Combinatoire des algèbres de Hopf

M. Petitot

Abstract

On introduit le concept d'algèbre de Hopf en vue d'application en combinatoire, en particulier la combinatoire des intégrales itérées et des fonctions quasi–symétriques.

1 Introduction

La notion d'*algèbre de Hopf* tire principalement son origine de la théorie des groupes. A toute algèbre de Hopf, on associe un groupe formé par certains éléments dits *group-like* de cette algèbre. D'autre part, moyennant une condition technique, l'algèbre des fonctions définies sur un groupe à valeurs dans un corps est une algèbre de Hopf.

Depuis longtemps, on sait que la donnée d'une k-variété (algébrique, resp. analytique, resp. C^∞ etc.) est la donnée d'une k-algèbre de fonctions (algébriques, resp. analytiques, resp. C^∞ etc.) définies sur la variété et à valeurs dans le corps k. Supposons que la variété soit un groupe G et notons $\mathcal{F}G$ une algèbre de fonctions de G dans k pour les trois opérations

$$\left\{\begin{array}{rcl} (f+g)(x) & := & f(x)+g(x) \qquad \forall x\in G, \quad f,g\in\mathcal{F}G \\ (fg)(x) & := & f(x)\,g(x), \\ (\alpha f)(x) & := & \alpha f(x) \qquad \alpha\in k, \end{array}\right. \tag{1}$$

Il est alors possible de définir trois opérations supplémentaires: le *coproduit* Δ, la *co–unité* ε et l'*antipode* a:

$$\left\{\begin{array}{rcl} (\Delta f)(x,y) & := & f(xy), \qquad \forall x,y\in G, \quad f\in\mathcal{F}G \\ \varepsilon(f) & := & f(e), \qquad e \text{ est élément neutre de } G \\ (af)(x) & := & f(x^{-1}), \end{array}\right. \tag{2}$$

les opérations dans le groupe G étant notées xy et x^{-1}.

Moyennant une condition technique portant sur $\mathcal{F}G$ permettant d'identifier[1] la fonction de deux variables Δf comme un élément du produit tensoriel $\mathcal{F}G\otimes\mathcal{F}G$, l'algèbre $\mathcal{F}G$ est alors munie d'une structure d'algèbre de Hopf (voir section 2.1) grâce à ces trois nouvelles opérations

$$\begin{array}{rcl} \Delta & : & \mathcal{F}G\to\mathcal{F}G\otimes\mathcal{F}G \\ \varepsilon & : & \mathcal{F}G\to k \\ a & : & \mathcal{F}G\to\mathcal{F}G. \end{array}$$

[1] Il faut pouvoir écrire $f(xy)$ comme une somme finie $\sum_i g_i(x)h_i(y)$ avec les $g_i,h_i\in\mathcal{F}G$.

Cette algèbre est ici commutative mais les mathématiciens se sont vite affranchis de la commutativité pour diverses raisons:

1. Les algèbres de Hopf sont accouplées deux par deux. Le dual (au sens des k-espaces vectoriels) d'une algèbre de Hopf moyennant certaines restrictions (sur les éléments du dual) est encore une algèbre de Hopf. Le dual d'une algèbre de Hopf commutative n'est pas en général commutative ; elle est dite *co–commutative.*

2. La géométrie non commutative et l'étude des groupes quantiques en physique statistique amènent à considérer des algèbres de Hopf qui ne sont ni commutatives ni co-commutatives.

Dès les années 70, des combinatoristes ont fait remarquer que la notion d'algèbre de Hopf rendait lumineuses un certain nombre de constructions combinatoires, en particulier la combinatoire des mots (concaténation, produit de mélange). La combinatoire des algèbres de Hopf était connue dans les années 70 mais depuis quelques années, cette théorie a permis de résoudre des questions importantes en physique des hautes énergies ainsi qu'en théorie des nombres :

1. Le célèbre physicien R. Feynmann avait l'habitude de coder certaines intégrales par des graphes particuliers appelés *diagrammes* de Feynmann. On sait aujourd'hui qu'un calcul rigoureux sur ces intégrales (certaines sont divergentes) est basée sur la structure d'algèbre de Hopf de ces diagrammes [2]. Cette structure généralise la structure d'algèbre de Hopf découverte par Butcher à propos des schémas de Runge-Kutta utilisés pour résoudre numériquement les equations différentielles ordinaires [6].

