\\ &= \exp\left(\sum_{m=1}^{\infty}m^{-1}(-1)^{m+1}(m\#l)\sum_{i=0}^{a-1}(\zeta_a^{im})t^m)\right)\\ &= \prod_{i=0}^{a-1}\prod_{d=1}^{\infty}\left(1-w_{d,l}(-\zeta_a^i t)^d\right). \end{aligned}\tag{24}$$

As before we eliminate the roots of unity and find

$$\begin{aligned}\prod_{d=1}^{\infty}(1+x_{d,l}^a t^a)=\sum_{n=0}^{\infty}\epsilon_{n,l,a}(-t)^n &= \exp\left(\sum_{N=1}^{\infty}(aN)^{-1}(-1)^{aN+1}\left(\sum_{d|aN}dw_{d\#l}\right)at^{aN}\right)\\ &\equiv \prod_{d=1}^{\infty}\left(1-w_{1,l}^a t^a\right). \end{aligned}\tag{25}$$

Since the exponential has coefficients in $\mathbb{Q}$ and the ϵ-series has coefficients in $\mathbb{Z}[\zeta_a]$, the resulting relation is, in fact, defined over $\mathbb{Z}$. In particular, for the exponential series E_a in (25) we see it to be

$$\begin{aligned}E_a = &= \exp\left(-\sum_{N=1}^{\infty}N^{-1}(-1)(aN\#l)t^{aN}\right)\\ &\equiv \exp\left(-\sum_{N=1}^{\infty}\frac{(w_{a\#l}t^a)^N}{N}\right)\\ &\equiv 1-w_{a\#l}t^a \qquad (26)\\ &\equiv 1-(-t)^a w_{a\#l}\ \mod\ \text{words of length } > \text{ length of } l. \qquad (27)\end{aligned}$$

In the following corollary we collect some consequences of the foregoing observations

Corollary 1.7 a.

$$\begin{aligned}\epsilon_{n,l} &= \sum_{k\geq 0; d_1<\ldots d_k} (-1)^n(-w_{d_1,l})(-w_{d_2,l}\cdots(-w_{d_k,l}) \\ &= \sum_{d\in \mathsf{Part}_n^{\mathrm{dp}}} (-1)^{|d|+l(d)} W_{d,l}. \qquad (28)\end{aligned}$$

$$(29)$$

(Here, the second sum is to be interpreted as a shorthand for the first sum.)

b. *In particular, if $M(\mathcal{W})$ is the set of all monomials in the Lyndon-Witt quasisymmetric functions, we let $\Delta(\mathcal{W})$ be the set of decomposable elements with respect to the elements of $\mathcal{W}$. Then*

$$\epsilon_{n,l} \equiv (-1)^{n+1} w_{n,l} \bmod \Delta(\mathcal{W}).$$

c.

$$\Lambda^\star = \mathbb{Z}[w_d | d \geq 1],$$

the free polynomial ring in the symmetric Lyndon-Witt functions w_d, $(d \geq 1)$.

d.

$$\mathsf{QSym}_{\mathbb{Q}} = \mathbb{Q}[\mathcal{W}],$$

the free polynomial ring, generated over $\mathbb{Q}$ by the Lyndon-Witt quasisymmetric functions.

e.

$$\mathbb{Z}[\mathcal{W}] \subset \mathsf{QSym}$$

is a Hopf subalgebra of QSym.

Proof. From **??**XXX) we see that $\Lambda^\star = \mathbb{Z}[\epsilon_m | m \geq 1] = \mathbb{Z}[w_d | d \geq 1]$. Moreover, $\Lambda^\star$ has a canonical embedding in QSym. □

Returning to formula (22) of [DS], it is clear that by part e. of the corollary we may conlude that $\mathbb{Z}[\mathcal{W}] = \mathsf{QSym}$, if we can prove that

$$\{(m\#l)^e | l \in \mathcal{L}_{\mathrm{red}}, m \geq 1\} \subset \mathbb{Z}[\mathcal{W}]. \qquad (30)$$

If $e = 1$, then $m\#l = w_{1,l} = l$ is a Lyndon word and belongs by definition to $\mathcal{W}$. If $e > 1$, we recall the situation of $\Lambda^\star$, where the curve $F_a e$ appeared to be the canonical curve - up to sign - on the free polynomial generators e_1^a, i.e. $F_a e$ contains $\epsilon_a = e^{(1^a)}$, defined by the partition (1^a), conjugate to (a). In the following sections we analyze this phenomenon in more detail,

but introduce already now the relevant notations. Since $\mathsf{QSym}_{\mathbb{Q}} = \mathbb{Q}[\mathcal{W}]$, the completion has canonical curves, denoted $\zeta_l = \sum_{n=0}^{\infty} \zeta_{l,n} t^{n|l|}(, l \in \mathcal{L})$, satisfying

$$\forall l, m \in \mathcal{L} : \zeta_l(w_m) = \delta_{l,m} t^{|l|}. \tag{31}$$

Moreover, as a vector space over $\mathbb{Q}$, the set $M(\mathcal{W})$ is a basis, and the dual basis will be denoted $\Pi = \{\pi_W | W \in M(\mathcal{W})\}$. This basis consists of point distributions on the monomials in the Lyndon-Witt functions. Notice, the canonicality of the curve ζ_l implies the relations

$$\forall n \geq 0 : \zeta_{l,n} = \pi_{l^n}.$$

Moreover, it is clear that

$$\mathcal{B} := \{\beta_l := \zeta_{l,1} = \pi_l | l \in \mathcal{L}\}$$

is a $\mathbb{Q}$-vector space basis for the lie algebra of primitive elements in $\mathsf{QSym}_{\mathbb{Q}}$. A priori, all these objects live in $\mathsf{QSym}_{\mathbb{Q}}$, but we intend to prove, that all these objects have all their coefficients in QSym. Given any $l \in \mathcal{L}_{\mathrm{red}}$, there is an endomorphism of the Hopf algebra $\mathcal{Z}_{\mathbb{Q}}$, f noncommutative symmetric functions over $\mathbb{Q}$, denoted ζ_l and determined by the fact that ζ_l is a curve, i.e. by

$$\forall n \geq 0 : \zeta_l(z_n) := \zeta_{l,n} = \pi_{l^n}.$$

Of course, by duality there is a transposed endomorphism $\zeta_l^\star$ of the Hopf algebra $\mathsf{QSym}_{\mathbb{Q}}$.

1.6 Formulae in small weight

We list the quasisymmetric functions in weight ≤ 4. For weights ≥ 5 see the appendix. For each composition (c) of length k, we let $s(c) \in \Lambda^\star$ be the sum of the elements in the orbit of c under the natural action of the symmetric group SS_k.

