CALCUL FORMEL
DEA Informatique

G. Jacob, N.E. Oussous et M. Petitot

7 novembre 2000

UNIVERSITE DES SCIENCES ET TECHNOLOGIES DE LILLE
U.F.R. d'I.E.E.A. Bât. M3, 59655 VILLENEUVE D'ASCQ CEDEX, Tél. 20 43 47 24

Table des matières

1

Quelques Rappels Mathématiques

1.1 Introduction

Dans ce chapitre, on va exposer quelques structures algébriques qui seront utilisées dans le module "Calcul Formel". On ne donnera que les définitions et quelques exemples pour les illustrer. Les personnes intéressées par les détails peuvent consulter des ouvrages de mathématiques plus complets.

1.2 Ensembles et relations d'équivalence

1.2.1 Ensembles

On peut considérer un ensemble simplement comme une *collection* d'objets spécifiés. Si A est un ensemble et si x est un objet de cet ensemble, on écrit $x \in A$ et on lit x appartient à A.

Un ensemble B est un sous-ensemble d'un autre ensemble A si tout élément de B est élément de A, on dira que B est *inclus* dans A ou que A *contient* B et on notera $B \subset A$.

Deux ensembles A et B sont *égaux* si tout élément de A est élément de B et réciproquement. On écrira $A = B$.

L'*ensemble vide,* noté ϕ est l'ensemble qui ne contient aucun élément. ϕ est inclus dans tout ensemble.

On appelera *singleton* tout ensemble formé d'un seul élément. Si cet élément est noté x, l'ensemble sera noté $\{x\}$.

On notera $\{x : P(x)\}$ l'ensemble de tous les éléments qui vérifient la propriété $P(x)$.

Pour les ensembles des nombres, on utilise couramment les symboles suivants :

- $\mathbb{N} = \{0,1,2,\dots\}$ l'ensemble des entiers naturels.
- $\mathbb{Z} = \{\dots, -2, -1,0,1,2,\dots\}$ l'ensemble des entiers relatifs.
- $\mathbb{Q} = \{x/y \mid x,y \in \mathbb{Z}, y \neq 0\}$ l'ensemble des nombres rationnels.
- $\mathbb{R}$ l'ensemble des nombres réels.

– $\mathbb{C} = \{x + iy | x,y \in \mathbb{R}\}$ avec $i^2 = -1$ l'ensemble des nombres complexes.

On a la chaine : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Sur les ensembles, on peut définir plusieurs opérations pour obtenir de nouveaux ensembles.

1. L'*union* de deux ensembles par : $A \cup B = \{x | x \in A \text{ ou } x \in B\}$.
2. L'*intersection* de deux ensembles par : $A \cap B = \{x | x \in A \text{ et } x \in B\}$.
3. La *différence* de deux ensembles par : $A \setminus B = \{x | x \in A \text{ et } x \notin B\}$.
4. Le *produit cartésien* de deux ensembles par : $A \times B = \{(x,y) | x \in A \text{ et } y \in B\}$. Les éléments de cet ensemble sont appelés des *couples*.
5. A partir d'un ensemble A, on peut former l'ensemble, noté $\mathcal{P}(A)$, de tous les sous-ensembles de A qu'on appelle *ensemble des parties* de A. $\mathcal{P}(A) = \{B | B \subset A\}$. L'ensemble vide ϕ et A lui-même appartiennent à $\mathcal{P}(A)$.

Définition 1.1 *Une partition d'un ensemble S est un ensemble $\pi \subset \mathcal{P}(S)$ de parties de S, tel que :*

a. Si $A \in \pi$, alors $A \neq \phi$.
b. Si $A,B \in \pi$, alors soit $A = B$ soit $A \cap B = \phi$.
c. Tout élément de S est dans un élément de π.

Exemple 1.1 Soit $S = \{1,2,3,4,5,6,7,8,9\}$. L'ensemble $\pi = \{\{1,4\},\{3,6,8\},\{2,9\},\{5,7\}\}$ est une partition de S.

Proposition 1.1 *Soient A,B et C trois ensembles. Alors*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

On dit que $\cap$ est distributive *par rapport à $\cup$.*

1.2.2 Relations d'équivalence

Une *relation binaire* R sur un ensemble A peut être définie comme étant un sous-ensemble de $A \times A$. On notera R^{-1} la relation appelée *inverse* de R et définie par $R^{-1} = \{(y,x) | (x,y) \in R\}$.

Définition 1.2 *Une relation E sur un ensemble A est une relation d'équivalence si elle satisfait les trois propriétés suivantes :*

1. $(x,x) \in E$ pour tout $x \in A$ (réflexivité)
2. $(x,y) \in E$ implique que $(y,x) \in E$ (symétrie)
3. $(x,y) \in E$ et $(y,z) \in E$ implique que $(x,z) \in E$ (transitivité).

On écrit $x \equiv_E y$ (ou simplement $x \equiv y$) pour $(x,y) \in E$ et on lit x est *équivalent* à y.

Soit A un ensemble muni d'une relation d'équivalence. Pour chaque élément $x \in A$, on construit l'ensemble $\bar{x} = \{y \in A | x \equiv y\}$. Cet ensemble est appelé la *classe d'équivalence* de x. Par la réflexivité, on montre que $x \in \bar{x}$. Un élément quelconque de $\bar{x}$ est appelé un représentant de $\bar{x}$.

On appelle *ensemble quotient* de A par la relation d'équivalence, l'ensemble

$$A/_{\equiv} \quad = \quad \{\bar{x} | x \in A\}.$$

Exemple 1.2 Sur l'ensemble $\mathbb{Z} \times \mathbb{Z}^*$, on définit la relation suivante :

$$(x,y) \equiv (x',y') \quad \text{si} \quad xy' = x'y.$$

On peut montrer facilement que c'est une relation d'équivalence. L'ensemble quotient $\mathbb{Z} \times \mathbb{Z}^*/_{\equiv}$ peut être identifié à l'ensemble des nombres rationnels $\mathbb{Q}$. Les éléments de $\mathbb{Q}$ sont représentés par des quotients $x/y, \quad x \in \mathbb{Z}, y \in \mathbb{Z}^*$, et $x/y = x'/y'$ si $xy' = x'y$. Ainsi, un élément de $\mathbb{Q}$ est précisément une classe d'équivalence.

Proposition 1.2 *Soit E une relation d'équivalence sur un ensemble A. Alors, l'ensemble quotient $A/E = \{\bar{a} | a \in A\}$ est une partition de A. Réciproquement, si π est une partition de A, alors on peut lui associer une relation d'équivalence dont l'ensemble quotient est exactement π.*

La démonstration de cette proposition est facile et est laissée aux lecteurs.

1.3 Monoïdes

Soit M un ensemble muni d'une *opération interne* binaire[1], notée multiplicativement '$\cdot$'. Cette opération sera dite *associative* si elle vérifie :

$$\forall\, x,y,z \in M, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Un élément $e \in M$ sera dit *élément neutre* pour cette opération si,

$$\forall\, x \in M, \quad x \cdot e = e \cdot x = x.$$

Définition 1.3 *Un monoïde est un ensemble M muni d'une opération interne binaire '$\cdot$' associative et admettant un élément neutre qu'on notera* 1.

Si l'opération $(\cdot)$ est *commutative,* c'est-à-dire :

$$\forall\, x,y \in M, \quad x \cdot y = y \cdot x,$$

alors le monoïde sera dit *commutatif.*

Le monoïde sera noté $\langle M, \cdot ,1\rangle$ et simplement M s'il n'y a pas de confusion.

Exemples 1.1

1. L'ensemble $\mathbb{N}^+ = \{1,2,\ldots\}$ muni de la multiplication est un monoïde commutatif.
2. De même, $\mathbb{N}$ muni de l'addition est un monoïde commutatif.

1. C'est une application de $M \times M$ dans M.

1.4 Groupes

Soit M un ensemble muni d'une opération interne admettant un élément neutre e. Un élément $x \in M$ admet un *inverse,* noté x^{-1}, si

$$x \cdot x^{-1} = x^{-1} \cdot x = e.$$

Définition 1.4 *Un groupe est un monoïde dans lequel tout élément admet un inverse.*

Un groupe sera dit *commutatif* si l'opération $(\cdot)$ est commutative.

Exemples 1.2

1. L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de l'addition, est un groupe commutatif.
2. L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de la multiplication, n'est pas un groupe.
3. L'ensemble $\mathbb{Q}$ (resp. $\mathbb{Q}^*$) des nombres rationnels, muni de l'addition (resp. la multiplication), est un groupe commutatif.

Soit B un sous-ensemble d'un groupe $(G, \cdot)$. B est un *sous-groupe* de G si pour tous x et y dans B, $x \cdot y \in B$ et $x^{-1} \in B$.

1.5 Anneaux

1.5.1 Anneau

Définition 1.5 *Un anneau A est un groupe commutatif, noté additivement dans la suite, muni d'une application (loi de composition* interne*) $(x,y) \longmapsto xy$ de $A \times A$ dans A vérifiant, pour tout $x,y,z \in A$:*

$$\begin{array}{rcll} x(yz) & = & (xy)z & (\textit{associativité}) \\ x(y+z) & = & xy + xz & (\textit{distributivité à droite}) \\ (x+y)z & = & xz + yz & (\textit{distributivité à gauche}) \end{array}$$

L'inverse de x pour l'addition est appelé symétrique de x et noté $-x$.

L'élément xy est appelé le *produit* des éléments x et y. Cet anneau sera noté $\langle A, +, \cdot \rangle$ ou simplement A s'il n'y a pas de confusion.

A sera dit à *élément neutre* s'il existe un élément de A, noté 1, tel que :

$$x \cdot 1 \; = \; 1 \cdot x \; = \; x \quad \forall x \in A.$$

Cet élément est *unique.*

L'anneau A sera dit *commutatif* si le produit est commutatif, c'est-à-dire,

$$\forall x,y \in A, \quad xy = yx$$

Exemple 1.3 L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de l'addition et de la multiplication, est un anneau commutatif à élément unité.

1.5.2 Sous-anneau

Soit B un sous-ensemble d'un anneau $(A,+,\cdot)$. B est un *sous-anneau* de A si $(B,+)$ est un sous-groupe de $(A,+)$, $1 \in B$ et

$$\forall\, x,y \in B, \qquad x \cdot y \in B \quad \text{(c-à-d } B \text{ est stable pour le produit).}$$

Soit $(A,+,\cdot)$ un anneau dont les éléments neutres sont 0 et 1 pour l'addition '+' et la multiplication '$\cdot$' respectivement.

Si $0 \neq \underbrace{1+1+\cdots+1}_{n\ \texttt{fois}}$ pour tout $n > 0$ Alors A est dit de *caractéristique* nulle. Sinon, on verra plus loin comment la calculer.

Exemple 1.4 Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle.

Définition 1.6 *Un élément $a \neq 0$ d'un anneau commutatif A est un diviseur de zéro s'il existe $b \neq 0$ dans A tel que $ab = 0$ (b est alors aussi un diviseur de zéro).*

Définition 1.7 *Un élément $u \neq 0$ d'un anneau commutatif A est un élément unité (ou inversible) s'il existe $v \neq 0$ dans A tel que $uv = 1$ (on notera $v = u^{-1}$).*

Exemple 1.5 $(\mathbb{Z}/_{\equiv_m},+,\cdot)$ où $\equiv_m$ est la *congruence modulo m*. On vérifie facilement que c'est un anneau commutatif. On définit la *somme* (resp. le *produit*) de deux classes d'équivalence comme étant la classe de la somme (resp. du produit) des représentants des deux classes.

Si $m = 6$, alors $\mathbb{Z}/_{\equiv_6} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$. On a

$$\bar{2}\cdot\bar{3} \;=\; \overline{2\cdot 3} \;=\; \bar{6} \;=\; \bar{0}$$

Ainsi, $\bar{2} \neq \bar{0}$ et $\bar{3} \neq \bar{0}$ et leur produit est égal à $\bar{0}$. Donc $\bar{2}$ et $\bar{3}$ sont des diviseurs de $\bar{0}$.

Si $m = 5$, alors $\mathbb{Z}/_{\equiv_5} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$. L'anneau $\mathbb{Z}/_{\equiv_5}$ n'admet pas de diviseurs de zéro. D'une manière générale, si m est premier, alors $\mathbb{Z}/_{\equiv_m}$ n'a pas de diviseurs de zéro.

D'autre part, tout élément non nul de $\mathbb{Z}/_{\equiv_5}$ est inversible et l'on a :

$$\bar{2}^{-1} \;=\; \bar{3}, \qquad \bar{3}^{-1} \;=\; \bar{2}, \qquad \bar{4}^{-1} \;=\; \bar{4}.$$

Un élément d'un anneau ne peut pas être à la fois unité et diviseur de zéro. Un anneau sera dit *non trivial* s'il n'est pas réduit à 0 et à ses unités.

Définition 1.8 *Un anneau commutatif et non trivial est dit intègre s'il n'a pas de diviseur de zéro.*

1.5.3 Idéaux

Définition 1.9 *Soient A un anneau. Un sous-ensemble $\mathcal{I}$ de A est un idéal à droite (resp. à gauche) de A si $(\mathcal{I},+)$ est un sous-groupe de $(A,+)$ et si*

$$x \in \mathcal{I} \text{ et } a \in A \quad\Longrightarrow\quad x\cdot a \in \mathcal{I} \ (\text{resp. } a\cdot x \in \mathcal{I}).$$

On dira que $\mathcal{I}$ est un idéal bilatère de A s'il est à la fois idéal à droite et à gauche.

Si l'anneau A est *commutatif,* les notions d'idéaux à droite, à gauche et bilatère coïncident et on dit simplement *idéal.*

Exemples 1.3

1. Le sous-ensemble $2\mathbb{Z}$ des entiers relatifs pairs, de l'anneau $\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
2. Soit $A = \mathbb{Z} \times \mathbb{Z}$ muni des deux opérations '$+$' et '$\cdot$' définies par :

$$\begin{aligned} (n,m) + (n',m') &= (n + n',m + m') \\ (n,m) \cdot (n',m') &= (nn',mm') \end{aligned}$$

   A est un anneau d'élément unité le couple $(1,1)$. Le sous-ensemble $B = \mathbb{Z} \times \{0\}$ est un idéal de A. C'est un anneau, *isomorphe* à $\mathbb{Z}$, d'élément unité $(1,0)$.

1.6 Corps

Définition 1.10 *Soit C un anneau. C est un corps si C est commutatif (la multiplication est commutative), admet un élément unité (noté 1) et tout élément non nul de C admet un inverse :*

$$\forall x \in C \setminus \{0\},\ \exists x^{-1} \in C \text{ tel que } xx^{-1} = x^{-1}x = 1.$$

Exemples 1.4

1. $(\mathbb{Z}, +, \cdot)$ n'est pas un corps.
2. $(\mathbb{Q}, +, \cdot)$ est un corps. Le corps des nombres rationnels.
3. $(\mathbb{R}, +, \cdot)$ est un corps. Le corps des nombres réels.