2. La combinatoire sur les mots s'est montrée d'une remarquable efficacité pour démontrer des identités en théorie des nombres ou sur certaines fonctions spéciales comme les polylogarithmes. Il faut noter que le calcul sur les *moules* introduit par J. Ecalle dans les années 80 s'inscrit dans ce courant de pensée.

   Cela prouve que le projet de démonstration *automatique* d'identités entre nombres définis par des séries ou des intégrales telles que
   $$\zeta(2) = \frac{\pi^2}{6} \qquad (Euler) \tag{3}$$
   avec $\zeta(2) := \sum_{n>0} 1/n^2$ et $\pi := \int_{x^2+y^2\leq 1} dxdy$ (autrement dit, π est la surface d'un cercle de rayon 1) est à l'ordre du jour [2].

Si les constructions combinatoires sont éclairés par la théorie des algèbres de Hopf, les calculs proprement dits reposent principalement sur l'utilisation de séries formelles en variables *non* commutatives. Toute application $w \to S_w$ où $w \in X^*$ est un mot construit avec les lettres de l'alphabet X est codé par la série
$$S = \sum_{w\in X^*} S_w\ w. \tag{4}$$

[2]Voir le projet de M. Kontsevitch à l'I.H.E.S.

Ceci est une généralisation de l'usage des séries génératrices en une seule variable z où l'étude d'une suite de nombres $n \in \mathbb{N} \to c_n$ est remplacée par l'étude de la série formelle $C(z) = \sum_{n>0} c_n z^n$.

2 Algèbres de Hopf

2.1 Axiomes

J'ai repris presque intégralement la présentation de Marc Rosso dans son article *Groupes quantiques: origines et applications* [5]. On désigne par k un corps commutatif de caractéristique nulle et par $\otimes$ le produit tensoriel au–dessus de k. Toutes les algèbres considérées sont à coefficients dans le corps k

(a) Soit (A, m, η) une algèbre *associative* et *unitaire*. Sa structure est donnée par deux applications linéaires $m : A \otimes A \to A$ et $\eta : k \to A$, à savoir la multiplication m et l'unité pour cette multiplication $\eta(\alpha) = \alpha 1_A$ (pour $\alpha \in k$) qui satisfont aux axiomes suivants représentés par des diagrammes commutatifs. La multiplication m est associative :

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "m\otimes\mathrm{Id}"] \arrow[d, "\mathrm{Id}\otimes m"'] & A \otimes A \arrow[d, "m"] \\ A \otimes A \arrow[r, "m"'] & A \end{tikzcd} \tag{5}$$

et l'élément 1_A est neutre à gauche et à droite :

$$\begin{tikzcd} k \otimes A \arrow[r, "\eta\otimes\mathrm{Id}"] \arrow[d] & A \otimes A \arrow[d, "m"] & A \otimes k \arrow[l, "\mathrm{Id}\otimes\eta"'] \arrow[d] \\ A \arrow[r, equal] & A \arrow[r, equal] & A \end{tikzcd} \tag{6}$$

(b) On peut alors définir la structure de *cogèbre* sur un espace vectoriel C comme étant formellement la structure duale de celle d'algèbre , i.e. celle obtenue en renversant les flèches dans les diagrammes commutatifs ci-dessus. La structure est donc donnée par deux applications linéaires $\Delta : C \to C \otimes C$ et $\varepsilon : C \to k$. Le coproduit Δ est coassociatif :

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & C \otimes C \arrow[d, "\Delta\otimes\mathrm{Id}"] \\ C \otimes C \arrow[r, "\mathrm{Id}\otimes\Delta"'] & C \otimes C \otimes C \end{tikzcd} \tag{7}$$

et ε est une *counité* à gauche et à droite :

$$\begin{tikzcd} C \arrow[r, equal] \arrow[d] & C \arrow[r, equal] \arrow[d, "\Delta"] & C \arrow[d] \\ k \otimes C & C \otimes C \arrow[l, "\varepsilon\otimes\mathrm{Id}"'] \arrow[r, "\mathrm{Id}\otimes\varepsilon"] & C \otimes k \end{tikzcd} \tag{8}$$

Soit $\sigma : C \otimes C \to C \otimes C$ la permutation telle que $\sigma(x \otimes y) = y \otimes x$. On pose $\Delta' = \sigma \circ \Delta$. Alors $(C, \Delta', \varepsilon)$ est encore une cogèbre appelée cogèbre opposée de (C, Δ, ε). Lorsque $\Delta' = \Delta$, C est dite *cocommutative*.