For more data one might wish to visit the web site www.cs.vu.nl/∼ejd/qslw

composition	corresponding Lyndon-Witt function
(1)	w_1
(2)	$2w_2 + w_1^2$
(11)	$-w_2$
(3)	$3w_3 + w_1^3$
(12)	w_{12}
(21)	$2w_1w_2 - 3w_3 - w_{12}$
s(21)	$2w_1w_2 - 3w_3$
(111)	$w_3 - w_1w_2$
(4)	$4w_4 + 2w_2^2 + w_1^4$
(13)	w_{13}
(22)	$w_2^2 + 2w_2w_1^2 - 2w_4$
(31)	$3w_1w_3 - 4w_4 - 2w_2^2 - w_{13}$
s(31)	$3w_1w_3 - 4w_4 - 2w_2^2$
(112)	w_{112}
(121)	$w_{12}w_1 - w_{13} - w_2^2 - 2w_2w_1^2 + 2w_4 - 2w_{112}$
(211)	$w_2^2 + w_2w_1^2 + w_{13} - 3w_1w_3 + 2w_4 + w_{112} - w_{12}w_1$
s(211)	$-w_2w_1^2 - 3w_1w_3 + 4w_4$
(1111)	$-w_4 + w_1w_3$

2 Quasi-symmetric functions

In this section, the notion of "symmetric" will be combined with a "total order as follows: let $n > k$ and let $f =\in B$ and write f in full:

$$f = \sum_{x_1,\dots,x_k} \lambda_{c_1,\dots,c_k}\lambda_{(c)}x_1^{c_1}\cdots x_k^{c_k}.$$

f will be called *quasi-symmetric* if the following is true: if $c = (c_1 \dots c_k)$ and $d = (d_1 \cdots d_k)$, then the coefficients λ_c and λ_d are the same. For example, $x_1x_2^2+x_1x_3^2+x_2x_3^2$ is quasi-symmetric and will be denoted in an obvious way: $f = (1, 2)$. Every sequence c determines a unique quasi-symmetric function, the *monomial quasi-symmetric function*, denoted M_c. Clearly, symmetric functions are quasi-symmetric. Sum and product of quasi-symmetric functions are quasi-symmetric, hence the set of quasi-symmetric functions in B is a commutative unitary ring $\mathsf{QSym}^{(n)}$ containing $\Lambda^{(n)}$ as a subring. The ring structure on QSym is given as follows: call a sequence $c = (c_1, \dots, c_k)$ of positive natural numbers a *composition* and Comp the set of all of them. A composition c such that the gcd of all its digits is 1 is called a *reduced* composition. Concatenation of compositions c and d will be denoted $c * d$. Introduce an *empty* composition () and define for nonempty compositions $c = (c_1, \dots c_k)$ the composition $\hat{c}$ by $c = c_1 * \hat{c}$, thus $\hat{c}$ is the longest nontrivial tail of c. The multiplication $\uplus$ in QSym is given by the rules: () acts as

neutral element 1 and

$$\forall c, d \in \mathsf{Comp} : c \uplus d := c_1 * (\hat{c} \uplus d) + d_1 * (c \uplus d\hat{d}) + (c_1 + d_1) * (\hat{c} \uplus \hat{d}). \tag{32}$$

2.1 Lyndon compositions

A composition $c = (c_1, \dots c_k)$ is called a *Lyndon composition* if in the phone book of all compositions, ordered "alphabetically" every proper tail of c may be found, **properly further than c**. For instance, my postgiro account number 1189189 defines a Lyndon composition. Concatenated with my (secret) bank account number on the Bahamas, 189327592, we get the Lyndon (1,1,8,9,1,8,9,1,8,9,3,2,7,5,9,2), still concatenating it with my pincode 1188 will involve loss of Lyndonacity, but with 1199 will conserve this property.. The theorem of Radford, [Rad] states:

Theorem 2.1 *If* $\mathsf{QSym}_{\mathbb{Q}}$ *denotes the commutative unitary ring of quasi-symmetric functions over the rational number* $\mathbb{Q}$*, then*

$$\mathsf{QSym}_{\mathbb{Q}} = \mathbb{Q}[\mathcal{L}],$$

the polynomial ring, freely generated over $\mathbb{Q}$ *by the set* $\mathcal{L}$ *of Lyndon compositions.*

Now I come to the main topic of my conference: it is easily verified, that the assertion:

$$\mathsf{QSym} = \mathbb{Z}[\mathcal{L}]$$

is false and in the early eighties of the last millenium I studied the structure of QSym in [D85]. Instead of the Lyndon compositons, I considered the set $\mathcal{L}^{\mathrm{mod}}$ of *modified Lyndon compositions*, as follows: a Lyndon composition c has a $\gcd(c)$ of all its digits and putting for a composition $c = (c_1, \dots, c_k)$ and a natural number a:

$$a\#c = (ac_1, \dots ac_k),$$

it is clear that $c_{\mathrm{red}} := \gcd(c)^1\#c$ ia a composition as well, hence the gcd-fold concatenation $c_{\mathrm{red}}^{*\gcd(c)}$ is still a composition, called a modified Lyndon composition, if c is Lyndon. Thus, *modification*: $\mu : \mathsf{Comp} \to \mathsf{Comp}$ is a well defined operation that can be compared to - and in fact is identical with - the transition from partitions to conjugate partitions in the theory of symmetric functions. As an example, (4) is Lyndon, and modifying it gives $(1)^{*4} = (1, 1, 1, 1)$. In loc cit. I announced the theorem

$$\mathsf{QSym} = \mathbb{Z}[\mathcal{L}^{\mathrm{mod}}] \tag{33}$$

and was happy to see that all compositions of weight ≤ 9 are unique polynomials in the modified Lyndon words with integer coefficients. As the

number of compositions of weight n is equal to 2^{n-1}, I had 255 polynomials with integral coefficients - data that I supposed to be sufficient material for illustration.

2.2 Lyndon-Witt functions

As usual, compositions of weight 1 are trivial to deal with. For weight 2 one sees by inspection $(1,1)$ to be a free generator. The case weight=3 is a job of 5 minutes, but weight 4 already asks for some 10 minutes. The growth time complexity seems to be exponentially, at any rate, much time has been spended in making a list. Let $l \in \mathcal{L}$ be an arbitrary reduced composition, for instance a *reduced Lyndon word* and $m > 1 \in \mathbb{N}$. Define recurrently

$$m\#r = \sum_{d|m} dw_{d\#r}.$$

The notation is chosen such that no confusion may arise with an element mr, belonging to the free abelian group on the set Comp of all compositions. Noticing every $l \in \mathsf{Comp}$ to have the unique form $l = m\#r$, the totality of all compositions is covered by this definition. Moreover, let us consider the following little computation:

$$\begin{aligned}
\sum_{i=0}^{\infty} \epsilon_{r,i} t^i &:= \exp\left(\sum_{m=1}^{\infty} m\#r \frac{t^m}{m}\right) \\
&= \exp\left(\sum_{m=1}^{\infty}\sum_{d|m} dw_{d\#r} \frac{t^m}{m}\right) \\
&= \exp\left(\sum_{a=1}^{\infty}\sum_{d=1}^{\infty} dw_{d\#r} \frac{(t^a)^d}{ad}\right) \\
&= \exp\left(\sum_{d=1}^{\infty} \log\left(1 - w_{d\#r}(t^d)\right)^{-1}\right) \\
&= \prod_{d=1}^{\infty}\left(1 - w_{d\#r} t^d\right)^{-1},
\end{aligned} \tag{34}$$

in order to show that $\mathbb{Z}[\epsilon_{r,i}, i \geq 1] = \mathbb{Z}[w_{d\#r} | r \in \mathbb{N}_+]$. This does not imply this ring to be a subring of QSym, but a little generalization of the theorem of Dieudonn´ Dwork, concerning integrality of exponential series guarantees this indeed to be the case, [Di02b] The particular set $(w_l, l \in \mathcal{L})$ will be called the set of *Lyndon-Witt functions* and from what has been said, we have

$$\mathcal{W} \subset \mathsf{QSym}\,.$$

. For $l = (m)$, they were introduced in the context of symmetric functions by Reutenauer in [Reut95, (2.1)]. In the preprints [Di02a] and [Di02b], I announced and sketched the proof of the first statement of

Theorem 2.2 Basis theorem for quasi-symmetric functions.

a. $\mathsf{QSym} = \mathbb{Z}[\mathcal{W}]$, *the polynomial ring over* $\mathbb{Z}$, *freely generated by the Lyndon-Witt functions.*

b. *There are isobaric curves, i.e.homomorphisms of commutative unitary rings or equivalently, infinite sequences of sequences of divided powers* $\mathsf{QSym} \to \mathbb{Z}[[t]]$, *denoted* $\gamma_l = \sum_{i=0}^{\infty} \gamma_{n,l} t^{|l|n}$ *which are canonical curves on the set* $\mathcal{W}$ *i.e.*

$$\forall w_l, w_{l'} \in \mathcal{W} : \gamma_{w_l}(w_{l'}) = \delta_{l,l'} t^{|l|}.$$

The set of all such curves will be denoted Γ.

ca. *(Trivial Hilbert version) The map* $\prod_{l\in\mathcal{L}} \gamma_l^{e_l} \mapsto (e_l | l \in \mathcal{L})$ *induces a bijection*

$$\mathcal{E}^{\mathsf{h}} \to \mathbb{N}^{\mathcal{L}}.$$

Moreover, such a homogeneous endomorphism is an automorphism if and only if $e_1, e_2 \in \{\pm 1\}$.

ca. *(Witt version) The map* $\prod_{l\in\mathcal{L}} [e_l]\gamma_l \mapsto (e_l | l \in \mathcal{L})$ *induces a bijection*

$$\mathcal{E}^{\mathsf{h}} \to \mathbb{N}^{\mathcal{L}}.$$

Moreover, such a homogeneous endomorphism is an automorphism if and only if $e_1, e_2 \in \{\pm 1\}$.

Example
The Hilbert structure and Witt structure on curves are different, the former being somewhat simpler in general. We found for the curve z^2 for example

$$z^2 = [2]z \cdot (\gamma_2\gamma_{12}^5\gamma_{13}^{-2}\gamma_{112}^{-10}\gamma_4^4\gamma_{113}^{13}\gamma_{1112}^{15}\gamma_5^{-6}\gamma_{113}^{-20}\gamma_{122}^{-18}\gamma_{114}^{29}\cdots)^{-1}$$

decomposition.

Corollary 2.3 *Every finite sequence of divided powers* $(x_0 = 1, x_1, \ldots, x_n)$ *can be extended to an infinite sequence.*

Proof. We summarize the proof in [Di02b]. Since then it appeared that use of plethysms and λ-rings allowed a simplification of the proof, since the use of a basis of primitive elements in the graded dual $\mathsf{QSym}^{*\mathrm{gr}}$ of QSym can be avoided. Since, however, this graded dual of QSym may be identified with the Hopf algebra of noncommutative symmetric functions, [MR, ??],

it remains a matter of taste, which kind of arguments is to be preferred. Using the commutator curves of [Shay] and a decomposition theorem for the 2-curve $\sum_{i=0}^{\infty} z_i(t_1+t_2)^i$, Hazewinkel proved in [Haz01, th 4.24, p 19], that $\mathcal{P}(\mathcal{Z})$ has a totally ordered basis $\mathcal{H} = \{h_l | l \in \mathcal{L}\}$, indexed by the set of Lyndon words and such that

$$h_l \equiv \gcd(l) z_l \text{ mod terms having length } > \text{length of } l.$$

We already mentioned in the foregoing discussion the fact

$$\mathcal{W} \subset \mathsf{QSym}$$

and, moreover, if $< -, - >: \mathsf{QSym} \otimes \mathcal{Z} \to \mathbb{Z}$ is the canonical duality pairing, then in view of lemma **??**.b we have for $l \geq m$ in $\mathcal{L}$:

$$< h_l, w_m > = < \gcd(l) z_l, w_m > = < z_l, \gcd(m) w_m > = < z_l, l > \overset{(*)}{=} \delta_{l,m}.$$

Here, δ is the Konecker delta. We used the fact $\gcd(m)m \equiv w_m$ modulo decomposable elements in $\mathcal{W}$ and that primitives in $\mathcal{Z}$ are zero on decomposable elements in QSym. Moreover we used the fact that h_l has z_l as *leading term*, hence possible terms having the form $c_n z_n$,r with $c_n \neq 0$ and $n \in \mathcal{L}$ satisfy $n > l$, consequently, $n > m$. Notice that there is no reason (and neither necessity) to suppose that both bases are dual bases, triangularity is sufficient. At any rate, we deduce by triangularity that the Lie algebra $\mathcal{P}(\mathcal{Z})$ of primitive elements can be transformed into a $\mathbb{Z}$-module basis $\mathcal{P} = \{\pi_l | l \in \mathcal{L}\}$ of homogeneous primitives,

$$\pi_l = \sum_{c \in \mathsf{Comp}} \lambda_{l,c} z_c, \tag{35}$$

having the property (P): $c \neq l, c \in \mathcal{L} \Rightarrow \lambda_{l,c} = 0$. It then is clear that $\mathcal{P}$ is the basis dual to the basis $\mathcal{W}$ of J/J^2 in $\mathsf{QSym}_{\mathbb{Q}}$, where J is the canonical augmentation ideal of $\mathsf{QSym}_{\mathbb{Q}}$. Since $\mathcal{P}$ is a basis for the primitives of $\mathcal{Z}$ over $\mathbb{Z}$, the dual QSym is the free polynomial ring, generated over $\mathbb{Z}$ by the Lyndon-Witt functions. □

Corollary 2.4 *Since pure primitives are canonical and $\mathcal{W}$ is dual to this basis, we consider $\mathcal{W}$ as canonical generators for* QSym.