Remarque 1.1 *Un corps est un anneau intègre.*

Exemple 1.6 $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps qui ont un nombre infini d'éléments.

Il existe des corps qui ont un nombre fini d'éléments qu'on appelle des *corps de Galois.*

Exemple 1.7 $\{0,1\}$ muni de l'addition modulo 2 et de la multiplication est un corps de Galois noté $CG(2)$.

On considère un corps de Galois de q éléments, $CG(q)$. On forme la séquence des sommes :

$$\sum_{1\le i\le k} 1 = \underbrace{1 + 1 + \cdots + 1}_{k \text{ fois}}, \qquad k = 1,2,3,\ldots$$

Puisque le corps est stable pour l'addition, ces sommes sont toutes des éléments de $CG(q)$. Comme $CG(q)$ est fini, il doit y avoir des répétitions dans ces sommes; c'est-à-dire, il existe k',k'' des entiers positifs, $k' < k''$ tels que

$$\sum_{1\le i\le k'} 1 = \sum_{1\le i\le k''} 1 \implies \sum_{1\le i\le k''-k'} 1 = 0$$

Il doit donc existter un plus petit entier positif λ tel que

$$\sum_{1 \leq i \leq \lambda} 1 = 0.$$

Cet entier λ est appelé la *caractéristique* du corps $CG(q)$.

Exemple 1.8 La caractéristique de $CG(2)$ est 2 car $1 + 1 = 0$.

2

Des mots sans les maux

2.1 Introduction

Le but de ce cours de CALCUL FORMEL (CF) est de vous donner les bases de l'algèbre non commutative et l'application de cette algèbre dans le calcul des tables des relations entre les valeurs des MZV (MULTIPLE ZÊTA VALUES).

2.1.1 Quelques définitions

La fonction zêta de Riemann est définie, pour tout entier naturel positif k, par la série suivante :

$$\zeta(k) \quad = \quad \sum_{n>0} \frac{1}{n^k} \tag{2.1}$$

Cette série converge pour $k \geq 2$.

La fonction zêta multi-indicée (ou MULTIPLE ZÊTA VALUES : MZV) est quand à elle définie, pour tout multi-indice d'entiers $s = (s_1,s_2,\ldots,s_k)$, par la série suivante :

$$\zeta(s) \quad = \quad \sum_{n_1>n_2>\cdots>n_k>0} \frac{1}{n_1^{s_1} n_2^{s_2} \cdots n_k^{s_k}} \tag{2.2}$$

$\zeta(s)$ converge pour $s_1 \geq 2$.

2.1.2 Question

Comment définir les relations entre les MZV ?

L'équipe canadienne de Borwein utilise des méthodes numériques pour identifier les coefficients des valeurs des MZV ce qui leur permet de déduire des relations entre ces valeurs.

A Lille, on utilise la combinatoire des mots, en particulier les mots de Lyndon, pour vérifier des relations entre les valeurs des MZV mais aussi pour en découvrir des nouvelles.

Essayez de montrer par exemple la relation :

$$\zeta(3) \quad = \quad \zeta(2,1)$$

Autrement dit, montrez l'égalité :

$$\sum_{k>0} \frac{1}{k^3} = \sum_{n>m>0} \frac{1}{n^2 \cdot m}$$

Pour étudier la méthode *Lilloise*, on doit se former à l'algèbre non commutative : étude des mots, des polynômes et des séries non commutatifs. Étude des algèbres de Lie et de leurs bases. Étude des exponentielles de Lie. Étude des algèbres de Hopf ...

2.2 Les mots d'abord

2.2.1 Définitions de base

Le but est de définir les mots de Lyndon et leurs propriétés. Soit X un alphabet fini (ensemble de symboles. Par exemple $\{x_0,x_1\},\{a,b\},\{0,1\},\dots$). On appelle mot sur X toute suite finie de lettres de X. Par exemple $w = x_0x_1x_0x_0x_1$ est un mot de cinq lettres sur l'alphabet $X = \{x_0,x_1\}$. La suite vide sera notée ε et appelée *mot vide*. L'ensemble des mots sur l'alphabet X sera noté X^*. On notera aussi $X^+ = X^* \setminus \{\varepsilon\}$.

Sur X^*, on définit une opération interne notée « $\cdot$ » et appelée opération ou produit de *concaténation*, comme suit : si $u = x_0x_1x_0$ et $v = x_0x_1$ alors $u \cdot v = x_0x_1x_0x_0x_1$ (c'est la juxtaposition des lettres de u et de celles de v). Il est clair que ε est l'élément neutre pour ce produit ($u \cdot \varepsilon = \varepsilon \cdot u = u$ pour tout $u \in X^*$). Il est également évident que ce produit n'est pas commutatif ($u \cdot v$ est en général différent de $v \cdot u$). Par contre, il est associatif ($(u \cdot v) \cdot w = u \cdot (v \cdot w)$).

$$\begin{array}{rcl} x_0x_1x_0 \cdot x_0x_1 & \neq & x_0x_1 \cdot x_0x_1x_0 \\ (x_0x_1x_0 \cdot x_0x_1) \cdot x_1 & = & x_0x_1x_0 \cdot (x_0x_1 \cdot x_1) \ = \ x_0x_1x_0x_0x_1x_1 \end{array}$$

$(X^*, \cdot)$ est le *monoïde libre non commutatif* sur l'alphabet X.

On appelle longueur d'un mot u que l'on note $|u|$, le nombre de lettres qui constituent ce mot. Ainsi, $|x_0x_1x_0| = 3$ et $|\varepsilon| = 0$.

On peut définir récursivement la longueur d'un mot comme suit :

$$|w| = \begin{cases} 0 & \text{si } w = \varepsilon \\ 1 + |u| & \text{si } w = xu \text{ avec } x \in X. \end{cases}$$

On notera X^n l'ensemble des mots sur X de longueur n et $X^{\leq n}$ l'ensemble des mots sur X de longueur inférieure ou égale à n. On a ainsi :

$$X^* = \bigcup_{i=0}^{\infty} X^i$$

Si X est ordonné (on a un ordre sur les lettres. Par exemple $x_0 < x_1$), alors on peut définir différents ordres sur X^*. Souvent, on se sert des deux ordres suivants :

– L'ordre *lexicographique* défini pour tous mots u et v de X^* par :

$$u < v \iff \begin{cases} \quad \exists\, w \in X^+ \text{ tel que } uw = v \\ \text{ou} \\ \quad \exists\, w_1,w_2,w_3 \in X^* \text{ et } x,y \in X \text{ tels que} \\ \qquad\qquad u = w_1xw_2 \quad v = w_1yw_3 \text{ et } x < y. \end{cases}$$

Par exemple $x_0x_1 < x_0x_1^2$ et $x_0x_1x_0x_1^2 < x_0x_1x_1$.

– L'ordre *lexicographique par longueur* défini pour tous mots u et v de X^* par :

$$u < v \iff \begin{cases} \quad |u| < |v| \\ \text{ou} \\ \quad |u| = |v| \text{ et } u < v \text{ pour l'ordre lexicographique.} \end{cases}$$

Par exemple $x_0x_1 < x_1x_0$ et $x_1 < x_0x_1$.

2.2.2 Opérations sur les mots

Soit $u \in X^*$. On définit le *résiduel à gauche* (resp. *à droite*) de u par la lettre $x \in X$, que l'on note $x \triangleleft u$ (resp. $u \triangleright x$), comme étant le mot $v \in X^*$ tel que $u = vx$ (resp. $u = xv$) si v existe et 0 sinon. Autrement dit

$$x \triangleleft u = \begin{cases} v & \text{si } u = vx, \quad v \in X^* \\ 0 & \text{sinon} \end{cases}$$

$$\left(\text{resp.} \quad u \triangleright x = \begin{cases} v & \text{si } u = xv, \quad v \in X^* \\ 0 & \text{sinon} \end{cases}\right)$$

Dans la suite, on s'intéresse aux résiduels à gauche sachant que l'on a les mêmes propriétés pour les résiduels à droite.

L'opération $\triangleleft$ est une *action à gauche* qui vérifie

$$y \triangleleft (x \triangleleft u) = (yx) \triangleleft u, \quad x,y \in X, \quad u \in X^*.$$

On peut donc étendre la notion de résiduel aux mots en posant

$$(vx) \triangleleft u = v \triangleleft (x \triangleleft u), \quad x \in X, \quad u,v \in X^*.$$

On a également la propriété suivante :

$$(u \triangleleft v) \triangleright w = (u \triangleleft (v \triangleright w), \quad u,v,w \in X^*.$$

2.2.3 Facteurs et conjugués d'un mot

Un mot $u \in X^*$ est un *facteur* d'un mot $v \in X^*$ s'il existe deux mots $w_1,w_2 \in X^*$ tels que

$$v = w_1uw_2$$

Un mot $u \in X^*$ est dit *facteur gauche* (resp. *droit*) d'un mot $v \in X^*$ s'il existe un mot $w \in X^*$ tel que

$$v \;=\; uw \qquad (\text{resp. } v \;=\; wu)$$

u est facteur gauche ou droit *propre*, si $w \neq \varepsilon$ et $u \neq \varepsilon$.

Exemple 2.1 *Soit le mot $v = x_0x_1x_1x_0x_1$. L'ensemble de ses facteurs droits est :*

$$\{x_1,\, x_0x_1,\, x_1x_0x_1,\, x_1x_1x_0x_1,\, x_0x_1x_1x_0x_1\}$$

Et l'ensemble de ses facteurs droits propres est :

$$\{x_1,\, x_0x_1,\, x_1x_0x_1,\, x_1x_1x_0x_1\}$$

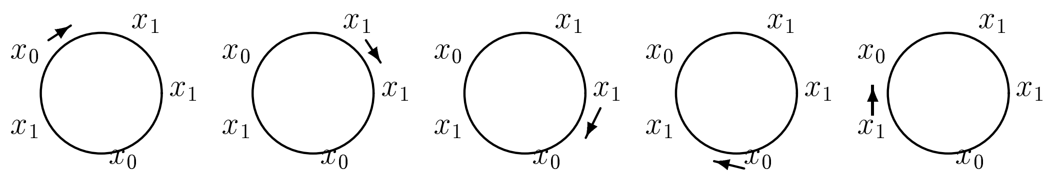
Deux mots w_1 et w_2 sont dits *conjugués* s'il existe deux mots u et v de X^+ tels que $w_1 = uv$ et $w_2 = vu$.

Soit $u \in X^*$. La *classe de conjuguaison* de u est l'ensemble de ses conjugués.

Exemple 2.2 *Soit le mot $v = x_0x_1x_1x_0x_1$. L'ensemble de ses conjugués est :*

$$\{x_0x_1x_1x_0x_1,\, x_1x_1x_0x_1x_0,\, x_1x_0x_1x_0x_1,\, x_0x_1x_0x_1x_1,\, x_1x_0x_1x_1x_0\}$$

On remarque de l'on obtient la classe de conjuguaison de w en plaçant les lettres de w sur un cercle et en enumérant tous les mots obtenus en accédant au cercle par ses différentes lettres.



$x_0x_1x_1x_0x_1$ $\quad$ $x_1x_1x_0x_1x_0$ $\quad$ $x_1x_0x_1x_0x_1$ $\quad$ $x_0x_1x_0x_1x_1$ $\quad$ $x_1x_0x_1x_1x_0$

2.3 Mots de Lyndon

Un mot $l \in X^*$ est un *mot de Lyndon* s'il est strictement plus petit, pour l'ordre lexicographique, que chacun de ses facteurs droits propres.

Ainsi, le mot w de l'exemple 2.1 n'est pas un mot de Lyndon car il est plus grand que x_0x_1 qui est un de ses facteurs droits propres. Par contre, le mot $l = x_0x_0x_1x_0x_1$ est un mot de Lyndon. Vérifiez le.

Une autre définition des mots de Lyndon : $l \in X^*$ est un *mot de Lyndon* s'il est strictement plus petit, pour l'ordre lexicographique, que chacun de ses conjugués propres. En particulier, les lettres sont des mots de Lyndon. Vérifez que $l = x_0x_0x_1x_0x_1$ est un mot de Lyndon au sens de cette deuxième définition.

Exercice 2.1 *Montrez que les deux définitions sont équivalentes.*

On notera $\mathcal{L}yndon(X)$, l'ensemble des mots de Lyndon sur l'alphabet X.

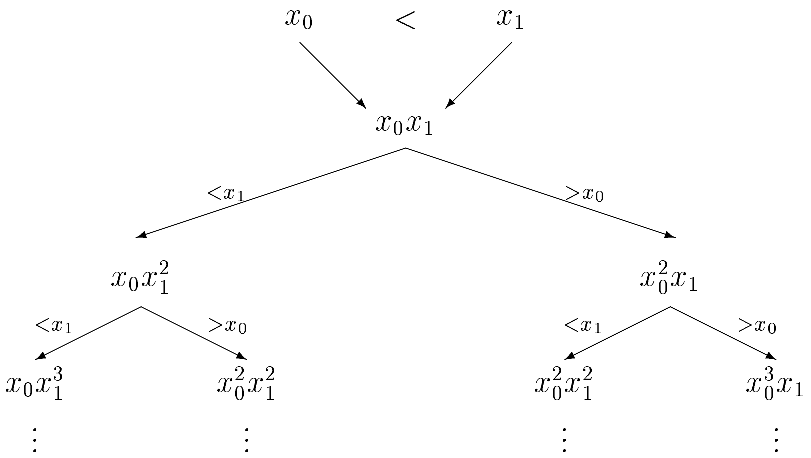
Proposition 2.1 *Si l_1 et l_2 sont deux mots de Lyndon, alors l_1l_2 est un mot de Lyndon si et seulement si $l_1 < l_2$ (pour l'ordre lexicographique).*

Preuve :

A faire en exercice ;-) $\diamondsuit$

Cette proposition donne un algorithme simple pour engendrer les mots de Lyndon par longueur en partant des lettres de l'alphabet ordonné X. Les lettres sont des mots de Lyndon.

Exemple 2.3 *Soit $X = \{x_0,x_1\}$ un alphabet ordonné avec $x_0 < x_1$. x_0 et x_1 appartiennent à $\mathcal{L}yndon(X)$. Comme $x_0 < x_1$, alors $x_0x_1 \in \mathcal{L}yndon(X)$. Comme $x_0 < x_0x_1$, alors $x_0^2x_1 \in \mathcal{L}yndon(X)$ ...*



Cet algorithme produit $x_0^2x_1^2$ deux fois !