(c) Un structure de *bigèbre* sur un k-espace vectoriel H est la donnée simultannée d'une structure d'algèbre unitaire (H, m, η) et d'une structure de cogèbre (H, Δ, ε) qui satisfont de plus à la condition: Δ et ε sont des morphismes d'algèbre, autrement dit $\Delta(xy) = \Delta(x)\,\Delta(y)$ et $\varepsilon(xy) = \varepsilon(x)\,\varepsilon(y)$ pour tout $x, y \in H$. Ceci est équivalent à la condition: m et η sont des morphismes de cogèbre. Notons que le produit $\Delta(x)\Delta(y)$ dans $A \otimes A$ est calculé en appliquant la règle $(x \otimes y).(x' \otimes y') = (xx') \otimes (yy')$ pour tout $x, x', y, y' \in A$.

(d) Si $(H, m, \Delta, \eta, \varepsilon)$ est une bigèbre, l'espace vectoriel End H des applications linéaires de H dans H est muni du *produit de convolution* de la manière suivante :

$$\forall f, g \in \mathrm{End}\ H, \quad f * g = m \circ (f \otimes g) \circ \Delta. \tag{9}$$

Muni de ce produit, End H est une algèbre avec élément unité $\eta \circ \varepsilon$. On dit que H est une *algèbre de Hopf* lorsque l'application identité $\mathrm{Id} \in \mathrm{End}\ H$ possède une inverse à gauche et à droite pour le produit de convolution. Cet inverse, noté a est appelé *antipode*. Il doit donc satisfaire l'égalité

$$a \circ \mathrm{Id} = \mathrm{Id} \circ a = \eta \circ \varepsilon \tag{10}$$

L'antipode a est alors un antihomomorphisme d'algèbre (i.e. $a(xy) = a(y)\,a(x)$ pour tout $x, y \in H$) et un antihomomorphisme de cogèbre (i.e. $\Delta \circ a = (a \otimes a) \circ \Delta'$).

(e) Soit H une algèbre de Hopf. Un élément $x \in H$ est dit *primitif* lorsque $\Delta(x) = x \otimes 1 + 1 \otimes x$. Il est dit *group-like* lorsque $\Delta(x) = x \otimes x$. On vérifie assez facilement que les éléments primitifs forment une k-algèbre de Lie (pour le crochet $[x, y] = xy - yx$ lorsque $x, y \in H$) et que les éléments group-like forment un groupe (pour le produit de H). On montre que l'antipode d'un élément primitif $p \in H$ vaut $a(p) = -p$ et que l'antipode d'un élément group-like $g \in H$ vaut $a(g) = g^{-1}$.

Lorsqu'elle est est définie, la transformation *exponentielle* de H dans H:

$$\exp x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots, \qquad x \in H \tag{11}$$

transforme un élément primitif en un élément group-like.

(f) Une algèbre A est dite *graduée* lorsqu'elle se décompose en une somme directe de k-espaces vectoriels (composantes homogènes) A_n, $n \in \mathbb{N}$:

$$A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$$

avec la condition $A_m A_n \subset A_{m+n}$ pour tout $m, n \in \mathbb{N}$. Si A est graduée, alors $A \otimes A$ l'est aussi en posant $(A \otimes A)_n := \sum_{i+j=n} A_i \otimes A_j$.

Dans la suite, on supposera toujours que $A_0 = k$ et que les composantes homogènes A_n sont des espaces vectoriels de dimension finie. Un élément dans A_n est dit de degré n.

Une algèbre de Hopf $(H, m, \Delta, \eta, \varepsilon, a)$ est dite *graduée* si chacune des trois applications m, Δ, a transforme un élément homogène en un élément homogène de même degré.

2.2 Exemples classiques

(a) Soit G un groupe k-algébrique. Alors l'algèbre des fonctions polynomiales de G dans k (i.e. l'anneau des coordonnées) munie des trois opérations (Δ, ε, a) définies par (2) est une algèbre de Hopf.

Prenons, par exemple, le groupe $G := \mathrm{SL}(n, k)$ formé des matrices $n \times n$ à coefficients dans k dont de déterminant est égal à un. On note $\rho_{i,j} : G \to k$ la fonction qui à toute matrice $X \in G$ associe l'élément $X_{ij} \in k$ positionné à la i-ième ligne et à la j-ième colonne de X. Alors les formules (2) donnent $\Delta(\rho_{ij}) = \sum_{k=1}^{n} \rho_{ik} \otimes \rho_{kj}$ et $\varepsilon(\rho_{ij}) = \delta_{ij}$.