Remark
Hazewinkel noticed that by using plethysms of quasi-symmetric functions, introduced by Reutenauer and Malvenuto in [**?**], one can define

$$A_\alpha = p_n \circ \alpha$$

to see at once that A_l coincides with my w_l *and is defined in* QSym , but (34) gives a direct relation with Witt vectors.
Remark It is clear that if one considers the Lyndon words as a canonical tool for the description of the structure of QSym , then so are the pure primitives $\pi_l, (l \in \mathcal{L})$, equally indexed by the Lyndon words, and containing only *one* nonzero term, involving z_l with $l \in \mathcal{L}$. As is the case by the commutative symmetric functions, the four automorphisms of the Hopf algebra Λ, induced by the curves $e, e^{-1}, [-1]e$ and $h = [-1]e^{-1}$ extend to $\mathcal{Z}$ by replacing e by the (noncommutative) canonical curve z. It then is clear, that the basis of $\mathcal{P}(\mathcal{Z})$, dual to the basis defined by the complete noncommutative symmetric functions, has the property, that every primitive, indexed by $l \in \mathcal{L}$, contains every $z_m, m \in \mathcal{L}, m > l$ with nonzero coefficient.

Modified Lyndon words What about the statement $\mathsf{QSym} = \mathbb{Z}[\mathcal{L}^{\mathrm{mod}}]$, published in [DS, thm 1.5] Here, under reference to a maxim, attributed to the former president Clinton[3]. I confess to bear the responsability for the error (33): it is true that QSym is freely generated over the field of rational numbers by the set of quasi-symmetric functions, indexed by modified Lyndon compositions. The error was noted by Hazewinkel (email) and Reutenauer, (private correspondence). It was only recently that I found (3,6) to be the counter example of lowest weight in $\mathbb{Z}[\frac{1}{7}][\mathcal{L}^{\mathrm{mod}}] \setminus \mathbb{Z}[\mathcal{L}^{\mathrm{mod}}]$. For this, see
LYNDON-WITT FUNCTIONS AND THE STRUCTURE OF QSYM erratum

3 Noncommutative symmetric functions

In the definitions given sofar, one can eliminate the noise, aroused by the parameter n, the number of x_i, used to define the symmetric functions and the quasi-symmetric functions. Technically: one takes the projective limit in the category of graded algebras and considers the object $\Lambda = \mathbb{Z}[e_i | i \geq 1]$. It is quite natural to introduce the noncommutative analog of Λ, in fact define as in [D72]

$$\mathcal{Z} = \mathbb{Z}\langle z_i | i \geq 1 \rangle,$$

the free polynomial ring over the integers in the noncommuting quantities $z_i, (i \geq 1)$. It is a graded Hopf algebra, if one defines the grading ω by $\omega(z_n) := n$ and the comultiplication Δ by

$$\forall n \geq 0 : \Delta(z_n) = \sum_{a+b=n} z_a \otimes z_b, \quad (z_0 := 1).$$

[3]To make errors is itself not an error. It is an error not to admit them

The object $\mathcal{Z}$ has been called the *Leibniz Hopf algebra*, since it represents generically the *Leibniz relations*: for a sequenece $z_i, (i \geq 0)$ one has for all arguments x, y:

$$z_n(xy) = \sum_{a+b=n} z_a(x) z_b(y).$$

A typical example is given by: let δ be a differentiation and substitute z_n by $\frac{\delta^n}{n}$. For this reason $\mathcal{Z}$ has been called too the Hopf algebra of *sequences of divided powers*. To be precise, a sequence

$$x = (x_0, x_1, \dots, x_n, \dots) \tag{36}$$

in a Hopf algebra of $H = (H, \Delta, \epsilon, \mu, \eta, S)$ is a subset of H such that

$$\forall n \geq 0 : \Delta(x_n) = \sum_{a+b=n} x_a \otimes x_b. \tag{37}$$

For each such sequence, denote $\overline{x}$ the generating series

$$\overline{x} = \sum_{i=0}^{\infty} x_i t^i,$$

The set of all such sequences is a group, such that the map $x \mapsto \overline{x}$ is a homomorphism of groups. Moreover this group is semidirect product of the subgroup $G(H)$, consisting of all sequences x with $i > 0 \Rightarrow x_i = 0$ and a normal subgroup characterized by $\overline{x} : x_0 = 1$. This normal subgroup is called the *group of curves in* H, denoted $\mathsf{SDP}(H)$. An obvious generalization of the notion of curve or sequence of divided powers is to consider instead of (36), sequences of elements $x = (x_\alpha | \alpha \in \mathsf{MI}(E))$, indexed by the set of multi-indices $\mathsf{MI}(E)$ for an arbitrary set E. Then consider the group $\mathsf{SDP}_E(H)$ of such elements with generating series $\overline{x}$ and group structure, induced by multiplication of formal power series in the set of variables $\{t^\alpha | \alpha \in \mathsf{MI}(E)\}$. An SDP-*Hopf algebra of type* E is a Hopf algebra, such that SDP_E has an element $\overline{x}$, such that $\{x_\alpha | \alpha \in \mathsf{MI}(E))\}$ is a basis for H. It is not obvious that both $\mathcal{Z}$ and Λ are SDP-Hopf algebras of type $\mathbb{N}_+$.

3.1 The Lie algebra $\mathcal{P}(\mathcal{Z})$

Definition 3.1 Let l be a Lyndon word and consider the following condition on a homogeneous primitive $\delta \in \mathcal{P}(\mathcal{Z})$ of weight $n \geq 1$:

$$\delta = \sum_{w \in \mathsf{Comp}_n} c_w z_w, \qquad (c_w \in \mathbb{Z}).$$

If $w \in \mathcal{L}$ has weight n, then the coefficient c_w of z_w is equal to $\gcd(l)\delta_{l,w}$. i.e. l is the *only* Lyndon word, having nonzero coefficient $\gcd(l)$ in δ.

A primitive satisfying this condition is called an *l-pure primitive*. Obviously, an l-pure primitive is unique, since the difference of two such do not contain any z_l with $l \in \mathcal{L}$ with nonzero coefficient.

Theorem 3.2 *There exists a basis for the Lie algebra $\mathcal{P}(\mathcal{Z})$ consisitng of pure primitives.*

Corollary 3.3 *Two bases of $\mathcal{P}(\mathcal{Z})$, consisting of pure primitives, coincide.*

Corollary 3.4 *Let $J = \mathrm{Ker}\,(\epsilon)$ in QSym, thus $\mathsf{QSym} = \mathbb{Z} \oplus (J/J^2) \oplus J^2$. There is exactly one set of generators $\mathcal{W} = \{w_l | l \in \mathcal{L}\}$ for QSym, having the property that the restriction of a pure basis for the primitives $\mathcal{P}(\mathcal{Z})$ to J/J^2 is the dual basis of the basis of images of $\mathcal{W}$ in J/J^2.*

Theorem 3.5 *The unique set of generators $\mathcal{W}$ satisfies: if $r \in \mathcal{L}$ is reduced, then*

$$w_r = r.$$

If $l \in \mathcal{L}$ has $\gcd(l) = n > 1$, and $r = r_{\mathrm{red}}$. then

$$l = \sum_{d|n} d w_{d\#r}^{n/d}.$$

In pure primitives, we have files, containing pure primitives.