Exercice 2.2 *Écrivez cet algorithme en Maple. Attention aux doublons.*

Proposition 2.2 *Soient l_1,l_2 et l trois mots de Lyndon tels que $l_1 < l$ et $l_2 < l$, alors $l_1l_2 < l$.*

Preuve :

A faire en exercice ;-) $\diamondsuit$

Proposition 2.3 *Soit $w \in \mathcal{L}yndon(X) \setminus X$ et soit m son plus long facteur droit propre dans $\mathcal{L}yndon(X)$. Si $w = lm$, alors l est aussi un mot de Lyndon et $l < lm < m$. Le couple $\sigma(w) = (l,m)$ est appelé* factorisation standard *de w.*

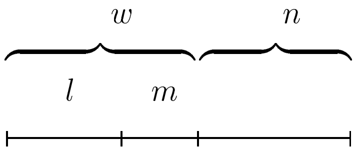
Lemme 2.1 *Soient $w \in \mathcal{L}yndon(X) \setminus X$ et $\sigma(w) = (l,m)$ sa factorisation standard, et soit $n \in \mathcal{L}yndon(X)$ un mot de Lyndon vérifiant $w < n$. Alors le couple (w,n) est la factorisation standard du mot wn si et seulement si $n \leq m$.*

Preuve :

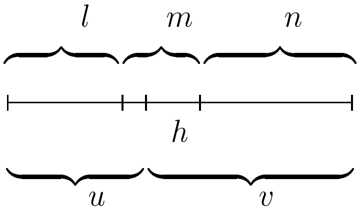
(a) Montrons que $\sigma(wn) = (w,n) \Longrightarrow n \leq m$.

Supposons que $m < n$. Alors, d'après la proposition 2.1, $mn \in \mathcal{L}yndon(X)$ et donc n n'est pas le plus facteur droit propre de wn ce qui contredit l'hypothèse : $\sigma(wn) = (w,n)$.

(b) Supposons que $w < n \leq m$ et que $\sigma(wn) = (u,v)$ avec $v \neq n$.



On a alors nécessairement $|v| > |n|$. Donc $v = hn$ où h est un facteur droit propre de w.



Soit alors k le plus petit facteur droit, différent de ε, propre ou non de h. On a lors $k < m$. En effet,

$$k \leq h < hn \quad = \quad v < n \leq m.$$

Or $m \leq k$, puisque k est un facteur droit propre de w, et que $\sigma(w) = (l,m)$. D'où la contradiction.

$\diamondsuit$

2.4 Listes standard et théorème de Lyndon

Définition 2.1 *Soit $L = [u_1,u_2,\ldots,u_n]$ une liste d'éléments de X^+. On dira que L est* standard *si et seulement si elle vérifie la propriété suivante :*

$$(S) \quad \left\{ \begin{array}{ll} & u_i \textit{ est une lettre,} \\ \textit{ou} & \\ & \textit{si } \sigma(u_i) = (x,y), \textit{ alors } y \geq u_j \textit{ pour tout } j \geq i \end{array} \right.$$

Si tous les éléments de L sont des lettres, alors L vérifie (S).

Si L est décroissante (c-à-d $u_1 \geq u_2 \geq \cdots \geq u_n$), alors elle vérifie (S).

Définition 2.2 *Soit $L = [u_1,u_2,\ldots,u_n]$ une liste d'éléments de X^+. On appelle* inversion *tout couple (u_i,u_{i+1}) tel que $u_i < u_{i+1}$.*

Théorème 2.1 *Tout mot $w \in X^+$ se décompose de manière unique comme produit décroissant de mots de Lyndon :*

$$w \quad = \quad l_1 l_2 \cdots l_n$$

où $l_i \in \mathcal{L}yndon(X)$ et $l_1 \geq l_2 \geq \cdots \geq l_n$.

Preuve :

Comme preuve de ce théorème, donnons un algorithme permettant de construire la décomposition d'un mot en produit décroissant de mots de Lyndon.

On se donne le mot $w = x_1x_2 \ldots x_n \in X^+$ à décomposer. On construit la liste L de ses lettres : c'est une liste standard (de mots de Lyndon).

On parcourt cette liste de droite à gauche. Si l'on trouve une inversion (x_i,x_{i+1}), alors on remplace dans L les deux éléments x_i et x_{i+1} par le produit x_ix_{i+1} qui est un mot de Lyndon. On recommence avec la nouvelle liste. Si au contraire, aucune inversion n'est trouvée, c'est que la liste est une liste décroissante de mots de Lyndon. Il suffit alors de faire le produit des éléments de L pour avoir la décomposition de w en produit décroissant de mots de Lyndon. $\diamondsuit$

Exercice 2.3 *Implantez cet algorithme en Maple et en faire la preuve.*

3

Polynômes et séries en variables non commutatives

3.1 Introduction

Dans ce chapitre, nous allons définir la notion de polynôme et de série en variables non commutatives. Ensuite, nous considérons un ensemble d'opérations sur ces objets. Ces opérations pemettent de définir différentes structures sur l'ensemble des polynômes mais aussi sur l'ensemble des séries formelles.

3.2 Polynômes non commutatifs

Soit $X = \{x_0, \ldots ,x_n\}$ un alphabet fini comme défini dans le chapitre précédent. X^* est le monoïde libre engendré par X (ensemble des mots sur X). On a défini sur X^* un produit appelé *concaténation* et noté m ou "$\cdot$". La concaténation de deux mots u et v de X^* est notée $m(u,v)$ ou $u \cdot v$ ou encore plus simplement uv.

Soit K un corps (qui peut être $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$). On appelle *polynôme non commutatif* sur X à coefficients dans K, toute combinaison linéaire "finie" de mots. On le note :

$$P \quad = \quad \sum_{w \in X^*} \alpha_w \, w \qquad \text{avec } \alpha_w \in K$$

Cette somme est finie (les coefficients α_w sont tous nuls sauf un nombre fini d'entre eux).

Le coefficient α_w du mot w dans le polynôme P sera noté $\langle P|w\rangle$. L'ensemble des polynômes sur X à coefficients dans K sera noté $K\langle X\rangle$.

On appelle *support* du polynôme P, noté $\mathrm{Supp}(P)$, l'ensemble des mots $w \in X^*$ dont le coefficient est non nul ($\alpha_w \neq 0$).

On appelle *degré* du polynôme P, noté $\deg(P)$, la longueur du plus long mot de $\mathrm{Supp}(P)$:

$$\deg(P) \quad = \quad \begin{cases} \max\{\ |w|,\, w \in \mathrm{Supp}(P)\ \} & \text{si } P \neq 0 \\ -\infty & \text{si } P = 0 \end{cases}$$

Ainsi, le degré d'un polynôme réduit à une constante est 0.

3.3 Structures sur $K\langle X\rangle$

Notons $+$ et $*$ les opérations du corps K. Ces opérations induisent sur $K\langle X\rangle$ les opérations suivantes :

3.3.1 Addition

Soient P et Q deux éléments de $K\langle X\rangle$, on pose

$$P+Q \;=\; \sum_{w\in X^*} \langle P+Q|w\rangle\, w \;=\; \sum_{w\in X^*} (\langle P|w\rangle + \langle Q|w\rangle)\, w$$

Cette opération est bien sûr commutative, associative et admet comme élément neutre le polynôme identiquement nul que l'on note 0.

Exemple 3.1 *Soit $X=\{a,b\}$. Soient les polynômes $P = 2\,aba + aab - 3\,abb$ et $Q = -aba + 5\,abb$. Alors*

$$P+Q \;=\; aba + aab + 2\,abb$$

3.3.2 Multiplication par un scalaire

Soit P un élément de $K\langle X\rangle$ et soit α un élément de K. On définit le polynôme $\alpha\,P$ par :

$$\alpha\,P \;=\; \sum_{w\in X^*} \langle \alpha\,P|w\rangle\, w \;=\; \sum_{w\in X^*} (\alpha\langle P|w\rangle)\, w$$

Exemple 3.2 *Soit $X=\{a,b\}$. Soit le polynôme $P = 2\,aba + aab - 3\,abb$ et $\alpha = -3$. Alors*

$$\alpha\,P \;=\; -6\,aba - 3\,aab + 9\,abb$$

3.3.3 Produit de concaténation ou de Cauchy

Nous avons défini le produit de concaténation sur les mots. Ce produit est associatif, non commutatif et admet ε pour élément neutre. Ainsi, pour tous mots $u,v,w \in X^*$, on a :

$$\begin{array}{lrcl} \text{Associativité} & (u\cdot v)\cdot w & = & u\cdot(v\cdot w) \\ \text{Elément neutre} & u\cdot\varepsilon & = & u \;=\; \varepsilon\cdot u \end{array}$$

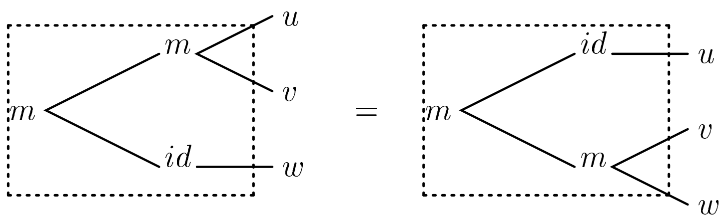
Quand on veut faire de l'algèbre, on donne un nom à ce produit, par exemple m, en notation parenthésée :

$$\begin{array}{rcl} m(m(u,v),w) & = & m(u,m(v,w)) \\ m(u,\varepsilon) & = & u \;=\; m(\varepsilon,u) \end{array}$$

Mais, m est une *application bilinéaire*, de $K\langle X\rangle \times K\langle X\rangle$ dans $K\langle X\rangle$. Pour cette raison, il vaut mieux l'écrire avec le *produit tensoriel*[1] :

$$m \ : \ K\langle X\rangle \otimes K\langle X\rangle \ \longrightarrow \ K\langle X\rangle$$

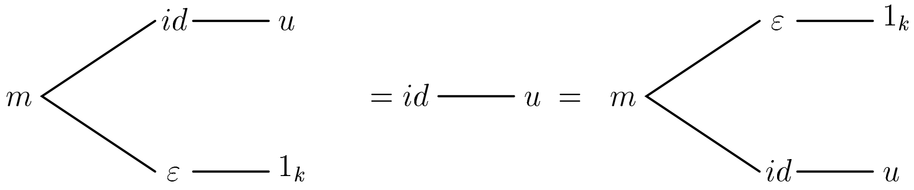
L'associativité peut s'écrire :



Et maintenant, on peut "oublier" les arguments u,v et w pour ne nous intéresser qu'aux propriétés des applications :

$$m \circ (m \otimes id) \ = \ m \circ (id \otimes m)$$

De ce point de vue, l'élément neutre ε doit être interprété comme une application linéaire de K dans $K\langle X\rangle$, celle qui envoie 1 sur $\varepsilon = 1_k \in K\langle X\rangle$. Il faut alors écrire les axiomes de l'élément neutre comme suit :



c'est-à-dire :

$$m \circ (id \otimes \varepsilon) \ = \ id \ = \ m \circ (\varepsilon \otimes id)$$

Ce produit s'étend par linéarité aux polynômes non commutatifs comme suit : Soient P et Q deux éléments de $K\langle X\rangle$, on pose

$$\begin{aligned} P \cdot Q \ &= \ \Big(\sum_{u\in X^*} \langle P|u\rangle\, u\Big) \cdot \Big(\sum_{v\in X^*} \langle Q|v\rangle\, v\Big) \\ &= \ \sum_{w\in X^*} \Big(\sum_{u\cdot v=w} \langle P|u\rangle * \langle Q|v\rangle\Big)\, w \end{aligned}$$

1. Le produit tensoriel de deux espaces vectoriels A et B, noté $A \otimes B$, est l'espace vectoriel quotient $A \times B/J$ où J est le sous-espace vectoriel de $A \times B$ engendré par les relations :

$$\begin{aligned} (\alpha\, a,b) \ &= \ (a,\alpha\, b) \ = \ \alpha\,(a,b) \quad \alpha \in K \\ (a + a',b) \ &= \ (a,b) + (a',b) \\ (a,b + b') \ &= \ (a,b) + (a,b') \end{aligned}$$

Exemple 3.3 *Soit $X = \{a,b\}$. Soient les polynômes $P = 2\,aba + aab - 3\,abb$ et $Q = ab + ba$. Alors*

$$\begin{aligned} P \cdot Q &= 2\,aba \cdot ab + 2\,aba \cdot ba + aab \cdot ab + aab \cdot ba - 3\,abb \cdot ab - 3\,abb \cdot ba \\ &= 2\,abaab + 2\,ababa + aabab + aabba - 3\,abbab - 3\,abbba \end{aligned}$$

$K\langle X\rangle$ muni de l'addition, la multiplication par un scalaire et le produit de Cauchy a une structure d'algèbre non commutative, appelée *algèbre de Cauchy*.