(b) Soit $\mathfrak{g}$ une algèbre de Lie et $\mathcal{U}\mathfrak{g}$ son algèbre enveloppante. On pose pour $x \in \mathfrak{g}$, $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0, a(x) = -x$ et on prolonge multiplicativement. Alors $\mathcal{U}\mathfrak{g}$ devient une algèbre de Hopf cocommutative.

Considérons comme premier exemple, l'ensemble $k\langle X \rangle$ des polynômes en variables non commutatives à coefficients dans le corps k. Un polynôme est une combinaison linéaire *finie* de mots $w \in X^*$ tous construits avec les lettres de l'alphabet X. Le coefficient du mot w dans le polynome p est noté $(p|w)$. Par suite, $p = \sum_{w \in X^*} (p|w)\ w$. Le mot vide est noté 1, $|w|$ désigne le nombre de lettres du mot w et $\tilde{w}$ désigne le mot "miroir" de w (le miroir de $w = abc$ est $\tilde{w} = cba$).

On pose pour tout $x \in X$, $\Delta(x) = x \otimes 1 + 1 \otimes x$ et pour tout $p \in k\langle X \rangle$, $\varepsilon(p) = (p|1)$ et $a(p) = \sum_{w \in X^*} (-1)^{|w|} (p|w) \tilde{w}$. Alors, $k\langle X \rangle$ est une algèbre de Hopf cocomutative graduée par la longueur des mots. L'ensemble des polynômes de Lie est noté $\mathcal{L}ie_k\langle X \rangle$; c'est le plus petit k-espace vectoriel de $k\langle X \rangle$ qui contient X et qui est fermé par le crochet de Lie $[p, q] = pq - qp$ pour $p, q \in k\langle X \rangle$. On montre que $\mathcal{U}\mathcal{L}ie_k\langle X \rangle = k\langle X \rangle$ et que les éléments primitifs de $k\langle X \rangle$ forment $\mathcal{L}ie_k\langle X \rangle$. Le seul élément group-like est l'élément neutre 1.

Une série formelle $S \in k\langle\langle X \rangle\rangle$ est une combinaison linéaire finie ou infinie de mots, i.e. $S = \sum_{w \in X^*} (S|w) w$. Les opérations définies précédemment munissent $k\langle\langle X \rangle\rangle$ d'une structure d'algèbre de Hopf. Les éléments primitifs sont appelés *séries de Lie* et les éléments group-like sont appelés *exponentielles de Lie*. La transformation exponentielle définie comme en (11) envoie les éléments primitifs sur les éléments group-like. Réciproquement, le logarithme

$$\log(1 + S) = S - S^2/2 + S^3/3 - \cdots + (-1)^{n+1} S^n/n + \cdots \tag{12}$$

envoie les exponentielles des Lie sur les séries de Lie.

3 Dualité

3.1 Dual restreint

On a vu que les axiomes des algèbres de Hopf forment un ensemble auto–dual, c'est à dire qu'il est invariant en inversant le sens des flèches et en échangeant produit et coproduit, unité et counité. Intéressons–nous à la dualité dans le cadre des espaces vectoriels. Le dual d'un k-espace vectoriel V est l'ensemble noté V^* des formes linéaires de V dans k. L'espace des séries formelles $k\langle\langle X\rangle\rangle$ peut être vu, soit comme le complété de $k\langle X\rangle$ en tant que module gradué par le degré, soit comme l'espace vectoriel dual de $k\langle X\rangle$. Dans ce dernier cas, une série formelle S est vue comme une forme linéaire $S : p \to (S|p)$ sur l'espace des polynomes (l'accouplement $(S|p)$ prolonge par linéarité l'accouplement défini sur les mots par $(u|v) = \delta_{u,v}$). Cette dualité est étendue à $k\langle X\rangle \otimes k\langle X\rangle$ en posant

$$(p \otimes q|p' \otimes q') := (p|p')(q|q') \tag{13}$$

Le dual d'une cogèbre est une algèbre mais il y a une difficulté: si (A, m, η) est une algèbre, l'espace vectoriel dual A^* n'est pas une cogèbre pour l'opération m^* duale de m car celle–ci envoie A^* dans $(A \otimes A)^*$ qui contient strictement $A^* \otimes A^*$ sauf si A est de dimension finie.