3.2 The goup of curves

Let k be a base ring and $H \in \mathsf{Hopf}_k$. It is clear that the group of sequences of divided powers in H, thus $\mathsf{SDP}(H)$ may be identified canonically with

$$\mathsf{Hopf}_k(\mathcal{Z}_k, H) \cong SDP(H).$$

Taking $k = \mathbb{Z}$ and $H = \mathcal{Z}$, we thus have

$$\mathsf{Hopf}(\mathcal{Z}, \mathcal{Z}) \cong SDP(\mathcal{Z}).$$

The subgroup of homogeneous endomorphisms of $\mathcal{Z}$ will be denoted $\mathcal{E}^{\mathsf{h}}$. There are various descriptions of the group $\mathcal{E}^{\mathsf{h}}$.

3.3 Gelfand and his school

It was not detected until 1995 by Gelfand and his school, [Gea], that there is every reason to call $\mathcal{Z}$ the Hopf algebra of the *noncommutative symmetric functions*. The introduction of noncommutative symmetric functions as done by Gelfand and his school asks - perhaps - for somewhat more justification: is there an action of the symmetric group on $\mathcal{Z}$, (or related to $\mathcal{Z}$), for which these are invariant? If so, do we have elementary noncommutative symmetric functions, complete noncommutative symmetric functions, noncommutative Schur functions and so on?. The first obstacle to be met is the problem: what about the enormous amount of determinants in the theory of commutative symmetric functions and the lack of a (classical) theory of matrices with entries in a noncommutative ring, for instance, does there exists a Cramer rule for a linear system of equations between noncommuting operators and complex coefficients? The answer, fortunately, is positive, as shown by Gelfand and Retakh in [GR2]. Thanks to [Gea] there exists already an abundant amount of literature on such functions, but as one may observe, the body of the theory is about noncommutative symmetric functions over a field of characteristic 0, instead of (arithmetically) over the integers[4].

3.4 Short summary

We first recall the important generalization of determinants to *quasi-determinants*. Let K be a field, n an integer and $A = \{a_{ij}, |1 \leq i, j, \leq n\}$ a set of n^2 noncommutative indeterminates. Let $K\{< A\} >$ be the free field eonstructed on K and generated by A. The quasi-determinant $|A|_{pq}$ of order pq of the generic matrix A is the element defined by

$$|A|_{pq} = a_{pq} - \sum_{i \neq p, j \neq q} a_{pq} \left((A^{pq})^{-1} \right) a_{pq}. \tag{38}$$

The component of degree n is denoted $\mathcal{Z}_{(n)}$. Clearly, if one passes to the largest abelian quotient of $\mathcal{Z}$ modulo the two-sided ideal, generated by all commutators $[z_i, z_j] = z_i z_j - z_j z_i$, it is clear that one recovers Λ. But far much more is true as well: As every graded Hopf algebra one may construct its graded dual. For our $\mathcal{Z}$ this graded dual is defined by

$$\mathcal{Z}^{*\mathrm{gr}} := \oplus_{n \geq 0} \left(\mathcal{Z}_{(n)}^{*} \right).$$

The following result is classical:

Theorem 3.6 *There is a canonical isomorphism of Hopf algebras*

$$\Lambda \cong \Lambda^{*\mathrm{gr}}.$$

[4] God made the integers, the rest is work of man, Kronecker

First of all we have the following theorem of Malvenuto-Reutenauer, [MR, ??]:

Theorem 3.7 *There is a canonical isomorphism of Hopf algebras*

$$\mathsf{QSym} \cong \mathcal{Z}^{*\mathrm{gr}} \text{ and } \mathcal{Z} \cong \mathsf{QSym}^{*\mathrm{gr}}.$$

given by the relations

$$\sum_{m=0}^{\infty} M_{(m)} t^m = \exp\left(p_m \frac{t^m}{m}\right).$$

Here, $M_{(i)}$ is the monomial quasi-symmetric function, defined earlier.

3.5 Multicurves and Newton relations

Recall that the set of *primitive elements* $\mathcal{P}(H)$ in a Hopf algebra H, that is $\mathcal{P}(H) = \{h \in H : \Delta(h) = h \otimes 1 + 1 \otimes h\}$ is a Lie algebra under the bracket $[h, h'] := hh' - h'h$. Let E be a set and consider subsets

Z. $Z = \{z_\alpha : \alpha \in \mathsf{MI}(E)\}$, with $z_0 = 1$,

R. $R = \{\rho_\alpha : \alpha \in \mathsf{MI}(E)\}$, with $\rho_0 = 0$,

X. $X = \{x_\alpha : \alpha \in \mathsf{MI}(E)\}$, with $x_0 = 0$ of H.

For convenience assume H to be a Hopf algebra over $\mathbb{Q}$. Consider equally expressions

$$\overline{z} := \sum_{\alpha \in \mathsf{MI}(E)} z_\alpha t^\alpha = \exp\left(\sum_{\alpha \in \mathsf{MI}(E)\setminus\{0\}} x_\alpha \frac{t^\alpha}{|\alpha|}\right). \tag{39}$$

$$\forall \alpha \mathsf{MI}(E) : \Delta(z_\alpha) = \sum_{\beta+\gamma=\alpha} z_\beta \otimes \gamma. \tag{40}$$

$$\forall \alpha : |\alpha| x_\alpha = \sum_{\beta+\gamma=\alpha} x_\beta \rho_\gamma. \tag{41}$$

We have the following relations between these elements:

Theorem 3.8 *The set Z defines a curve of type E if and only if the set X is a subset of the Lie algebra $\mathcal{P}(H)$. Moreover, in this case, the set R satisfying (41) is a subset of $\mathcal{P}(H)$, and conversely, define the set $R \subset \mathcal{P}(H)$ by the relation (41), then Z defines a multicurve. The relations (41) are called the* right Newton relations *or* primitives of the first kind *and the primtives, defined by (39) are the* primitives of the second kind. *If necessary, we write $\rho_\gamma(x)$ and $\rho(x)$ instead of ρ_γ and ρ. If necessary, we write $r_\gamma(x)$ and $r(x)$ instead of r_γ and r.*

More about multi-curves and a decomposition theorem for them see
In order to facilitate the translation of fifferent notations in literature, we give the following table

[Gea]	l	[McD79] comm	l	ours
$\lambda(t)$	(21)	$e(t)$		$z = z(t)$
$\sigma(t)$	(22)	$h(t)$		$n = n(t)$
Ψ_k	(23)	–		$\rho_k(n(t))$
Φ_k	(26)	–		$r_{[-1]z^{-1}{}_k} =: r_k$