3.3.4 Produit de mélange

Pour les mots

On définit récursivement le *produit de mélange*, pour tous mots u et v de X^* et toutes lettres x et y de X, par :

$$\begin{cases} u \sqcup\!\sqcup\, \varepsilon = \varepsilon \sqcup\!\sqcup\, u = u \\ (xu) \sqcup\!\sqcup\, (yv) = x \cdot (u \sqcup\!\sqcup\, (yv)) + y \cdot ((xu) \sqcup\!\sqcup\, v) \end{cases} \tag{3.1}$$

Exemple 3.4 *Soit $X = \{a,b\}$. Soient les deux mots $u = ab$ et $v = b$. Alors*

$$\begin{aligned} u \sqcup\!\sqcup\, v &= a \cdot (b \sqcup\!\sqcup\, b) + b \cdot (ab \sqcup\!\sqcup\, \varepsilon) \\ &= a \cdot (b \cdot (\varepsilon \sqcup\!\sqcup\, b) + b \cdot (b \sqcup\!\sqcup\, \varepsilon) + b \cdot ab \\ &= a \cdot (b \cdot b + b \cdot b) + b \cdot ab \\ &= abb + abb + bab \\ &= 2\,abb + bab \end{aligned}$$

Proposition 3.1 *Le produit de mélange est commutatif.*

Preuve :

On fait une démonstration par récurrence sur la somme des longueurs $|u| + |v|$:

1. $\varepsilon \sqcup\!\sqcup\, \varepsilon = \varepsilon$ (par définition).
2. Supposons que pour tous u et v de X^* tels que $|u| + |v| \leq n$, on ait $u \sqcup\!\sqcup\, v = v \sqcup\!\sqcup\, u$.
3. Soient $u,v \in X^*$ tels que $|u| + |v| = n - 1$ et soient $x,y \in X$. On a

$$\begin{aligned} xu \sqcup\!\sqcup\, yv &= x \cdot (u \sqcup\!\sqcup\, yv) + y \cdot (xu \sqcup\!\sqcup\, v) && \text{(par définition)} \\ &= x \cdot (yv \sqcup\!\sqcup\, u) + y \cdot (v \sqcup\!\sqcup\, xu) && \text{(par hypothèse de récurrence)} \\ &= y \cdot (v \sqcup\!\sqcup\, xu) + x \cdot (yv \sqcup\!\sqcup\, u) && \text{(commutativité de l'addition)} \\ &= yv \sqcup\!\sqcup\, xu && \text{(par définition)} \end{aligned}$$

$\diamondsuit$

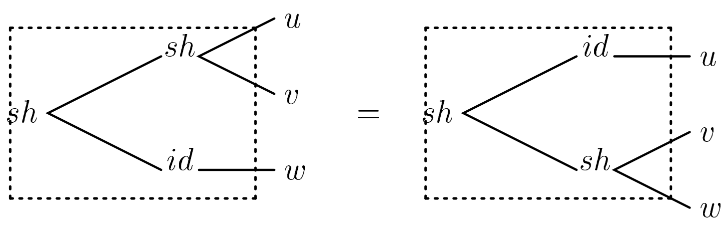
Proposition 3.2 *Le produit de mélange de deux mots u et v est un polynôme homogène (tous ses monômes sont de même degré) de degré $|u| + |v|$.*

Exercice 3.1 *Démontrez ce résultat en faisant une récurrence sur les longueurs des mots.*

Le produit de mélange est associatif et admet ε pour élément neutre. On utilisera sh pour la notation parenthésée. Ainsi, pour tous mots $u,v,w \in X^*$, on a :

$$\begin{array}{lrcl} \text{Associativité} & (u \shuffle v) \shuffle w & = & u \shuffle (v \shuffle w) \\ \text{Élément neutre} & u \shuffle \varepsilon & = & u \;=\; \varepsilon \shuffle u \end{array}$$

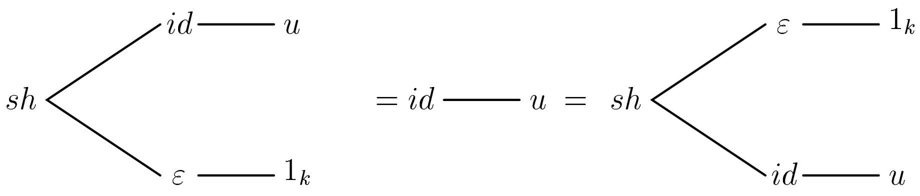
que l'on peut écrire aussi :



soit

$$sh \circ (sh \otimes id) \quad = \quad sh \circ (id \otimes sh)$$

et



soit

$$sh \circ (id \otimes \varepsilon) \quad = \quad id \quad = \quad sh \circ (\varepsilon \otimes id)$$

Le produit de mélange de deux mots u et v est un polynôme homogène (tous ses monômes sont de même degré) de degré $|u| + |v|$.

Exercice 3.2 *Démontrez ce résultat en faisant une récurrence sur les longueurs des mots.*

Pour les polynômes

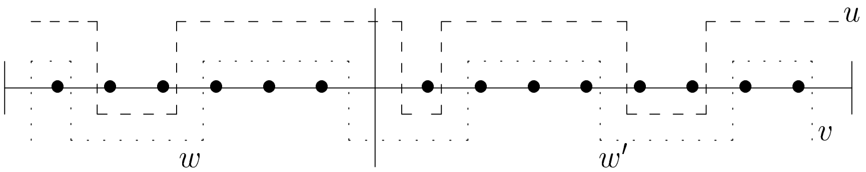
Le produit de mélange s'étend par linéarité aux polynômes en posant, pour P et Q des polynômes de $K\langle X\rangle$:

$$\begin{aligned} P \shuffle Q &= \left(\sum_{u \in X^*} \langle P|u\rangle \, u \right) \shuffle \left(\sum_{v \in X^*} \langle Q|v\rangle \, v \right) \\ &= \sum_{u,v \in X^*} \langle P|u\rangle\langle Q|v\rangle u \shuffle v \end{aligned}$$

$K\langle X\rangle$ muni de l'addition, la multiplication par un scalaire et le produit de mélange a une structure d'algèbre commutative, appelée *algèbre de mélange.*

3.4 Réconciliation des deux algèbres

Par le calcul de $\langle ww' | u \sqcup\!\sqcup\, v\rangle$. Dessinons ww' et la *bipartition* en u et v :



On constate qu'il y a autant de bipartitions de ww' (pour former $u \sqcup\!\sqcup\, v$) qu'il y a de couples formés

- d'une bipartition de w (pour former $u_1 \sqcup\!\sqcup\, v_1$) et
- d'une bipartition de w' (pour former $u'_1 \sqcup\!\sqcup\, v'_1$).

Les choix des décompositions sur les deux mots w et w' sont indépendants. Soit :

$$\langle ww' | u \sqcup\!\sqcup\, v\rangle = \sum_{\substack{u_1, v_1, u'_1, v'_1 \\ u = u_1 u'_1 \\ v = v_1 v'_1}} \langle w | u_1 \sqcup\!\sqcup\, v_1\rangle \langle w' | u'_1 \sqcup\!\sqcup\, v'_1\rangle$$

Finalement, en interprétant algébriquement les contraintes sur les indices de sommation, on a :

Lemme 3.1

$$\langle ww' | u \sqcup\!\sqcup\, v\rangle \;=\; \sum_{u_1, v_1, u'_1, v'_1} \langle u | u_1 u'_1\rangle \langle v | v_1 v'_1\rangle \langle w | u_1 \sqcup\!\sqcup\, v_1\rangle \langle w' | u'_1 \sqcup\!\sqcup\, v'_1\rangle$$

3.5 Cogèbres

On va définir le *coproduit de décomposition* Γ comme suit :

$$\Gamma \;:\; K\langle X\rangle \longrightarrow K\langle X\rangle \otimes K\langle X\rangle$$

$K\langle X\rangle \otimes K\langle X\rangle$ est le *produit tensoriel* de $K\langle X\rangle$ par lui-même.

Définition 3.1 *On définit Γ pour tout mot $w \in X^*$ en posant :*

$$\begin{aligned} \langle \Gamma(w) | u \otimes v\rangle &= \langle w | u \sqcup\!\sqcup\, v\rangle \\ \Longrightarrow \quad \Gamma(w) &= \sum_{u, v \in X^*} \langle w | u \sqcup\!\sqcup\, v\rangle u \otimes v \end{aligned}$$

D'où le calcul de $\Gamma(\varepsilon)$ et de $\Gamma(x)$ si $x \in X$:

$$\langle \Gamma(\varepsilon) | u \otimes v\rangle \;=\; \langle \varepsilon | u \sqcup\!\sqcup\, v\rangle \;=\; \begin{cases} 1 & \text{si } u = \varepsilon \text{ et } v = \varepsilon \\ 0 & \text{sinon} \end{cases}$$

Donc $\Gamma(\varepsilon) = \varepsilon \otimes \varepsilon$ (notation $1 \otimes 1$).

$$\langle \Gamma(x) | u \otimes v \rangle = \langle x | u ⧢ v \rangle = \begin{cases} 1 & \text{si } u = x \text{ et } v = \varepsilon \\ 1 & \text{si } u = \varepsilon \text{ et } v = x \\ 0 & \text{sinon} \end{cases}$$

Donc $\Gamma(x) = x \otimes 1 + 1 \otimes x$.

Proposition 3.3 *Γ est un morphisme pour le produit de concaténation. C'est-à-dire*

$$\Gamma(ww') = \Gamma(w)\Gamma(w')$$

Preuve :

On a :

1. $\langle \Gamma(ww') | u \otimes v \rangle = \langle ww' | u ⧢ v \rangle$
2. $\Gamma(w) = \sum_{u_1, v_1} \langle w | u_1 ⧢ v_1 \rangle u_1 \otimes v_1$ et $\Gamma(w') = \sum_{u'_1, v'_1} \langle w' | u'_1 ⧢ v'_1 \rangle u'_1 \otimes v'_1$

D'où

$$\begin{aligned} \Gamma(w)\Gamma(w') &= \sum_{u_1, v_1, u'_1, v_2} \langle w | u_1 ⧢ v_1 \rangle \langle w' | u'_1 ⧢ v'_1 \rangle u_1 u'_1 \otimes v_1 v'_1 \\ \langle \Gamma(w)\Gamma(w') | u \otimes v \rangle &= \sum_{u_1, v_1, u'_1, v'_1} \langle w | u_1 ⧢ v_1 \rangle \langle w' | u'_1 ⧢ v'_1 \rangle \langle u_1 u'_1 | u \rangle \langle v_1 v'_1 | v \rangle \\ &= \langle ww' | u ⧢ v \rangle \\ &= \langle \Gamma(ww') | u \otimes v \rangle \end{aligned}$$

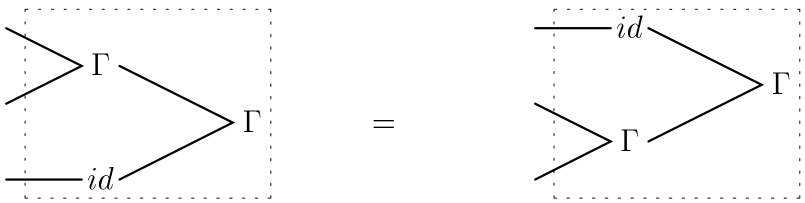
$\diamondsuit$

Exemple 3.5 *Soit $X = \{a,b\}$. Alors*

$$\begin{aligned} \Gamma(a \cdot b) &= \Gamma(a) \cdot \Gamma(b) \\ &= (1 \otimes a + a \otimes 1) \cdot (1 \otimes b + b \otimes 1) \\ &= 1 \otimes ab + b \otimes a + a \otimes b + ab \otimes 1 \end{aligned}$$

3.5.1 Propriétés de Γ

Coassociativité de Γ. On a :



Preuve :

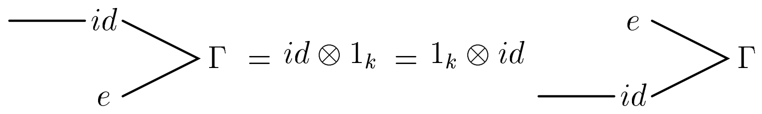
$$\begin{aligned}(\Gamma\otimes id)\Gamma(w) &= \sum_{u,v}(\Gamma\otimes id)\langle w|u \shuffle v\rangle u\otimes v\\ &= \sum_{u,v}\langle w|u \shuffle v\rangle \Gamma(u)\otimes v\\ &= \sum_{u,v}\langle w|u \shuffle v\rangle \sum_{u_1,u_2}\langle u|u_1 \shuffle u_2\rangle u_1\otimes u_2\otimes v\\ &= \sum_{u_1,u_2,v}\langle w|u_1 \shuffle u_2 \shuffle v\rangle u_1\otimes u_2\otimes v\end{aligned}$$

De même

$$(id\otimes\Gamma)\Gamma(w) = \sum_{u,v_1,v_2}\langle w|u \shuffle v_1 \shuffle v_2\rangle u\otimes v_1\otimes v_2$$

C'est donc la même chose, aux indices muets de sommation près. $\diamondsuit$

Counité de Γ. Il faut chercher $e\ :\ K\langle X\rangle \longrightarrow K$ tel que



Preuve :

$$\begin{aligned}(id\otimes e)\Gamma(w) &= \sum_{u,v}(id\otimes e)\langle w|u \shuffle v\rangle u\otimes v\\ &= \sum_{u,v}\langle w|u \shuffle v\rangle u\otimes e(v)\end{aligned}$$

Posons

$$e(v) \;=\; \begin{cases} 0 & \text{si } v\neq\varepsilon\\ 1 & \text{si } v=\varepsilon\end{cases} \qquad \text{ainsi, } e(S) \;=\; \langle S|\varepsilon\rangle.$$

Donc les termes de la somme sont nuls si $v\neq\varepsilon$.

$$(id\otimes e)\Gamma(w) \;=\; \langle w|w\rangle w\otimes 1_k \;=\; w\otimes 1_k$$

La preuve est identique pour l'égalité symétrique. $\diamondsuit$

$K\langle X\rangle$ muni de l'addition, de la multiplication par un scalaire et du coproduit de décomposition Γ a une structure de cogèbre, appelée *cogèbre de décomposition.*

Ainsi $(K\langle X\rangle,m,\varepsilon,\Gamma,e)$ est une *bigèbre* car Γ est un morphisme d'algèbre pour la multiplication m.

Le produit de mélange défini précédemment est donc le "dual" de Γ, c'est-à-dire que l'on a pour tous mots u et v de X^* :

$$\langle u \shuffle v|w\rangle \;=\; \langle\Gamma(w)|u\otimes v\rangle \qquad \text{(voir définition 3.1)}$$

3.5.2 Résiduels et mélange

Dans le chapitre 2, section 2.2.2, on avait défini les résiduels à gauche et à droite d'un mot par une *lettre*. Ces résiduels sont des *dérivations* pour le produit de mélange. Autrement dit, soient u et v des mots de X^* et soit x une lettre de X. Alors, on a :

$$\begin{aligned} x \triangleleft (u ш v) &= (x \triangleleft u) ш v + u ш (x \triangleleft v) \\ (u ш v) \triangleright x &= (u \triangleright x) ш v + u ш (v \triangleright x) \end{aligned}$$

En effet, on a :

$$\begin{aligned} \langle w|(u ш v) \triangleright x\rangle &= \langle xw|u ш v\rangle \\ &= \langle \Gamma(x)\Gamma(w)|u \otimes v\rangle \\ &= \langle (1 \otimes x)\Gamma(w)|u \otimes v\rangle + \langle (x \otimes 1)\Gamma(w)|u \otimes v\rangle \\ &= \langle \Gamma(w)|u \otimes (v \triangleright x)\rangle + \langle \Gamma(w)|(u \triangleright x) \otimes v\rangle \\ &= \langle u ш (v \triangleright x)|w\rangle + \langle (u \triangleright x) ш v|w\rangle \\ &= \langle u ш (v \triangleright x) + (u \triangleright x) ш v|w\rangle \end{aligned}$$

Remarque 3.1 *Le résiduel par un mot n'est pas une dérivation (car la composée de deux dérivations n'en est pas une) !*

Lemme 3.2 *[de reconstruction] Soit $P \in k\langle X\rangle$ un polynôme. Alors on peut écrire*

$$P = \langle P|\varepsilon\rangle + \sum_{x\in X} x\,(P \triangleright x)$$

Ainsi, à partir du terme constant et des résiduels d'un polynôme par les lettres, on peut retrouver le polynôme initial.