On définit le dual *restreint* [3] de (A, m) comme l'ensemble des formes linéaires $\lambda \in A^*$ telles que $m^*(\lambda) \in A^* \otimes A^*$, autrement dit telles que $m^*(\lambda)$ soit une somme *finie* d'éléments de la forme $\alpha \otimes \beta$ avec les $\alpha, \beta \in A^*$.

Théorème 1 ([3]) *Si $(H, m, \Delta, \eta, \varepsilon, a)$ est une algèbre de Hopf, son dual restreint est une algèbre de Hopf pour les opérations duales de celles de H.*

Par exemple, le dual restreint de l'algèbre $k\langle X\rangle = \mathcal{UL}ie_k\langle X\rangle$ est l'ensemble des séries S telles que (I est fini)

$$\Phi(S) = \sum_{i \in I} T_i \otimes U_i, \qquad T_i, U_i \in k\langle\langle X\rangle\rangle. \tag{14}$$

Le coproduit Φ est obtenu en dualisant le produit de concaténation. Pour un mot $w \in X^*$, on a

$$\Phi(w) := \sum_{uv=w} u \otimes v \tag{15}$$

On montre que les séries vérifiant la condition (14) sont reconnaissables et réciproquement. Un théorème classique de M.P. Schutzenberger dit qu'une série est reconnaissable si et seulement si elle est rationnelle [1].

3.2 Dual gradué

Le dual gradué A^g d'une algèbre graduée $A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots$ est construit en dualisant séparément chaque composante homogène:

$$A^g := A_0^* \oplus A_1^* \oplus A_2^* \oplus \cdots \tag{16}$$

Si l'on suppose que les composantes homogènes sont de dimension finie, il est possible d'identifier A et A^* en tant qu'espace vectoriel mais cet isomorphime n'est pas canonique car il dépend du choix d'une base de A.

Théorème 2 *Si $(H, m, \Delta, \eta, \varepsilon, a)$ est une algèbre de Hopf graduée, son dual gradué est une algèbre de Hopf graduée pour les opérations duales de celles de H.*

L'algèbre de Hopf graduée $k\langle X\rangle = \mathcal{UL}ie_k\langle X\rangle$ admet comme algèbre de Hopf duale graduée, l'algèbre de mélange $\mathrm{Sh}_k(X) = (k\langle X\rangle, ш, \Phi, \eta, \varepsilon, a)$. Cette algèbre de Hopf a pour produit, le produit de mélange (commutatif) défini en dualisant le coproduit Δ de $\mathcal{UL}ie_k\langle X\rangle$

$$(p \,ш\, q|w) = (p \otimes q|\Delta(w)). \tag{17}$$

L'unité est η, la counité $\varepsilon : p \to (p|1)$, l'antipode $a : x \to -x$ pour tout $x \in X$ et le coproduit Φ est défini par (15).

3.3 Structure d'une algèbre de Hopf graduée

L'algèbre de mélange $\mathrm{Sh}_j(X)$ est une algèbre (commutative) de polynômes (i.e. elle est libre), autrement dit il existe un système de générateurs de cette algèbre qui ne sont liés par aucune relation k-polynomiale. On retiendra particulièrement que les mots de Lyndon sur l'alphabet ordonné X forment une base de transcendance de $\mathrm{Sh}_k(X)$.

Théorème 3 (Radford) *Tout polynôme de $k\langle X\rangle$ s'écrit de manière unique comme une combinaison linéaire* unique *de "shuffles" de mots de Lyndon, i.e.* $\mathrm{Sh}_k(X) \simeq k[\mathcal{L}yndon(X)]$.

La liberté de $\mathrm{Sh}_k(X)$ est un cas particulier du thm suivant:

Théorème 4 (Milnor–Moore)

1. *Une algèbre de Hopf commutative graduée est libre.*
2. *Une algèbre de Hopf cocommutative graduée est isomorphe (comme algèbre de Hopf) à l'algèbre enveloppante de ses éléments primitifs.*

4 Séries génératrices

Toute application linéaire $f : \mathrm{Sh}_k(X) \to A$ où A est une k-algèbre commutative peut être décrite par la série génératrice

$$F = \sum_{w \in X^*} f(w) w. \tag{18}$$

En effet, la connaissance de l'application linéaire f sur les mots $w \in X^*$ détermine complètement f.