One has the following relations between these quantities

$$z(t) = \sum_{k=0}^{\infty} \Lambda_k t^k = \exp\left(\sum_{m=1}^{\infty} m^{-1} x_m t^m\right). \tag{42}$$

$$\sigma(t) = \sum_{n=0}^{\infty} S_k t^k = \exp\left(\sum_{m=1}^{\infty} (-1)^{m+1} m^{-1} x_m t^m\right). \tag{43}$$

4 The general context

4.1 Some arithmetical results and conjectures

a. Let F be a smooth n-parameter formal group law, defined over an arbitrary base ring k, for example, arising in the commutative case from completion of a Jacobiam variety or more generally, an abelian variety, defined over k, in the noncommutative case from a smooth Lie group. Associate to F its contravariant formal coordinate ring $\theta(F) = k[[x_1, \ldots x_n]]$ and its covariant algebra of invariant functionals $U(F)$. One can prove that commutative F have an embedding into the direct categorical direct sum of n copies of the completion $\Lambda_{\hat{k}}$, and in the noncommutative situation this extends to an embedding into the categorical direct sum of n copies of the completion $\mathsf{QSym}_{\hat{k}}$. For instance for ζ-functions of algebraic curves, k is typically a finite field $k = \mathbb{F}_q$. In the study of noncommutative Lie groups over such objects, or over ultrametrically complete p-adic fields, the embedding is in a direct sum of copies of $\mathsf{QSym}_{\hat{k}}$, thus knowing only $\mathsf{QSym}_{\mathbb{Q}}$, is of no much help.

b. Campbell-Hausdorff structures
We saw that $\mathcal{P}(\mathcal{Z}) = \{\pi_l | l \in \mathcal{L}\}$. Notice, moreover, that every curve in $\mathcal{Z}$ defines an endomorphism of the Hopf algebra $\mathcal{Z}$ of the noncommutative symmetric functions. We let $\mathcal{E}^{\mathrm{h}}$ be the subgroup of homogeneous curves in $\mathcal{Z}$, i.e. the set of all isobaric endomorphisms of the Hopf

algebra $\mathcal{Z}$. The *generic endomorphism* $\gamma(x)$ of $\mathcal{Z}$ is defined to be the curve, uniquely detrmined by

$$\gamma(x) = \sum_{l\in\mathcal{L}} x_l \pi_l t^{|l|} + \sum_{n=1}^{\infty} D_n(x) t^n.$$

Here we have $D_1(x) = 0$, $D_n(x)$ is determined inductively by the condition that $\gamma(x)$ is a curve, hence the coefficient of t^n is determined uniquely modulo primitive elements be the coefficients of $t^d, (d < n)$, and then the coefficient of t^n is sum of the part $D_n(x)$ that is zero on $\mathrm{Ker}\,(\epsilon)$ and the generic primitive element $\sum_{l\in\mathcal{L},|l|=n} x_l\pi_l$. A *Campbell-Haussdorff relation* is a relation betweeng generic curves

$$\gamma(x)\gamma(y) = \gamma(x\cdot y). \tag{44}$$

For the curve $\gamma(x)$ see the form file
$\gamma(x)$. There are more representations of $\mathcal{E}^{\mathrm{h}}$, for example we may put

$$\gamma(x) = \exp\left(\sum_{l\in\mathcal{L}} \xi_l \pi_l t^{|l|}\right), \tag{45}$$

or

$$\gamma(x) = \prod_{l\in\mathcal{L}} \exp\left(\eta_l \pi_l t^{|l|}\right). \tag{46}$$

In each case, (44) gives rise to a Campbell-Haussdorff relation. Modulo commutators, the structure of $\mathcal{E}^{\mathsf{h}}$ is rather clear: Let $\mathcal{C}$ be the two-sided ideal in $\mathcal{Z}$, generated by all commutators $[z_i, z_j]$. Denoting $\mathcal{E}^{\mathsf{h}^{\mathrm{ab}}}$ the ring of isobaric endomorphisms of the Hopf algebra Λ of the symmetric functions, the map $\gamma : \mathcal{Z} \to \mathcal{Z}/\mathcal{C} = \Lambda$ induces a map

$$\mathcal{E}^{\mathsf{h}} \to \mathcal{E}^{\mathsf{h}^{\mathrm{ab}}} = W(\mathbb{Z}).$$

The identification between homogeneous endomorphisms and Witt vectors is given by the relation

$$f = (f_1, f_2, \dots)\{\leftrightarrow\}\sigma_m \mapsto w_m(f)\sigma_m.$$

Here $w_m(f) = \sum_{d|m} d f_f^{m/d}$, the ghost component of the Witt vector $\underline{f}$, determined by the endomorphisms f. If the base ring is $\mathbb{Z}$, there is another way to represent these endomorphism ring $\mathcal{E}^{\mathsf{h}^{\mathrm{ab}}}$ Define $\hat{f}_m := \sum_{d|m} d f_d$ and addition and multiplication by

$$f \hat{+} g_m = \hat{f}_m + \hat{g}_m \quad , \quad f \hat{\cdot} g_m = \hat{f}_m \cdot \hat{g}_m \quad .$$

This gives a representation of the necklace ring $\mathsf{Nr}(\mathbb{Z})$ as ring of homogeneous endomorphisms of the Hopf algebra Λ. c.f. [MeRo, thm 3, p 107] and the fact that $W(\mathbb{Z})$ admits - via the trivial Hilbert structure on $\mathbb{Z}$ a representations as $H(\mathbb{Z})$, [D90].

c. ***S*-adic symmetric functions**.

Let P be the set of all prime numbers in $\mathbb{N}$ and let S be a possibly empty set subset of P, with complementary set $S^\star = P \setminus S$. Denote $\mathbb{N}(S)$ the set of natural numbers, having all prime factors in S. Then there is a unique decomposition of the multiplicative monoid $\mathbb{N} = \mathbb{N}(S) \times \mathbb{N}(S^\star)$. In the same vein we let $\mathbb{Z}_S$ be the subring of $\mathbb{Q}$, having in reduced form denominators only in S, hence, denoting for a prime p as usual the localized ring $\mathbb{Z}_{(p)}$, one has $\mathbb{Z}_S = \cap_{p\in S}\mathbb{Z}_{(p)}$. The problem of the S-adic symmetric functions is to characterize those symmetric functions having all their coefficients in $\mathbb{Z}_S$. One might ask the same question for noncommutative - and quasi-symmetric functions, and the answer turns out to be very nontrivial. The simplest case is $S = P$ or $S = \emptyset$.