3.5.3 Coproduit de factorisation

On définit le *coproduit de factorisation* Φ par dualité du produit de Cauchy en posant :

$$\langle \Phi(w)|u \otimes v\rangle = \langle w|u \cdot v\rangle$$

En d'autres termes :

$$\begin{aligned} \Phi(w) &= \sum_{u,v\in X^*} \langle w|uv\rangle\, u \otimes v \\ &= \sum_{\substack{u,v \in X^* \\ uv=w}} u \otimes v \end{aligned}$$

On montre de même que $(K\langle X\rangle, ш ,\varepsilon,\Phi,e)$ est une bigèbre. Pour cela, il faut montrer que Φ est un morphisme pour le mélange, c'est-à-dire

$$\Phi(u ш v) = \Phi(u) ш \Phi(v)$$

où le mélange dans $K\langle X\rangle \otimes K\langle X\rangle$ est défini par :

$$(u_1 \otimes v_1) ш (u_2 \otimes v_2) = (u_1 ш u_2) \otimes (v_1 ш v_2)$$

La preuve se fait à nouveau en utilisant le lemme de réconciliation des deux produits.

3.5.4 Convolution et antipode

Soient $f,g : K\langle X\rangle \longrightarrow K\langle X\rangle$ deux applications linéaires. Si $P \in K\langle X\rangle$, alors

$$f(P) = \sum_{u\in X^*} \langle P|u\rangle f(u)$$

On appelle *graphe* de f, la série double :

$$F = \sum_{u\in X^*} u \otimes f(u)$$

Pour retrouver $f(P)$, il suffit de remplacer dans F chaque terme u par $\langle P|u\rangle$

$$F(P) = (P \otimes id)(F) = \sum_{u\in X^*} \langle P|u\rangle f(u)$$

On définit le *produit de convolution* des deux applications f et g, que l'on note $f \circledast g$ par

$$f \circledast g = m \circ (f \otimes g) \circ \Gamma$$

$$\begin{aligned}
(f \circledast g)(P) &= m \circ (f \otimes g)\Gamma(P) \\
&= m \circ (f \otimes g) \sum_{u,v} \langle P|u \sqcup\!\sqcup v\rangle u \otimes v \\
&= \sum_{u,v} \langle P|u \sqcup\!\sqcup v\rangle m(f(u) \otimes g(v)) \\
&= \sum_{u,v} \langle P|u \sqcup\!\sqcup v\rangle f(u) \cdot g(v)
\end{aligned}$$

Posons maintenant

$$F \circledast G = \sum_{u,v} (u \sqcup\!\sqcup v) \otimes f(u) \cdot g(v)$$

Alors

$$(F \circledast G)(P) = \sum_{u,v} \langle P|u \sqcup\!\sqcup v\rangle\, f(u) \cdot g(v)$$

$F \circledast G$ est donc le graphe de $f \circledast g$. Il est ici donné de façon "implicite". On pourrait aussi le calculer sous la forme "explicite" :

$$(F \circledast G)(w) = \sum_{u,v} \langle w|u \sqcup\!\sqcup v\rangle\, f(u)g(v) = (f \circledast g)(w)$$

Élément neutre : la série $\varepsilon \otimes \varepsilon$ est élément neutre du produit de convolution.

Preuve :

$$\begin{aligned}
\left(\sum_{u\in X^*} u \otimes f(u)\right) \circledast (\varepsilon \otimes \varepsilon) &= \sum_{u\in X^*} (u \sqcup\!\sqcup \varepsilon) \otimes f(u) \cdot \varepsilon \\
&= \sum_{u\in X^*} u \otimes f(u)
\end{aligned}$$

Soit E tel que

$$E(v) \quad = \quad \begin{cases} \varepsilon & \text{si } v = \varepsilon \\ 0 & \text{si } v \neq \varepsilon \end{cases}$$

$\diamondsuit$

Définition 3.2 *On appelle* antipode *un inverse a (à droite et à gauche) de id pour le produit de convolution. C'est-à-dire*

$$a \circledast id \quad = \quad id \circledast a \quad = \quad E$$

Théorème 3.1 *L'antipode, pour Γ, est l'application linéaire définie, pour tout mot w. par :*

$$a(w) \quad = \quad (-1)^{|w|}\, \widetilde{w}$$

où $\widetilde{w}$ est le miroir de w.

Preuve :

Posons $\partial_z(u \otimes v) = (z \triangleleft u) \otimes v$. Alors

$$\partial_z(F \circledast G) \quad = \quad \partial_z F \circledast G + F \circledast \partial_z G$$

car l'application $u \mapsto z \triangleleft u$ est une dérivation pour le produit de mélange (voir la section 3.5.2).

Posons $Id = \sum_{u \in X^*} u \otimes u$ la *série double* et $A = \sum_{w \in X^*} w \otimes (-1)^{|w|}\, w$. Alors

$$\begin{aligned} \partial_z Id &= Id(1 \otimes z) \\ \partial_z A &= -(1 \otimes z)A \end{aligned}$$

d'où

$$\begin{aligned} \partial_z(Id \circledast A) &= Id(1 \otimes z) \circledast A - Id \circledast (1 \otimes z)A \\ &= 0 \end{aligned}$$

On en déduit que $Id \circledast A = \varepsilon \otimes \varepsilon$ et donc $id \circledast a = E$.

Pour l'égalité symétrique, il faut utiliser le résiduel à droite (qui est aussi une dérivation pour le mélange). $\diamondsuit$

3.6 Séries formelles non commutatives

On appelle *série formelle non commutative* à coefficient dans un corps K toute somme formelle infinie de la forme :

$$S \quad = \quad \sum_{w \in X^*} \beta_w\, w \qquad \beta_w \in K$$

Comme pour les polynômes, le coefficient β_w sera noté $\langle S|w\rangle$. La série S peut être vue comme une application de X^* dans K, qui à tout $w \in X^*$ associe $S(w) = \langle S|w\rangle$.

L'ensemble des séries formelles sur les variables non commutatives $x_0,x_1,\ldots,x_n$ à coefficients dans le corps K sera noté $K\langle\langle X\rangle\rangle$.

Toutes les opérations définies sur $K\langle X\rangle$ peuvent être étendues, par continuité, à $K\langle\langle X\rangle\rangle$. On obtient ainsi les mêmes structures pour $K\langle\langle X\rangle\rangle$ que celles que l'on a pour $K\langle X\rangle$.

4

Algèbres de Lie libres

4.1 Introduction

On aimerait pouvoir calculer, en quelque sorte, la "distance de non commutativité" de deux mots comportant les mêmes lettres, et chacune d'elles le même nombre de fois.

On rappelle que l'ensemble des polynômes non commutatifs sur un alphabet X à coefficients dans un corps K, noté $K\langle X\rangle$ est une algèbre associative libre.

4.2 Définition dans l'algèbre associative libre

Soit X un alphabet fini, et P et Q deux polynômes sur X, on définit le *"crochet de Lie"* de P et Q par :

$$[P,Q] \quad = \quad P \cdot Q - Q \cdot P \tag{4.1}$$

où le produit est le produit de Cauchy de l'algèbre associative $K\langle X\rangle$.

Ce crochet est nul si et seulement si P et Q commutent (ie, si $PQ = QP$).

On construit alors le plus petit sous-espace vectoriel de $K\langle X\rangle$, noté $\mathcal{L}ie\langle X\rangle$ qui contient les lettres et qui est "fermé" pour l'opération "*crochet de Lie*". Autrement dit, on a :

(1) tout polynôme réduit à une lettre est dans $\mathcal{L}ie\langle X\rangle$,
(2) si P et Q sont dans $\mathcal{L}ie\langle X\rangle$, alors $[P,Q]$ est aussi dans $\mathcal{L}ie\langle X\rangle$.
(3) Toute combinaison linéaire d'éléments de $\mathcal{L}ie\langle X\rangle$ est aussi dans $\mathcal{L}ie\langle X\rangle$.
(4) Il n'y a pas dans $\mathcal{L}ie\langle X\rangle$ d'autres polynômes que ceux qui sont construits par les règles (1), (2) et (3).

Les éléments de $\mathcal{L}ie\langle X\rangle$ sont appelés "*polynômes de Lie*".

Lemme 4.1 *Si P, Q et R sont des polynômes de Lie, alors*

1) $[P, P] \;=\; 0$ *(anticommutativité)*
2) $[P, [Q, R]] + [Q, [R, P]] + [R, [P, Q]] \;=\; 0$ *(identité de Jacobi).*

Preuve : (du 2))

Il suffit de développer les crochets de Lie, en utilisant l'égalité 4.1 :

$$\begin{array}{rcccl} [P, [Q, R]] & = & [P, QR - RQ] & = & PQR - QRP - PRQ + RQP \\ [Q, [R, P]] & = & [Q, RP - PR] & = & QRP - QPR - RPQ + PRQ \\ [R, [P, Q]] & = & [R, PQ - QP] & = & RPQ - RQP - PQR + QPR \end{array}$$

En additionnant membre à membre les trois égalités, on obtient 0 à droite. $\diamondsuit$

Le 1) implique que, pour tous P et Q, on a

$$[Q, P] \;=\; -[P, Q] \tag{4.2}$$

En effet,

$$\begin{array}{rcl} [P + Q, P + Q] & = & [P, P + Q] + [Q, P + Q] \\ & = & [P, P] + [P, Q] + [Q, P] + [Q, Q] \\ & = & [P, Q] + [Q, P] \\ & = & 0 \end{array}$$

4.3 Définition "abstraite" des algèbres de Lie

Si E est un espace vectoriel sur K, on dira que E est une $K-$algèbre de Lie s'il existe un opérateur binaire bilinéaire sur E, appelé encore "*crochet de Lie*", qui vérifie, pour tous $a,b,c \in E$:

1) $[a, a] \;=\; 0$ (anticommutativité)
2) $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] \;=\; 0$ (identité de Jacobi).

Exemple 4.1 *Une algèbre de Lie de matrices. Les matrices 2×2 à coefficients dans $\mathbb{Q}$ forment une $\mathbb{Q}$-algèbre associative pour le produit usuel des matrices. Elles forment aussi une algèbre de Lie pour le crochet de Lie défini par la règle :*

$$[M,N] \;=\; M\,N - N\,M$$

Exercice 4.1 *Considérons les quatre matrices suivantes :*

$$E_{11} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad E_{12} \;=\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad E_{21} \;=\; \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad E_{22} \;=\; \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Calculer les crochets de Lie de ces matrices prises deux à deux.

Montrer qu'elles engendrent une algèbre de Lie de dimension finie égale à 4.

Théorème 4.1 *Soit F un ensemble fini et soit $\mathcal{L}$ une algèbre de Lie. Si $\varphi : F \to \mathcal{L}$ est une application de F dans $\mathcal{L}$, alors il existe un unique morphisme d'algèbre de Lie χ de l'algèbre*

$\mathcal{L}ie\langle F\rangle$ dans $\mathcal{L}$ qui rend "commutatif" le diagramme

$$\begin{tikzcd} F \arrow[r, "\varphi"] \arrow[dr] & \mathcal{L} \\ & \mathcal{L}ie\langle F\rangle \arrow[u, "\chi"'] \end{tikzcd}$$

Ce théorème explique en fait que $\mathcal{L}ie\langle F\rangle$ est l'algèbre de Lie libre sur F. Il montre que l'on peut coder tout calcul dans l'algèbre $\mathcal{L}$ en effectuant les calculs correspondants dans $\mathcal{L}ie\langle F\rangle$. Le résultat des calculs dans $\mathcal{L}$ sera l'image par χ du résultat calculé dans $\mathcal{L}ie\langle F\rangle$.

Définition 4.1 *Un polynôme de Lie est dit* homogène *de degré $n \in \mathbb{N}$ si et seulement si tous les mots de son support (voir 3) sont de degré n.*

Exemple 4.2 *Donnons les formes explicites de quelques polynômes de Lie homogènes sur l'alphabet $X = \{x_0,x_1\}$.*

$$\begin{array}{lrcl}
\text{Degré } 1: & x_0,\, x_1 & & \\
\text{Degré } 2: & [x_0,\, x_1] & = & x_0x_1 - x_1x_0 \\
\text{Degré } 3: & [x_0,\, [x_0,\, x_1]] & = & x_0^2x_1 - 2\,x_0x_1x_0 + x_1x_0^2 \\
 & [[x_0,\, x_1],\, x_1] & = & x_0x_1^2 - 2\,x_1x_0x_1 + x_1^2x_0 \\
\text{Degré } 4: & [x_0,\, [x_0,\, [x_0,\, x_1]]] & = & x_0^3x_1 - 3\,x_0^2x_1x_0 + 3\,x_0x_1x_0^2 - x_1x_0^3
\end{array}$$

Remarque 4.1 *Tout polynôme est une combinaison linéaire finie de mots. On en déduit sans difficulté (c'est un bon exercice) que tout polynôme de Lie est une combinaison linéaire finie de polynômes de Lie homogènes. Ou mieux encore :*

Exercice 4.2 *Si P est un polynôme de Lie, alors pour tout entier n, la* composante homogène *de degré n de P est un polynôme de Lie.*

Définition 4.2 *On appelle* série de Lie *toute somme de polynômes de Lie homogènes de degrés tous différents.*

On définit le crochet de Lie de deux séries de Lie S et T exactement comme dans le cas des polynômes :

$$[S, T] \;=\; S \cdot T - T \cdot S$$

4.4 Représentation adjointe

Pour tout $Q \in \mathcal{L}ie\langle X\rangle$, on définit l'*application adjointe* de Q, notée Ad_Q, comme étant l'application linéaire :

$$\begin{array}{rcl}
\mathcal{L}ie\langle X\rangle & \longrightarrow & \mathcal{L}ie\langle X\rangle \\
P & \longmapsto & Ad_Q(P) \;=\; [Q,\, P]
\end{array}$$

Exemple 4.3

$$\begin{array}{rcl} Ad_{[x_0,\, x_1]}(x_0) & = & [[x_0,\, x_1],\, x_0] \\ & = & [x_0x_1 - x_1x_0,\, x_0] \\ & = & x_0x_1x_0 - x_1x_0^2 - x_0^2x_1 + x_0x_1x_0 \\ & = & 2\, x_0x_1x_0 - x_1x_0^2 - x_0^2x_1 \end{array}$$

Les applications linéaires de $\mathcal{L}ie\langle X\rangle$ dans $\mathcal{L}ie\langle X\rangle$ forment une algèbre associative. On peut donc définir l'algèbre de Lie engendrée par les opérateurs Ad_Q avec $Q \in \mathcal{L}ie\langle X\rangle$.