L'application f est un morphisme pour le produit de mélange ssi $f(u \,ш\, v) = f(u)f(v)$ pour tout $u, v \in X^*$, ce qui se traduit pour la série génératrice associée par $(F|u \,ш\, v) = (F|u)(F|v)$. D'après (17), on a $(F|u \,ш\, v) = (\Delta(F)|u \otimes v)$ et d'après (13), on a $(F|u)(F|v) = (F \otimes F|u \otimes v)$. Par suite $(\Delta(F)|u \otimes v) = (F \otimes F|u \otimes v)$.

Proposition 1 (Friederich) *L'application f est un morphisme pour le produit de mélange ssi la série génératrice associée est une exponentielle de Lie, i.e.* $\Delta(F) = F \otimes F$.

4.1 Série double

Nous allons d'abord examiner le cas $A = \mathrm{Sh}_k(X)$. L'identité Id dans $\mathrm{Sh}_k(X)$ admet pour série génératrice la série double $\sum_{w \in X^*} w \otimes w$. La série F définie en (18) s'écrit alors

$$F = (f \otimes \mathrm{Id}) \sum_{w \in X^*} w \otimes w \tag{19}$$

Comme l'identité est un morphisme pour le produit de mélange, d'après la prop. 1 la série double est une exponentielle de Lie. Soit $\mathcal{B}$ une base homogène de $k\langle X \rangle$, c'est à dire $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots$ où $\mathcal{B}_n$ est une base de l'espace des polynômes *homogènes* de degré n. On considère la base duale $\mathcal{B}^* = \mathcal{B}_0^* \cup \mathcal{B}_1^* \cup \mathcal{B}_2^* \cup \cdots$ où $\mathcal{B}_n^*$ est la base duale de $\mathcal{B}_n$. Alors

$$\sum_{w \in X^*} w \otimes w = \sum_{b \in \mathcal{B}} b^* \otimes b. \tag{20}$$

La preuve est immédiate en partant de $w = \sum_{b \in \mathcal{B}} (w|b^*)\ b$. Le calcul donne

$$\begin{aligned}
\sum_{w \in X^*} w \otimes w &= \sum_{w \in X^*} w \otimes \sum_{b \in \mathcal{B}} (w|b^*)\ b \\
&= \sum_{b} \Big(\sum_{w} (b^*|w) w \Big) \otimes b \\
&= \sum_{b \in \mathcal{B}} b^* \otimes b.
\end{aligned}$$

4.2 Séries génératrices et produit de convolution

Dans la suite, on considère la série double comme un élément de $\mathrm{Sh}_k(X)\langle\langle X \rangle\rangle$, autrement dit comme une série en variables non commutatives à coefficients dans l'algèbre de mélange (cette dernière est commutative et intègre). Le calcul du produit se fait donc selon la règle

$$(a \otimes u).(b \otimes v) = (a \sqcup\!\sqcup b) \otimes (uv), \qquad \forall a, b \in \mathrm{Sh}_k(X),\ \forall u, v \in X^*. \tag{21}$$

Le produit de deux séries génératrices correspond alors au produit de convolution $*$ défini par (9) pour l'algèbre de Hopf $\mathrm{Sh}_k(X)$

$$\Big(\sum_{u \in X^*} f(u) \otimes u \Big) \Big(\sum_{v \in X^*} g(v) \otimes v \Big) = \Big(\sum_{w \in X^*} (f * g)(w) \otimes w \Big). \tag{22}$$

La preuve qui est facile repose sur l'égalité $(f * g)(w) = \displaystyle\sum_{uv = w} f(u) \sqcup\!\sqcup g(v)$.

L'antipode a définie en (10) est l'inverse de l'identité pour le produit de convolution. Par suite, la série génératrice de la fonction $a : \mathrm{Sh}_k(X) \to \mathrm{Sh}_k(X)$ est l'inverse de la série double :

$$\Big(\sum_{u \in X^*} a(u) \otimes u \Big) \Big(\sum_{v \in X^*} v \otimes v \Big) = \Big(\sum_{v \in X^*} v \otimes v \Big) \Big(\sum_{u \in X^*} a(u) \otimes u \Big) = 1. \tag{23}$$

Notons au passage que si f^* est l'application *adjointe* de f i.e. $(f(u)|v) = (u|f^*(v)$ pour tout $u, v \in X^*$ alors

$$\sum_{w \in X^*} f(w) \otimes w = \sum_{w \in X^*} w \otimes f^*(w). \tag{24}$$

4.3 Factorisation de la série double

Nous allons maintenant donner une factorisation de la série double qui est en fait une factorisation *universelle* de toute exponentielle de Lie.