case $S = \emptyset$**.** Then $\mathsf{QSym} = \mathbb{Q}[\mathcal{L}]$ and $\mathcal{Z}_{\mathbb{Q}} = \mathbb{Q} < x_m | m \geq 1 >$. The Lie algebra of primitive elements in $SS_{\mathbb{Q}}$ is the free Lie algebra, generated over $\mathbb{Q}$ by the x_m, thus a basis is the set of all $\{x_l | l \in \mathcal{L}\}$.

case $S = P$**.** Then $\mathsf{QSym} = \mathbb{Z}[\mathcal{Q}]$ and $\mathcal{Z} = \mathcal{Z}$, admitting a basis of *pure primitives* $\Pi = \{\pi_l | l \in \mathcal{L}\}$.
pure primitives.

case $S = \{2\}$. We have the *universal curve*

$$z = \sum_{i=0}^{\infty} z_i t^i = \exp\left(\sum_{m=1}^{\infty} x_m \frac{t^m}{m}\right)$$

and we try to decompose this into a product curve: modulo t^4 we try

$$z \equiv \left(1 + E_1 t + E_2 t^2 + X t^3\right)\left(1 + \lambda \pi_3 t^3\right) \bmod t^4.$$

We are forced to solve $E_1 = z_1$, $E_2 = z_2$. Since $\pi_3 = 3z_3 - 3z_{2,1} + z_{111}$, we take $\lambda := \frac{1}{3} \in \mathbb{Z}_S$ and find

$$X + \frac{1}{3}\pi = z_3 \Rightarrow X = E_{21} - \frac{1}{3}E_{111}.$$

Continue this way: for E_4 we find the expression $E_4 = z_4 - z_{13} + z_{121} - \frac{1}{3}z_{1111}$ has coefficients in $\mathbb{Z}_S$. Recall from π_5 that

$$\pi_5 = z_{11111} - 5z_{1121} + 5z_{1211} - 5z_{2111} + 5z_{212} + 5z_{311} - 5z_{32} - 5z_{41} + 5z_5.$$

Next try to solve

$$z \equiv \left(1 + E_1 t + E_2 t^2 + X t^3 + E_4 t^4 + Y t^5\right)(1+\lambda\pi_3 t^3)(1+\frac{1}{5}\pi_5 t^5) \bmod t^6.$$

It turns out, that there is a unique solution $Y \in \mathcal{Z}_S < E_1, E_2, E_4 >$, giving a decomposition mod t^6 of the universal curve into curves, belonging to *strictly smaller* Hopf algebras than $\mathcal{Z} \otimes \mathbb{Z}_S$. The following - arithmetical - theorem is a not too difficult consequence of the theorem $\mathsf{QSym} = \mathbb{Z}[\mathcal{Q}]$: First let $\overline{E} = \sum_{i=0} E_i t^i$ be a curve in H. Call $\overline{x}$ a *S-pure curve*, if, putting for $s \in \mathbb{N}(S) : E_s := x_s$, and attaching to x_s weight s, then every $E_n = E_n(x_s | s \in S)$ is a (noncommutative) polynomial in the $x_s, (s \in S)$, isobaric of weight n. The set $\{x_s | s \in \mathbb{N}(S)\}$ then is called a *S-pure set*.

Theorem 4.1 *For every $S \subset P$ there exist S-pure sets*

$$\{x_{s,s^\star} | s^\star \in \mathbb{N}(S^\star)\} \subset \mathcal{Z} \otimes \mathbb{Z}_S,$$

indexed by the elements of $\mathbb{N}(S^\star)$ with the following properties:

a. For each pair $(s, s^\star)$ we have

$$x_{s,s^\star} \equiv z_{s^\star . s} \text{ mod decomposable in } \{z_i | i \geq 1\}.$$

b. These sets define the S-pure curves $H_{s^\star}$, such that

$$z = \prod_{s^\star \in \mathbb{N}(S^\star)} U_{s^\star} H_{s^\star}.$$

inducing a decomposition of $\mathcal{Z} \otimes \mathbb{Z}_S$ and

c. For each $s^\star$ the object $\mathbb{Z}_S < x_{s,s^\star} | s \in \mathbb{N}(S)$ is a Hopf subalgebra of $\mathcal{Z} \otimes \mathbb{Z}_S$. In the special case $s^\star = 1$, the elements x_s, i will be denoted E_s and if $S = \{p\}$ a singleton, we mostly write E_i instead of E_{p^i}, (logarithmic notation). The curve will be denoted

$$E = \sum_{i=0}^{\infty} E_i(y_0, \ldots, y_i) t^i.$$

The Hopf algebra $\mathbb{Z}_S < y_s | s \in \mathbb{N}_S$ will be denoted $\mathcal{U}_S$ and will be called the Hopf algebra of the S-typical noncommutative symmetric functions.

c.

Dually, this decomposition theorem induces on the level of quasi-symmetric functions:

Theorem 4.2

*a. Let $\mathcal{Q}_S$ be the set of all generators $\{q_l | l \in \mathcal{L}\}$ that have all their digits in $\mathbb{N}(S)$. For each $s \in S^\star$ we let $s^\star \# \mathcal{Q}_S$ be the set of all $s^\star c$ with $c \in \mathcal{Q}_S$. Then the objects $\mathbb{Z}_S[s^\star \mathcal{Q}_S]$ all are Hopf subalgebras of $\mathsf{QSym} \otimes \mathbb{Z}_S$. The special Hopf subalgebra, corresponding to $s^\star = 1$ will be denoted QSym_S and calle the*Hopf algebra of the S-adic quasi-symmetric functions*. Warning: the tensorproduct $\mathsf{QSym} \otimes \mathbb{Z}_S$ is distinct from QSym_S.*

c. For each $s^\star$ the object $\mathbb{Z}_S[x_{s,s^\star}] | s \in \mathbb{N}(S)$ is a Hopf subalgebra of $\mathsf{QSym} \otimes \mathbb{Z}_S$. (The special case $s = (1)$ will be called the Hopf algebra of the S-adic quasi-symmetric functions*.*

d.