Proposition 4.1 *L'application linéaire*

$$\begin{array}{rcl} \mathcal{L}ie\langle X\rangle & \longrightarrow & End(\mathcal{L}ie\langle X\rangle) \\ P & \longmapsto & Ad_P \end{array}$$

où $End(\mathcal{L}ie\langle X\rangle)$ est l'algèbre de Lie des endomorphismes linéaires *de $\mathcal{L}ie\langle X\rangle$ dans $\mathcal{L}ie\langle X\rangle$, est un homomorphisme d'algèbres de Lie.*

Preuve :

$$\begin{array}{rcl} Ad_{[P,\, Q]}(R) & = & [[P,\, Q],\, R] \\ [Ad_P,\, Ad_Q](R) & = & Ad_P\, Ad_Q(R) - Ad_Q\, Ad_P(R) \\ & = & Ad_P([Q,\, R]) - Ad_Q([P,\, R]) \\ & = & [P,\, [Q,\, R]] - [Q,\, [P,\, R] \\ & = & [[P,\, Q],\, R] \end{array}$$

En effet, d'après l'identité de Jacobi (voir lemme 4.1), on a :

$$\begin{array}{rcl} -[R,\, [P,\, Q]] & = & [P,\, [Q,\, R]] + [Q,\, [R,\, P]] \\ \Longrightarrow\ [[P,\, Q],\, R] & = & [P,\, [Q,\, R]] - [Q,\, [P,\, R]] \end{array}$$

En conclusion,

$$Ad_{[P,\, Q]}(R) \;=\; [Ad_P,\, Ad_Q](R)$$

$\diamondsuit$

Proposition 4.2 *L'application Ad_P est une dérivation pour le produit dans l'algèbre de Lie $\mathcal{L}ie\langle X\rangle$.*

Preuve :

On utilise encore l'identité de Jacobi (lemme 4.1).

$$\begin{array}{rcl} Ad_P([Q,\, R]) & = & [P,\, [Q,\, R]] \\ & = & -[Q,\, [R,\, P]] - [R,\, [P,\, Q]] \\ & = & [[P,\, Q],\, R] + [Q,\, [P,\, R]] \\ & = & [Ad_P(Q),\, R] + [Q,\, Ad_P(R)] \end{array}$$

$\diamondsuit$

4.5 Éléments primitifs

Nous avons vu dans la chapitre 3, section 3.5 que les lettres de l'alphabet sont des "*éléments primitifs*" pour le coproduit Γ. C'est-à-dire

$$\forall\, x \in X, \quad \Gamma(x) \;=\; x \otimes 1 + 1 \otimes x$$

Ce ne sont pas les seuls éléments à jouir de cette propriété.

Théorème 4.2 *Tout élément de Lie (c'est-à-dire, tout polynôme de Lie et toute série de Lie) est un élément primitif.*

Preuve :

1. Les lettres sont des éléments primitifs.
2. Si P et Q sont primitifs, alors leur crochet de Lie l'est aussi. En effet :

$$\begin{aligned}
\Gamma([P,Q]) &= \Gamma(PQ - QP) \\
&= \Gamma(P)\Gamma(Q) - \Gamma(Q)\Gamma(P) \\
&= (P \otimes 1 + 1 \otimes P)(Q \otimes 1 + 1 \otimes Q) - (Q \otimes 1 + 1 \otimes Q)(P \otimes 1 + 1 \otimes P) \\
&= \quad PQ \otimes 1 + P \otimes Q + Q \otimes P + 1 \otimes PQ \\
&\quad -QP \otimes 1 - Q \otimes P - P \otimes Q - 1 \otimes QP \\
&= (PQ - QP) \otimes 1 + 1 \otimes (PQ - QP) \\
&= [P,Q] \otimes 1 + 1 \otimes [P,Q]
\end{aligned}$$

3. Si tout polynôme de Lie est primitif alors toute série de Lie est primitive. En effet, soit $S = \sum_{i=0}^{\infty} P_i$ une série de Lie, présentée comme somme de ses composantes homogènes P_i. On a lors :

$$\begin{aligned}
\Gamma(S) &= \sum_{i=0}^{\infty} \Gamma(P_i) \\
&= \sum_{i=0}^{\infty} (P_i \otimes 1 + 1 \otimes P_i) \\
&= \left(\sum_{i=0}^{\infty} P_i\right) \otimes 1 + 1 \otimes \left(\sum_{i=0}^{\infty} P_i\right) \\
&= S \otimes 1 + 1 \otimes S
\end{aligned}$$

$\diamondsuit$

Théorème 4.3 *Un polynôme (une série) P sans terme constant de $K\langle X\rangle$ est un élément primitif si et seulement s'il (elle) est orthogonal(e) à tous les "mélanges propres"*[1]*, c'est-à-dire, si*

$$u,v \in X^+ \implies \langle P | u \sqcup\!\sqcup\, v \rangle \;=\; 0$$

1. mélange de deux mots non vides.

Preuve :

1. Supposons P primitif. On a, pour u et v dans X^+ :

$$\begin{aligned}\langle P|u \sqcup\!\sqcup\, v\rangle &= \langle \Gamma(P)|u\otimes v\rangle\\ &= \langle P\otimes 1+1\otimes P|u\otimes v\rangle\\ &= \langle P\otimes 1|u\otimes v\rangle + \langle 1\otimes P|u\otimes v\rangle\\ &= \langle P|u\rangle\langle 1|v\rangle + \langle 1|u\rangle\langle P|v\rangle\end{aligned}$$

Comme $u{,}v \in X^+$, on a $\langle 1|v\rangle = 0$ et $\langle 1|u\rangle = 0$ et donc

$$\langle P|u \sqcup\!\sqcup\, v\rangle = 0$$

2. Supposons P orthogonal à tous les mélanges propres. Par définition de Γ, on a, pour u et $v \in X^+$:

$$\langle P|u \sqcup\!\sqcup\, v\rangle \quad = \quad \langle \Gamma(P)|u\otimes v\rangle$$

On en déduit :

$$\begin{aligned}\Gamma(P) &= \sum_{u,v\in X^*} \langle \Gamma(P)|u\otimes v\rangle\, u\otimes v\\ &= \sum_{u,v\in X^*} \langle P|u \sqcup\!\sqcup\, v\rangle\, u\otimes v\end{aligned}$$

Comme $\langle P|u \sqcup\!\sqcup\, v\rangle = 0$ si $u \neq \varepsilon$ et $v \neq \varepsilon$

$$\begin{aligned}\Gamma(P) &= \sum_{u\in X^*} \langle P|u \sqcup\!\sqcup\, \varepsilon\rangle\, u\otimes\varepsilon + \sum_{v\in X^*} \langle P|\varepsilon \sqcup\!\sqcup\, v\rangle\, \varepsilon\otimes v\\ &= P\otimes 1 + 1\otimes P\end{aligned}$$

$\diamondsuit$

Nous allons nous servir de cette dernière propriété pour démontrer le théorème suivant :

Théorème 4.4 *Un polynôme (une série) de $K\langle X\rangle$ (de $K\langle\langle X\rangle\rangle$) sans terme constant est un élément de Lie si et seulement si c'est un élément primitif.*

Définition 4.3 *On définit le* crochet de Dynkin *comme étant l'application $\ell : K\langle X\rangle \to K\langle X\rangle$ définie par :*

(i) $\ell(\varepsilon) \;=\; 0$
(ii) $\ell(x) \;=\; x$ *pour toute lettre* $x \in X$
(iii) $\ell(vx) \;=\; [\ell(v),x]$ *pour tout mot* $v \in X^*$ *et toute lettre* $x \in X$.

Ainsi $\ell(xzyzx) = [[[[x,z],y],z],x]$.

On définit la *série double* L, graphe de ℓ par :

$$L \quad = \quad \sum_{u\in X^*} u\otimes \ell(u)$$

On rappelle la définition du graphe Id de l'identité id:

$$Id = \sum_{u \in X^*} u \otimes u$$

On va utiliser l'*opérateur* ∂_z pour toute lettre z, opérant sur les séries doubles par:

$$\partial_z(u \otimes v) = (z \triangleleft u) \otimes v$$

On rappelle enfin la définition du *produit de convolution*:

$$(u \otimes v) \circledast (u' \otimes v') = (u \sqcup\!\sqcup u') \otimes vv'$$

Lemme 4.2 *L'opérateur ∂_z est une dérivation pour le produit de convolution.*

Preuve :

$$\partial_z((u \otimes v) \circledast (u' \otimes v')) = \partial_z((u \sqcup\!\sqcup u') \otimes vv')$$

Comme $z\triangleleft$ est une dérivation pour le mélange

$$\begin{aligned}
&= (z \triangleleft (u \sqcup\!\sqcup u')) \otimes vv' \\
&= ((z \triangleleft u) \sqcup\!\sqcup u' + u \sqcup\!\sqcup (z \triangleleft u')) \otimes vv' \\
&= ((z \triangleleft u) \sqcup\!\sqcup u') \otimes vv' + (u \sqcup\!\sqcup (z \triangleleft u')) \otimes vv' \\
&= ((z \triangleleft u) \otimes v) \circledast (u' \otimes v') + (u \otimes v) \circledast ((z \triangleleft u') \otimes v') \\
&= (\partial_z(u \otimes v)) \circledast (u' \otimes v') + (u \otimes v) \circledast (\partial_z(u' \otimes v'))
\end{aligned}$$

$\diamondsuit$

Lemme 4.3 *La série double Id vérifie*

$$\partial_z Id = Id \circledast (1 \otimes z)$$

Preuve :

$$\begin{aligned}
\partial_z \left(\sum_{u \in X^*} u \otimes u \right) &= \sum_{u \in X^*} (z \triangleleft u) \otimes u \qquad (z \triangleleft u \text{ est nul sauf si } u = vz) \\
&= \sum_{v \in X^*} v \otimes vz \\
&= Id \circledast (1 \otimes z)
\end{aligned}$$

$\diamondsuit$

Lemme 4.4 *La série L de Dynkin vérifie*

$$\partial_z L = 1 \otimes z + L \circledast (1 \otimes z) - (1 \otimes z) \circledast L$$

Preuve :

$$\begin{aligned}\partial_z L &= \partial_z \left(\sum_{u\in X^*} u\otimes \ell(u)\right)\\ &= \sum_{u\in X^*} (z \triangleleft u)\otimes \ell(u)\\ &= \sum_{v\in X^*} v\otimes \ell(vz)\end{aligned}$$

Attention ! $\ell(vz) = [\ell(v),z]$ si $v\neq\varepsilon$ et $\ell(z) = z$ si z est une lettre.

$$\begin{aligned}\partial_z L &= 1\otimes z + \sum_{v\neq\varepsilon} v\otimes \ell(v)z - \sum_{v\neq\varepsilon} v\otimes z\ell(v)\\ &= 1\otimes z + L\circledast(1\otimes z) - (1\otimes z)\circledast L\end{aligned}$$

$\diamondsuit$

Proposition 4.3

$$Id \circledast L \;=\; \sum_{w\in X^*} |w|\, w\otimes w$$

Preuve :

$$\begin{aligned}\partial_z(Id\circledast L) &= \partial_z(Id)\circledast L + Id\circledast \partial_z(L)\\ &= Id\circledast(1\otimes z)\circledast L + Id\circledast(1\otimes z) + Id\circledast L\circledast(1\otimes z) - Id\circledast(1\otimes z)\circledast L\\ &= Id\circledast(1\otimes z) + Id\circledast L\circledast(1\otimes z)\end{aligned}$$

On a aussi, (puisque $w \sqcup\!\sqcup\, \varepsilon = w = w\cdot 1$)

$$\partial_z(Id\circledast L) = Id\cdot(1\otimes z) + (Id\circledast L)\cdot(1\otimes z)$$

(“$\cdot$” est la concaténation à la fois à gauche et à droite), car 1 est élément neutre pour le produit de mélange.

On peut reconstruire la série $Id\circledast L$ à partir de ses dérivées par ∂_z, $z\in X$ (cf lemme de reconstruction 3.2 du chapitre 3).

Le terme constant (ε à gauche) est nul : il correspond à $u \sqcup\!\sqcup\, v = \varepsilon$, soit en particulier $v=\varepsilon$. Mais $\ell(\varepsilon) = 0$. On a donc

$$Id\circledast L \;=\; Id\cdot\sum_{z\in X} z\otimes z + (Id\circledast L)\cdot\sum_{z\in X} z\otimes z$$

Posons $\mathcal{E} = \sum_{z\in X} z\otimes z$. On a alors

$$Id \;=\; \varepsilon\otimes\varepsilon + \mathcal{E} + \mathcal{E}^2 + \cdots \;=\; \mathcal{E}^*$$

D'où enfin

$$\begin{aligned}
Id \circledast L &= \mathcal{E}^* \cdot \mathcal{E} + (Id \circledast L) \cdot \mathcal{E} \\
&= \mathcal{E}^* \cdot \mathcal{E} + (\mathcal{E}^* \cdot \mathcal{E} + (Id \circledast L) \cdot \mathcal{E}) \cdot \mathcal{E} \\
&= \mathcal{E}^* \cdot \mathcal{E} + \mathcal{E}^* \cdot \mathcal{E}^2 + (Id \circledast L) \cdot \mathcal{E}^2 \\
&= \mathcal{E}^* \cdot \mathcal{E} + \mathcal{E}^* \cdot \mathcal{E}^2 + (\mathcal{E}^* \cdot \mathcal{E} + (Id \circledast L) \cdot \mathcal{E}) \cdot \mathcal{E}^2 \\
&= \mathcal{E}^* \cdot \mathcal{E} + \mathcal{E}^* \cdot \mathcal{E}^2 + \mathcal{E}^* \cdot \mathcal{E}^3 + \cdots \\
&= \mathcal{E}^* \cdot \mathcal{E} \cdot (\varepsilon \otimes \varepsilon + \mathcal{E} + \mathcal{E}^2 + \cdots) \\
&= \mathcal{E}^* \cdot \mathcal{E} \cdot \mathcal{E}^* \\
&= \sum_{n \geq 1} \sum_{p+q=n-1} \mathcal{E}^p \mathcal{E} \mathcal{E}^q \\
&= \sum_{n \geq 1} n \mathcal{E}^n
\end{aligned}$$

Ce qui s'écrit encore :

$$Id \circledast L = \sum_{w \in X^*} |w| \, w \otimes w$$

$\diamondsuit$

Preuve : (du théorème 4.4)

Montrons que tout élément primitif (polynôme ou série) est un élément de Lie.