On s'inspire de la théorie classique de Lie qui dit qu'au voisinage de l'élément neutre, tout élément g d'un groupe de Lie G (réel ou complexe) de dimension n s'écrit de manière unique comme un produit de n exponentielles ($k = \mathbb{R}$ ou $\mathbb{C}$)

$$g = \exp[\xi_1(g)X_1] \times \exp[\xi_2(g)X_2] \times \cdots \times \exp[\xi_n(g)X_n], \qquad \xi_i(g) \in k, \tag{25}$$

où $(X_1, X_2, \ldots, X_n)$ est une base *ordonnée* de l'algèbre de Lie du groupe G (espace vectoriel tangent en l'élément neutre). On en déduit que les fonctions $(\xi_1, \xi_1, \ldots \xi_n)$ forment un système de coordonnées locales (analytiques) sur G au voisinage de l'élément neutre.

Lorsqu'on développe les exponentielles figurant dans le membre de droite de (25) en utilisant la formule de Taylor (11), on obtient une série écrite dans la base de Poincaré–Birkhoff–Witt (PBW). Un élément b de cette base $\mathcal{B}$ s'écrit

$$b = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}, \qquad \alpha_i \in \mathbb{N} \tag{26}$$

et son coefficient est égal à

$$(g|b) = \frac{\xi_1(g)^{\alpha_1} \xi_2(g)^{\alpha_2} \ldots \xi_n(g)^{\alpha_n}}{\alpha_1! \alpha_2! \ldots \alpha_n!}. \tag{27}$$

L'idée est de considérer l'algèbre de mélange comme l'algèbre des coordonnées du groupe des exponentielles de Lie ; dans le cadre formel, la formule (25) sera vraie *globalement* sur tout le groupe.

Théorème 5 *Soit $\mathcal{B}$ une base PBW construite en partant d'une base homogène (notée $\mathcal{L}$) quelconque de l'algèbre de Lie libre $\mathcal{L}ie_k\langle X\rangle$. Soit $\mathcal{B}^*$ la base homogène duale de $\mathcal{B}$. Alors, on a la factorisation de la série double*

$$\sum_{w \in X^*} w \otimes w = \sum_{b \in \mathcal{B}} b^* \otimes b = \prod_{b \in \mathcal{L}} \exp(b^* \otimes b), \tag{28}$$

la base $\mathcal{L}$ étant balayée dans le sens décroissant.

Posons $\mathcal{L} = (P_i \mid i \in \mathbb{N})$ où les P_i sont des polynômes de Lie homogènes. La preuve du thm. repose principalement sur le fait que si $b \in \mathcal{B}$ s'écrit sous la forme $b = P_{i_1}^{\alpha_1} P_{i_2}^{\alpha_2} \cdots P_{i_n}^{\alpha_n}$ tels que $i_1 > i_2 > \cdots > i_n$ avec $n \geq 0$, alors l'élément dual $b^* \in \mathcal{B}^*$ s'écrit grâce au produit de mélange selon une formule semblable à (27) :

$$b^* = \frac{(P_{i_1}^*)^{ш\, \alpha_1} ш\, (P_{i_2}^*)^{ш\, \alpha_2} ш \cdots ш\, (P_{i_n}^*)^{ш\, \alpha_n}}{\alpha_1!\alpha_2!\cdots\alpha_n!}, \tag{29}$$

sachant que l'élément dual d'un P_i est noté P_i^*. On conclut en utilisant la formule (20).

Pour les applications aux polylogarithmes et aux MZV, on a grand intérêt à choisir comme base de l'algèbre de Lie libre, la base dite de Lyndon, obtenue en crochetant les mots de Lyndon: $\mathcal{L} := \{P_l \mid l \in \mathcal{L}yndon(X)\}$. Les éléments de la base PBW associée à $\mathcal{L}$ sont alors de la forme

$$b = P_{l_1}^{\alpha_1} P_{l_2}^{\alpha_2} \cdots P_{l_n}^{\alpha_n}, \quad l_i \in \mathcal{L}yndon(X), \quad l_1 > l_2 > \cdots > l_n, \quad \alpha_i \in \mathbb{N}. \tag{30}$$

Compte-tenu du fait que tout mot $w \in X^*$ s'ecrit de manière unique en un produit décroissant de mots de Lyndon: $w = l_1^{\alpha_1} l_2^{\alpha_2} \ldots l_n^{\alpha_n}$ avec $l_1 > l_2 > \cdots > l_n$ comme dans (30), il est possible d'indicer la base PBW par des mots $w \in X^*$ et de noter P_w un élément de cette base. Notons $\mathcal{B} = \{P_w \mid w \in X^*\}$ la base PBW obtenue (elle est bien homogène).