We give an example of this curve for the case $S = \{2\}$.

$$
\begin{aligned}
E \;=\; & \\
& 1+ \;\; t(E_1) \\
& + \;\; t^2(E_2) \\
& + \;\; t^3(-\frac{1}{3}E_{111} + E_{21}) \\
& + \;\; t^4(E_4) \\
& + \;\; t^5(+\frac{2}{15}E_{11111} - \frac{1}{3}E_{2111} + E_{41}) \\
& + \;\; t^6(\frac{1}{45}E_{111111} + \frac{1}{9}E_{11121} - \frac{1}{3}E_{11211} + \frac{4}{9}E_{12111} + \frac{1}{3}E_{1221} - \frac{2}{3}E_{141} \\
& - \;\; \frac{2}{9}E_{21111} - \frac{1}{3}E_{2211} - \frac{1}{3}E_{222} + \frac{2}{3}E_{24} + \frac{2}{3}E_{411} + \frac{1}{3}E_{42}) \\
& + \;\; t^7(-\frac{2}{63}E_{1111111} + \frac{1}{9}E_{111211} - \frac{1}{3}E_{112111} + \frac{4}{9}E_{121111} + \frac{1}{3}E_{12211} - \frac{2}{3}E_{1411} \\
& - \;\; \frac{4}{45}E_{211111} - \frac{1}{3}E_{22111} - \frac{1}{3}E_{2221} + \frac{2}{3}E_{241} + \frac{1}{3}E_{4111} + \frac{1}{3}E_{421}) \\
& + \;\; t^8(+E_8) \\
& + \;\; t^9(+\frac{41}{2835}E_{111111111} - \frac{1}{27}E_{11121111} + \frac{1}{9}E_{11211111} - \frac{4}{27}E_{12111111} - \frac{1}{9}E_{1221111} + \frac{2}{9}E_{141111} \\
& + \;\; \frac{19}{945}E_{21111111} + \frac{1}{9}E_{2211111} + \frac{1}{9}E_{222111} - \frac{2}{9}E_{24111} - \frac{4}{45}E_{411111} - \frac{1}{9}E_{42111} + E_{81})
\end{aligned}
\tag{47}
$$

Frobenius and Verschiebung The classification of smooth commutative formal groups (and group laws) proceeds by means of an endomorphism $f_a, (a \geq 1)$ of the Hopf algebra Λ, on primitive elements determined by $f_a(\sigma_m) = \sigma_{am}$. Note that abelian group $\Lambda/\mathbb{Z}[\sigma_m | m \geq 1]$ has nontrivial additive torsion, thus it is not trivial, that all f_a are defined over $\mathbb{Z}$. There is an endomorphism v_a of the Hopf algebra Λ, called the *Verschiebung*, satisfying $v_a(\sigma_m) = a\sigma_{m/a}$, if m is divisible by a and 0 otherwise. One has $v_a \circ f_a = a$ which plays a very important role for the ζ-function, taking $a = p$. Both endomorphisms of Hopf algebras naturally extend to the Hopf algebras $\mathcal{Z}$ and QSym : indeed, there a pure homogeneous curves $F_a = \sum_{i=0}^{\infty} \pi_{a,m} t^m$, lying over every primitive $\pi_m, (m \geq 1)$. The very definition of curve implies the map $z_m \mapsto \pi_{a,m}$ to be an endomorphism of Hopf algebras.

References

[Bal] Bertet, K., Krob, D., Morvan, M., Novelli, J.-C., Phan, H.D., Thibon, J.-Y.: *An overview of* Λ*-type operations on quasi-symmetric functions.*

[Co] Cohn, P. *Skew field constructions*, London Math. Soc. Lect. Notes Series, **27**, Cambridge University Press, (1977).

[D72] Ditters, E.J: *Curves and formal (co)groups*, Inventiones Math, 17, 1 - 20, (1972).

[D85] Ditters, E.J. *Sur une extension non-cocommutative d'algèbre de Hopf des fonctions symétriques*, Rapport **300**, Vrije Universiteit Amsterdam, (1985).

[D90] Ditters, E.J.: *Hilbert functions and Witt functions. An identity for congruences of Atkin and of Swinnerton - Dyer type*, Math. Z., **205**, 247 - 278, (1990).

[DH] Ditters, E.J. and Hazewinkel, M.: *Explicit generators for the ring of quasi-symmetric functions over the integers*, in preparation, Amsterdam, (2002).

[Di01] Ditters, E,J,: *Lectures on symmetric and quasisymmetric functions*, Free University Amsterdam, Spring 2001.

[Di02a] Ditters, E.J.: Letter to Chr. Reutenauer, 9-4-2002, (Fays en Vosges), (2002).

[Di02b] Ditters, E.J.: *Lyndon-Witt functions and the structure of* QSym , preprint, Amsterdam, May 2002.

[Di02c] Ditters, E.J.: *Lecture on the various types of symmetric functions*, preprint, Amsterdam, www/cs.vu.nl/∼ejd/qslw, Jume 2002.

[DS] Ditters, E.J. and Scholtens, A.C.J. *Free polynomial generators for the Hopf algebra* QSym *of quasi-symmetric functions*, Journal of Pure and Applied Algebra, **144**, 213-227, (1999).

[Gea] Gelfand, I.M., Krob, D., Lascoux,A., Leclerc, B., Retakh, V.,Thibon, J-Y. *Noncommutative Symmetric Functions*, Adv. in Math., **112**, 218-348, (1995).

[GR2] Gelfand, I. and Retakh, V.S. *A theory of noncommutative determinants and characteristic functions of graphs*, Funct. Anal. Appl., **26**, 1-20, (1992). *Publ LACIM, UQAM, Montreal*, **14**, 1-26.

[Haz] Hazewinkel, M.: *The algebra of quasi-symmetric functions is free over the integers*, Adv. Math., **164**, 283-300, (2001).

[Haz01] Hazewinkel. M.: *The primitives of the Hopf algebra of noncommutative symmetric functions*, preprint, 20 october 2001, CWI, Amsterdam.

[McD79] MacDonald, I.G. *Symmetric functions and Hall polynomials*, Clarendon Press, Oxford, (1979).

[Kob77] Koblitz, N.: *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Graduate Texts in Mathematics, **58**, Springer-Verlag, New York Heidelberg Berlin, (1977).

[MR] Malvenuto, C. and Reutenauer, C. *Duality between quasi-symmetric functions and the Solomon descent algebra*, Journal of Algebra, **177**, 967-982, (1995).

[MR98] Malvenuto, C. and Reutenauer, C. *Plethysm and conjugation of quasi-symmetric functions*, Discrete Math., **193**, 225-233, (1995).

[MS] Meijer, S.: QSym *-package: java software for quasi-symmetric functions*,Free University, Amsterdam, (2002).

[MeRo] Metropolis, N. and Rota, G-C.: *Witt vectors and the algebra of necklaces*, Adv. Math., **50**, 95-125, (1983).

[Rad] Radford, D.E. *A natural ring basis for the shuffle algebra and an application to group schemes*, Journal of Algebras, **58**, 432-454, (1979).

[Reut93] Reutenauer, Chr. *Free Lie Algebras*, Clarendom Press, Oxford (1993).

[Reut95] Reutenauer, Chr.: *On symmetric functions related to Witt vectors and the free Lie algebra*, Adv. Math, **110**, 234-246, (1995).

[Rob00] Robert.A.: *A course in p-adic analysis*, Graduate Texts in Mathematics 198, Springer-Verlag, New York, Inc., (2000).

[Shay] Shay, P.B. *An Obstruction Theory for Smooth Formal Group Structure*, Preprint, (unpublished). Hunter College. CUNY.

[Ver] Vermaseren, J.A.M. *Symbolic Manipulation with FORM*, Tutorial and reference manual, version 2, CAN, (Computer Algebra Nederland), Amsterdam, (1991).

Contents