Soit S une série primitive. Elle est donc orthogonale à tous les mélanges propres. Considérons l'application linéaire :

$$\begin{aligned}
f : K\langle\langle X \otimes X \rangle\rangle &\longrightarrow K\langle X \rangle \\
u \otimes v &\longmapsto \langle S|u \rangle v
\end{aligned}$$

D'après la proposition 4.3, on a :

$$\sum_{u \in X^*} (u \sqcup\!\sqcup v) \otimes u\ell(v) \quad = \quad \sum_{w \in X^*} |w| \, w \otimes w$$

Prenons l'image par f des deux membres :

$$\sum_{u \in X^*} \langle S|u \sqcup\!\sqcup v \rangle \, u\ell(v) \quad = \quad \sum_{w \in X^*} |w| \, \langle S|w \rangle \, w$$

Puisque S est orthogonale aux mélanges propres, et que $\ell(\varepsilon) = 0$, cette égalité se ramène à :

$$\sum_{v \in X^*} \langle S|v \rangle \ell(v) \quad = \quad \sum_{w \in X^*} |w| \, \langle S|w \rangle w$$

On en déduit, pour tout $n > 0$:

$$\sum_{|w|=n} \langle S|w \rangle \, w \quad = \quad \frac{1}{n} \sum_{|v|=n} \langle S|v \rangle \ell(v)$$

Ainsi, chacune des composantes homogènes de S est un polynôme de Lie. S est donc une série de Lie. $\diamondsuit$

4.6 Caractérisation des exponentielles de Lie

Théorème 4.5 *Soit T une série formelle. Les conditions suivantes sont équivalentes.*

(i) *T est l'exponentielle d'une série de Lie*
(ii) *$\Gamma(T) = T \otimes T$ (on dit alors que T est* group-like*)*
(iii) *L'application $w \mapsto \langle T|w\rangle$ est un morphisme pour le produit de mélange.*

Preuve :

$(i) \Longrightarrow (ii)$ Supposons $T = e^L$ où L est une série de Lie. Le coproduit Γ est un morphisme pour la concaténation. On en déduit qu'il commute avec l'exponentielle. On a alors :

$$\Gamma(T) \;=\; \Gamma(e^L) \;=\; e^{\Gamma(L)} \;=\; e^{L\otimes 1 + 1 \otimes L}$$

Or les deux termes $L \otimes 1$ et $1 \otimes L$ commutent, l'exponentielle de la somme est le produit des exponentielles :

$$\begin{aligned}
\Gamma(T) &= e^{L\otimes 1} \cdot e^{1\otimes L} \\
&= (e^L \otimes 1) \cdot (1 \otimes e^L) \\
&= e^L \otimes e^L \\
&= T \otimes T
\end{aligned}$$

On peut mener les calculs autrement :

$$\begin{aligned}
\Gamma(T) &= e^{L\otimes 1 + 1\otimes L} \\
&= \sum_{n\geq 0} \frac{1}{n!}(L\otimes 1 + 1 \otimes L)^n
\end{aligned}$$

On utilise la formule du binôme et la commutativité de $L \otimes 1$ et $1 \otimes L$

$$\begin{aligned}
&= \sum_{n\geq 0} \frac{1}{n!} \sum_{p+q=n} \frac{n!}{p!q!} L^p \otimes L^q \\
&= \left(\sum_{p\geq 0} \frac{1}{p!} L^p\right) \otimes \left(\sum_{q\geq 0} \frac{1}{q!} L^q\right) \\
&= e^L \otimes e^L \\
&= T \otimes T
\end{aligned}$$

$(ii) \Longrightarrow (i)$ Supposons maintenant que $\Gamma(T) = T \otimes T$ et $\langle T|\varepsilon\rangle = 1$. On peut calculer son logarithme. On pose $T = 1 + H$ et on a :

$$\log(T) = H - \frac{1}{2}H^2 + \frac{1}{3}H^3 - \frac{1}{4}H^4 + \cdots$$

Le produit de $T \otimes 1$ par $1 \otimes T$ est commutatif. Le logarithme du produit est donc la somme des logarithmes.

$$\begin{aligned}
\Gamma(\log(T)) &= \log(\Gamma(T)) \\
&= \log(T \otimes T) \\
&= \log((T \otimes 1) \cdot (1 \otimes T))
\end{aligned}$$

or le produit $(T \otimes 1) \cdot (1 \otimes T)$ est commutatif,

$$\begin{aligned} &= \log(T \otimes 1) + \log(1 \otimes T) \\ &= \log(T) \otimes 1 + 1 \otimes \log(T) \end{aligned}$$

On en déduit que $\log(T)$ est un élément primitif, c'est donc une série de Lie. T est donc l'exponentielle d'une série de Lie.

$(i) \Longrightarrow (iii)$ Supposons que $\Gamma(T) = T \otimes T$. Soient $u,v \in X^*$ deux mots. On a :

$$\begin{aligned} \langle T | u ⧢ v \rangle &= \langle \Gamma(T) | u \otimes v \rangle \\ &= \langle T \otimes T | u \otimes v \rangle \\ &= \langle T | u \rangle \langle T | v \rangle \end{aligned}$$

Donc, l'application $w \mapsto \langle T | w \rangle$ est un morphisme pour le produit de mélange.

$(iii) \Longrightarrow (i)$ On suppose que l'application $w \mapsto \langle T | w \rangle$ est un morphisme pour le produit de mélange. On a alors

$$\begin{aligned} \Gamma(T) &= \sum_{u,v \in X^*} \langle \Gamma(T) | u \otimes v \rangle \, u \otimes v \\ &= \sum_{u,v \in X^*} \langle T | u ⧢ v \rangle \, u \otimes v \\ &= \sum_{u,v \in X^*} \langle T | u \rangle \langle T | v \rangle \, u \otimes v \\ &= T \otimes T \end{aligned}$$

$\diamondsuit$

4.7 Bases de l'algèbre de Lie

Les deux bases les plus connues sont la *base de Lyndon* et la *base de Hall*. Dans ce cours, nous nous intéressons à la base de Lyndon.

4.7.1 Crochets de Lyndon

Soit X un alphabet ordonné. L'ensemble des *crochets de Lyndon* sur X, noté $Lyndon\langle X \rangle$, est défini récursivement de la façon suivante :

- (i) Les lettres de X sont des crochets de Lyndon.
- (ii) Si x est une lettre et $y \in Lyndon\langle X \rangle$ est un crochet de Lyndon, alors $[x,y]$ est un crochet de Lyndon si et seulement si $x < y$
- (iii) Si $[x,y],z \in Lyndon\langle X \rangle$ sont des crochets de Lyndon, alors $[[x,y],z]$ est un crochet de Lyndon si et seulement si $xy < z \leq y$.

Dans cette définition, on a utilisé un ordre sur les éléments de $Lyndon\langle X\rangle$. Cet ordre est hérité de l'ordre lexicographique défini sur X^*. En effet, soit δ la fonction qui à tout élément de $Lyndon\langle X\rangle$ associe le mot de X^* obtenu en supprimant tous les crochets, on dira que $u < v$, pour $u,v \in Lyndon\langle X\rangle$ si et seulement si $\delta(u) < \delta(v)$ dans X^*.

Exemple 4.4 *Soit $X = \{x_0,x_1\}$ avec $x_0 < x_1$. Les premiers crochets de Lyndon sont :*

$$\{x_0, x_1, [x_0, x_1], [x_0, [x_0, x_1]], [[x_0, x_1], x_1], [x_0, [x_0, [x_0, x_1]]], \dots\}$$

Ces crochets sont produits dans l'ordre :

$$x_0 < x_1 < [x_0, x_1] < [x_0, [x_0, x_1]] < [[x_0, x_1], x_1] < [x_0, [x_0, [x_0, x_1]]]$$

car

$$x_0 < x_1 < x_0x_1 < x_0x_0x_1 < x_0x_1x_1 < x_0x_0x_0x_1$$

Théorème 4.6 *Les crochets de Lyndon forment une base de l'algèbre de Lie libre $\mathcal{L}ie\langle X\rangle$ appelée* base de Lyndon.

4.7.2 Crochetage et décrochetage

Décrochetage

Théorème 4.7 *L'opération de décrochetage δ définie précédemment est une bijection de $Lyndon\langle X\rangle$ dans $\mathcal{L}yndon(X)$.*

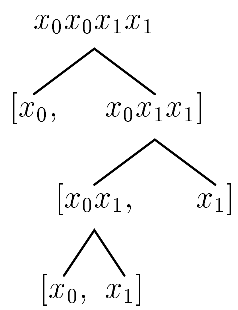
Crochetage des mots de Lyndon

Définition 4.4 *Soit $w \in \mathcal{L}yndon(X)$ un mot de Lyndon. La* factorisation *$w = lm$ est dite standard si et seulement si m est le* plus long *facteur droit propre de w qui est un mot de Lyndon*

L'opération c de crochetage des mots de Lyndon peut être définie récursivement comme suit :

$$\begin{cases} c(x) = x & \text{si } x \text{ est une lettre} \\ c(w) = [c(l), c(m)] & \text{si } \sigma(w) = (l,m) \text{ est la factorisation standard.} \end{cases}$$

Exemple 4.5 *Soit $X = \{x_0,x_1\}$ avec $x_0 < x_1$. Soit le mot $w = x_0^2x_1^2$.*



Autrement dit $c(x_0^2x_1^2) = [x_0,[[x_0,x_1],x_1]]$ *et non pas* $[[x_0,[x_0,x_1]],x_1]$.

Exercice 4.3 *Sur* $X = \{x_0,x_1\}$ *avec* $x_0 < x_1$, *on considère le mot de Lyndon* $l = x_0^2x_1x_0x_1^2$. *Donner son crochetage de Lyndon.*

4.8 Représentation dans la base de Lyndon

Un polynôme de Lie $P \in \mathcal{L}ie\langle X\rangle$ est considéré comme une combinaison linéaire de crochets de Lyndon :

$$P \;=\; \sum_{i=1}^{n} \alpha_i[l_i], \qquad \text{avec } \alpha_i \in K$$

où $[l_i] = c(l_i)$ est le crochetage de Lyndon du mot de Lyndon l_i.

4.8.1 Calcul du crochet de Lie de deux polynômes

Il suffit de savoir calculer le crochet de Lie de deux crochets de Lyndon. Soient u et v deux crochets de Lyndon. Le problème vient du fait que $\sigma(\delta(u)\delta(v))$ n'est pas toujours égale à $(\delta(u),\delta(v))$.

Si $u < v$, alors $\delta(u)\delta(v)$ est un mot de Lyndon. On peut toujours se ramener à ce cas en utilisant éventuellement l'anticommutativité du crochet de Lie.

Si $\sigma(\delta(u)\delta(v)) = (\delta(u),\delta(v))$, alors le problème est réglé puisque $c(\delta(u)\delta(v)) = [u,v]$. Sinon, on pose $u = [u_0,u_1]$ avec $\sigma(\delta(u)) = (\delta(u_0),\delta(u_1))$. Si $u_1 \geq v$ alors la factorisation uv est standard et le problème est résolu. Dans le cas contraire, on utilise l'identité de Jacobi :

$$\begin{aligned} [u,v] &= [[u_0,u_1],v] \\ &= [u_0,[u_1,v]] + [[u_0,v],u_1] \end{aligned}$$

Par hypothèse, on a :

$$u_0 \;<\; u_0u_1 \;<\; u_1 \;<\; v$$

Posons $x = \delta([[u_0,u_1],v])$. Sa factorisation n'est pas forcément standard, mais on est passé de $[[u_0,u_1],v]$ à $[u_0,[u_1,v]]$ dont la longueur du facteur gauche a strictement diminué.

Posons $y = \delta([[u_0,v],u_1])$. On sait que $\delta([u_0,v])$ est un mot de Lyndon, ce qui nous ramène au problème de départ à ceci près :

$$[[u_0,u_1],v] \;<\; [[u_0,v],u_1]$$

pour l'ordre lexicographique.

4.8.2 Calcul du miroir d'un polynôme de Lie

Par définition, le miroir d'un polynôme P est obtenu en y remplaçant chacun de ses mots par son miroir.

Exemple 4.6 *Soit $X = \{x_0,x_1\}$ avec $x_0 < x_1$. Soit le polynôme*

$$\begin{aligned} P &= [x_0, x_1] + [x_0, [x_0, x_1]] \\ &= x_0x_1 - x_1x_0 + x_0^2x_1 - 2\,x_0x_1x_0 + x_1x_0^2 \end{aligned}$$

Alors

$$\begin{aligned} \tilde{P} &= x_1x_0 - x_0x_1 + x_1x_0^2 - 2\,x_0x_1x_0 + x_0^2x_1 \\ &= -[x_0, x_1] + [x_0, [x_0, x_1]] \end{aligned}$$

Proposition 4.4 *Le miroir d'un polynôme de Lie est obtenu par simple changement de signe de ses crochets de longueur paire. C'est-à-dire*

$$P \;=\; \sum_i \alpha_i\,[l_i] \quad\Longrightarrow\quad \tilde{P} \;=\; \sum_i -(-1)^{|l_i|}\alpha_i\,[l_i]$$

4.8.3 Identification d'un polynôme de Lie

Étant donné un polynôme en variables non commutatives, existe-t-il un algorithme simple pour décider si c'est un polynôme de Lie ? Si oui, comment calculer sa décomposition en crochets de Lyndon ?

Soit l un mot de Lyndon. On note $[l]$ le polynôme de Lie correspondant.

Lemme 4.5 *l est le plus petit mot apparaissant dans $[l]$ et son coefficient est égal à 1. Autrement dit*

$$[l] \;=\; l + \sum_{\substack{w\in X^{|w|}\\ w>l}} \alpha_w\,w$$

Preuve : (par récurrence sur la longueur des mots de Lyndon)

On va montrer que l est le plus petit mot de $[l]$.

(a) Si l est une lettre, alors $[l] = l$. Donc $[l]$ est un polynôme homogène de plus petit mot l.

(b) Supposons que tout mot de Lyndon de longueur inférieure ou égale à un entier $n > 1$ vérifie la proposition.

(c) Soit l un mot de Lyndon de longueur $n + 1$. Nous avons $[l] = [l_1][l_2] - [l_2][l_1]$ avec $\sigma(l) = (l_1,l_2)$ et donc $l_1 < l_2$. Par hypothèse, $[l_1]$ et $[l_2]$ sont deux polynômes homogènes de plus petits mots l_1 et l_2 respectivement. Les mots l_1l_2 et l_2l_1 sont les plus petits dans les polynômes $[l_1][l_2]$ et $[l_2][l_1]$ respectivement. Nous savons de plus que $l = l_1l_2 < l_2$ et par définition de l'ordre lexicographique $l_2 < l_2l_1$. Donc l est le plus petit mot du polynôme $[l]$.

$\diamondsuit$

Exemple 4.7

$$[x_0,[x_1,x_2]] \quad = \quad x_0x_1x_2 - x_0x_2x_1 - x_1x_2x_0 + x_2x_1x_0$$

Certains de la somme peuvent être eux-même des mots de Lyndon. Dans l'exemple précédent, $x_0x_2x_1$ est un mot de Lyndon.