C. Reutenauer [4] donne une méthode constructive pour construire la base duale graduée

$$\mathcal{B}^* = \{P_w^* \mid w \in X^*\}$$

basée principalement sur la formule (29). On a, par définition, $(P_u | P_v^*) = \delta_{u,v}$ (symbole de Kroneker) pour tous mots $u, v \in X^*$.

Le choix de la base de Lyndon est justifié par le fait que les MZV sont codées par des mots $w \in X^*$ avec $X = \{x_0, x_1\}$. Le nombre $\zeta(w)$ est convergent ssi $w \in x_0 X^* x_1$. Dans ce cas, le mot est dit convergent. Un polynome est dit convergent lorsqu'il est une combinaison linéaire de mots tous convergents. On vérifie que les mots de Lyndon pour l'ordre $x_0 < x_1$ sont tous convergents sauf les deux lettres x_0 et x_1. On a le lemme

Lemme 1 *L'élément $P_w^* \in \mathcal{B}^*$ est convergent ssi $w \in X^*$ est convergent.*

4.4 Factorisation d'une exponentielle de Lie

Soit une série génératrice définie comme en (18) qui est une exponentielle de Lie. Alors, on a la factorisation

$$\sum_{w \in X^*} f(w)\ w = \prod_{l \in \mathcal{L}} \exp[f(l^*)\ l]. \tag{31}$$

La preuve découle du fait que si φ est un morphisme entre deux $\mathbb{Q}$-algèbres A et B, il existe une unique prolongation $\tilde{\varphi} : A\langle\langle X\rangle\rangle \to B\langle\langle X\rangle\rangle$ telle que $\tilde{\varphi}(x) = x$ pour tout $x \in X$. Dans ce cas, on vérifie que $\tilde{\varphi}$ commute aux produits et aux exponentielles. On applique alors la prolongation $\tilde{f}$ de la fonction f aux deux membres de la formule (28).

Comme exemple d'application, prenons le procédé de régularisation des MZV en respectant le produit de mélange ш. L'application reg : $\mathrm{Sh}_{\mathbb{Q}}(X) \to \mathrm{Sh}_{\mathbb{Q}}(X)$, pour $X = \{x_0, x_1\}$, est par définition, l'unique application $\mathbb{Q}$-linéaire telle que

1. $\text{reg}(p \sqcup\!\sqcup\, q = \text{reg}(p) \sqcup\!\sqcup\, \text{reg}(q), \quad \forall p, q \in \text{Sh}_{\mathbb{Q}}(X)$,

2. $\text{reg} w = w$ si $w \in x_0 X^* x_1$,

3. $\text{reg} x_0 = \text{reg} x_1 = 0$.

On déduit de tout ce qui précède que la série génératrice du morphisme reg vaut

$$\begin{aligned}
\sum_{w \in X^*} \text{reg}(w) \otimes w &= \exp(-x_1 \otimes x_1) \Big(\sum_{w \in X^*} w \otimes w \Big) \exp(-x_0 \otimes x_0) \\
&= \prod_{l \in \mathcal{L}yndon(X) - \{x_0, x_1\}} \exp(P_l^* \otimes P_l).
\end{aligned}$$

References

[1] J. Berstel and C. Reutenauer. *Les séries rationnelles et leurs langages.* Etudes et Recherches en Informatique. Masson, 1984.

[2] A. Connes and D. Kreimer. Hopf algebras, renormalisation and noncommutative geometry. *IHES/M/98/60*, 1998.

[3] A. Guichardet. *Groupes quantiques: introduction au point de vue formel.* Cnrs Editions, Paris, 1995.

[4] C. Reutenauer. *Free Lie Algebras*, volume New Series-7 of *London Mathematical Society Monographs.* Oxford Science Publications, 1993.

[5] M. Rosso. Groupes quantiques: origines et applications. *Journal CNRS*, 1993.

[6] M. Schatzman. Analyse numérique des équations différentielles ordinaires. Cours de dea, Université Lyon I, 2000.