Corollaire 4.1 *Le plus petit mot d'un polynôme de Lie est un mot de Lyndon*

Preuve :

Il suffit de considérer le plus petit crochet de Lyndon intervenant dans la décomposition de polynôme de Lie. $\diamondsuit$

4.9 L'algèbre enveloppante

Définition 4.5 *L'*algèbre enveloppante *d'une algèbre de Lie $\mathcal{L}$ est définie comme le quotient $\mathcal{U} = \mathcal{T}/\mathcal{I}$ de l'*algèbre tensorielle $\mathcal{T} = \mathcal{L}^0 \oplus \mathcal{L}^1 \oplus \mathcal{L}^2 \oplus \cdots \oplus \mathcal{L}^n \oplus \cdots$ *avec*

$$\mathcal{L}^0 \quad = \quad K, \qquad \mathcal{L}^n \quad = \quad \underbrace{\mathcal{L} \otimes \mathcal{L} \otimes \cdots \otimes \mathcal{L}}_{n \text{ facteurs}}$$

par l'idéal $\mathcal{I}$ engendré par les éléments de la forme :

$$x \otimes y - y \otimes x - [x,y] \quad \text{pour } x,y \in \mathcal{L}$$

Théorème 4.8 *L'algèbre enveloppante de l'algèbre de Lie libre $\mathcal{L}ie\langle X\rangle$ s'identifie à l'algèbre des polynômes non commutatifs $K\langle X\rangle$.*

4.9.1 Base de Poincaré-Birkoff-Witt

Théorème 4.9 (PBW) *Soit $(P_i)_{i\geq 1}$ une base totalement ordonnée de l'algèbre de Lie libre $\mathcal{L}ie\langle X\rangle$. Alors son algèbre enveloppante admet comme base l'ensemble des éléments de la forme $P_{i_1}P_{i_2}\cdots P_{i_n}$ avec $P_{i_1} \geq P_{i_2} \geq \cdots \geq P_{i_n}$ et $n \geq 0$.*

Ce théorème appliqué à la base de Lyndon $Lyndon(X)$ de l'algèbre de Lie libre $\mathcal{L}ie\langle X\rangle$ nous fournit une base de l'algèbre $K\langle X\rangle$, que nous noterons *PBWL*.

Remarque 4.2 *Il existe une bijection entre les deux bases X^* (base canonique) et PBWL.*

Soit $w \in X^*$; considérons la factorisation en produit décroissant de mots de Lyndon :

$$w \quad = \quad l_1l_2\cdots l_n \quad \text{avec } l_1 \geq l_2 \cdots \geq l_n.$$

Il lui correspond alors un élément Q_w de la base *PBWL* défini par

$$Q_w \quad = \quad [l_1][l_2]\cdots[l_n]$$

où $[l_1],[l_2],\ldots,[l_n]$ désignent les polynômes de Lie associés aux mots de Lyndon $l_1,l_2,\ldots,l_n$ respectivement.

4.9.2 Décomposition d'un mot dans la base *PBWL*

L'algorithme est basé sur la formule :

$$x_0x_1 \quad = \quad [x_0,x_1] + x_1x_0$$

qui est la décomposition du mot x_0x_1 dans la base *PBWL*.

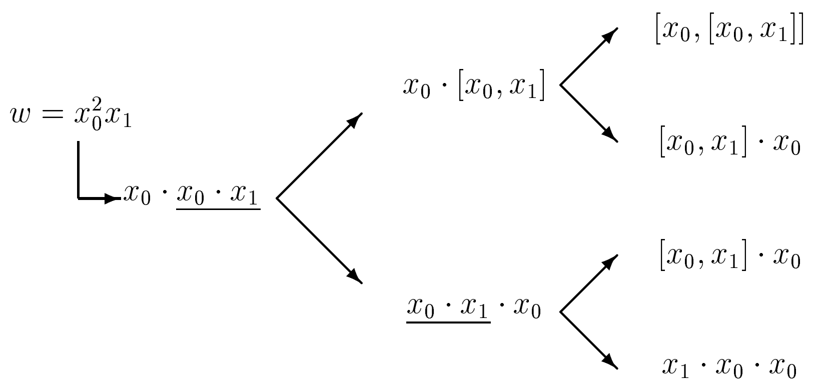
Lemme 4.6 *Soit $ll = \{x_1,x_2,\cdots,x_n\}$ une liste standard (voir chapitre 2, section 2.4) représentant un produit de crochets de Lyndon. Soit (x_i,x_{i+1}) la dernière inversion $x_i < x_{i+1}$ de ll. Alors les listes*

$$\begin{cases} ll_0 & = & \{x_1,\ldots, & [x_i,x_{i+1}], & \ldots,x_n\} \\ ll_1 & = & \{x_1,\ldots, & x_{i+1},x_i, & \ldots,x_n\} \end{cases}$$

sont standards.

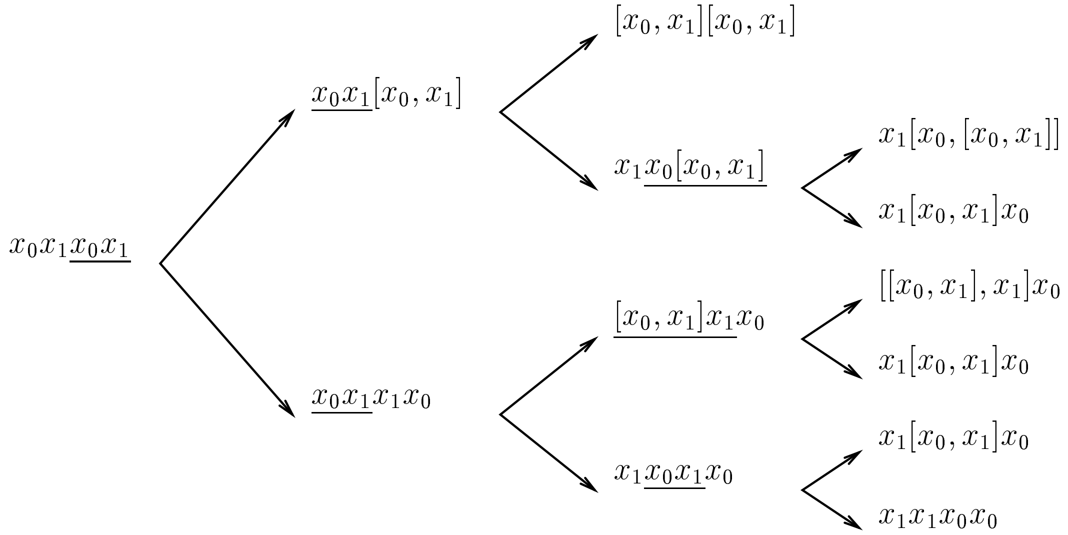
L'algorithme de décomposition d'un mot w peut être vu comme un système de réécriture $ll \longrightarrow ll_0 + ll_1$ où la liste ll initiale est formée des lettres de w.

Exemple 4.8 *Soit $X = \{x_0,x_1\}$ un alphabet. Soit à décomposer le mot $w = x_0^2x_1$ dans la base PBWL. Le déroulement de l'algorithme est le suivant :*



$$\textit{Ainsi,} \qquad w = [x_0,[x_0,x_1]] + 2\,[x_0,x_1] \cdot x_0 + x_1x_0^2.$$

Soit maintenant à décomposer le mot $w = x_0x_1x_0x_1$.



D'où

$$x_0x_1x_0x_1 \quad = \quad [x_0,x_1]^2 + x_1 \cdot [x_0,[x_0,x_1]] + 3\,x_1 \cdot [x_0,x_1] \cdot x_0 + [[x_0,x_1],x_1] \cdot x_0 + x_1^2x_0^2$$

4.9.3 Les polynômes dans la base de *PBWL*

L'idée est de représenter les polynômes de $K\langle X\rangle$ dans la base de *PBWL* et de maintenir cette représentation pour les opérations de somme et de produit. La représentation d'un polynôme dans la base *PBWL* revient à la représentation de chacun de ses mots dans cette base.

Produit de deux polynômes

Le problème est résolu si l'on sait multiplier deux éléments de la base de *PBWL* et exprimer le produit dans cette même base.

Soient $u = p_1p_2\cdots p_i$ et $v = q_1q_2\cdots q_j$ deux éléments de la base *PBWL*.

On a :

$$uv \quad = \quad p_1\cdots p_i \bullet q_1\cdots q_j$$

Si $p_i \geq q_1$, c'est fini ; sinon on effectue la réécriture :

$$\begin{aligned} uv \quad = \quad & p_1\ldots p_{i-1} \bullet [p_i,q_1] \bullet q_2\ldots q_j \\ & + p_1\ldots p_{i-1} \bullet \ q_1\ p_i\ \bullet q_2\ldots q_j \end{aligned}$$

Il convient de traiter le crochet $[p_i,q_1]$ car cette factorisation n'est pas forcément standard.

Les $\bullet$ signalent les endroits où l'ordre des facteurs est peut–être incorrect. Il faut donc relancer récursivement l'algorithme pour traiter les inversions éventuelles. Il est assez facile de prouver que ce processus termine. Cependant, l'algorithme doit être programmé avec soin si l'on souhaite limiter le nombre de comparaisons à effectuer.

Expression d'un polynôme distribué dans la base *PBWL*

Le problème consiste à calculer la décomposition dans la base *PBWL* d'un polynôme p exprimé comme une combinaison linéaire de mots de X^*.

Il est bien sûr possible de convertir séparément chaque mot de p ; un autre algorithme inspiré du lemme suivant peut être plus efficace.

Lemme 4.7 *w est le plus petit mot du polynôme Q_w i.e.*

$$Q_w \;=\; w + \sum_{\substack{u \in X^* \\ |u|=|w| \\ u<w}} \alpha_u u \quad \textit{avec } \alpha_u \in K$$

Preuve :

Assez facile à partir du lemme 4.5. $\diamondsuit$

Exercice 4.4 *Écrire en Maple l'algorithme de décomposition d'un polynôme dans la base PBWL.*

Théorème 4.10 (Radford) *Tout mot $w \in X^*$ peut s'écrire comme combinaison linéaire (finie) de produits de mélange de mots de Lyndon.*

Preuve :

Elle se fait par la construction d'un système d'équations "triangulaire".

On va se contenter de montrer comment marche l'algorithme sur tous les mots comportant 2 occurences de la lettre x_0 et 2 occurences de la lettre x_1. Il y a donc six mots à considérer. On va les examiner par ordre lexicographique.

1) $x_0x_0x_1x_1 \in \mathcal{L}yndon(X)$. Il n'y a rien à faire.
2) $x_0x_1x_0x_1 = x_0x_1 {\cdot} x_0x_1$ (factorisation de Lyndon). On calcule alors le produit de mélange $x_0x_1 ш x_0x_1$:

$$\begin{aligned} x_0x_1 ш x_0x_1 &= 2\,x_0\,(x_1 ш x_0x_1) \\ &= 2\,x_0x_1x_0x_1 + 4\,x_0x_0x_1x_1 \end{aligned}$$

on en déduit

$$x_0x_1x_0x_1 = \frac{1}{2} x_0x_1 ш x_0x_1 - 2\,x_0x_0x_1x_1 \tag{4.3}$$

or x_0x_1 et $x_0x_0x_1x_1$ sont des mots de Lyndon, donc c'est fini.
3) $x_0x_1x_1x_0 = x_0x_1x_1 {\cdot} x_0$ (factorisation de Lyndon). On calcule alors le produit de mélange $x_0x_1x_1 ш x_0$:

$$x_0x_1x_1 ш x_0 = 2\,x_0x_0x_1x_1 + x_0x_1x_0x_1 + x_0x_1x_1x_0$$

on en déduit

$$x_0x_1x_1x_0 = x_0x_1x_1 \sqcup\!\sqcup\, x_0 - 2\, x_0x_0x_1x_1 - x_0x_1x_0x_1 \tag{4.4}$$

or x_0,$x_0x_1x_1$ et $x_0x_0x_1x_1$ sont des mots de Lyndon et l'on a déjà calculé $x_0x_1x_0x_1$ comme combinaison linéaire de produits de mélange de mots de Lyndon, donc c'est fini.

4) $x_1x_0x_0x_1 = x_1 \cdot x_0x_0x_1$ (factorisation de Lyndon). On calcule le produit de mélange $x_1 \sqcup\!\sqcup\, x_0x_0x_1$:

$$x_1 \sqcup\!\sqcup\, x_0x_0x_1 = x_1x_0x_0x_1 + x_0x_1x_0x_1 + 2\, x_0x_0x_1x_1$$

on en déduit

$$x_1x_0x_0x_1 = x_1 \sqcup\!\sqcup\, x_0x_0x_1 - x_0x_1x_0x_1 - 2\, x_0x_0x_1x_1 \tag{4.5}$$

les mots x_1, $x_0x_0x_1$ et $x_0x_0x_1x_1$ sont des mots de Lyndon et le mot $x_0x_1x_0x_1$ a déjà été décomposé. C'est donc fini.

5) $x_1x_0x_1x_0 = x_1 \cdot x_0x_1 \cdot x_0$ (factorisation de Lyndon). On calcule le produit de mélange $x_1 \sqcup\!\sqcup\, x_0x_1 \sqcup\!\sqcup\, x_0$:

$$x_1 \sqcup\!\sqcup\, x_0x_1 \sqcup\!\sqcup\, x_0 = x_1x_0x_1x_0 + 2\, x_1x_0x_0x_1 + 3\, x_0x_1x_0x_1 + 4\, x_0x_0x_1x_1 + 2\, x_0x_1x_1x_0$$

on en déduit

$$\begin{aligned} x_1x_0x_1x_0 = {} & x_1 \sqcup\!\sqcup\, x_0x_1 \sqcup\!\sqcup\, x_0 - 2\, x_1x_0x_0x_1 - 3\, x_0x_1x_0x_1 \\ & - 4\, x_0x_0x_1x_1 - 2\, x_0x_1x_1x_0 \end{aligned} \tag{4.6}$$

les mots x_1, x_0x_1 et $x_0x_0x_1x_1$ sont des mots de Lyndon et les mots $x_1x_0x_0x_1$,$x_0x_1x_0x_1$ et $x_0x_1x_1x_0$ ont déjà été décomposés (4.5, 4.3 et 4.4).

6) $x_1x_1x_0x_0 = x_1 \cdot x_1 \cdot x_0 \cdot x_0$ (factorisation de Lyndon). On calcule le produit de mélange $x_1 \sqcup\!\sqcup\, x_1 \sqcup\!\sqcup\, x_0 \sqcup\!\sqcup\, x_0$:

$$\begin{aligned} x_1 \sqcup\!\sqcup\, x_1 \sqcup\!\sqcup\, x_0 \sqcup\!\sqcup\, x_0 = {} & 4\, x_1x_1x_0x_0 + 4\, x_1x_0x_1x_0 + 4\, x_1x_0x_0x_1 \\ & + 4\, x_0x_0x_1x_1 + 4\, x_0x_1x_0x_1 + 4\, x_0x_1x_1x_0 \end{aligned}$$

on en déduit

$$\begin{aligned} x_1x_1x_0x_0 = {} & \frac{1}{4} x_1 \sqcup\!\sqcup\, x_1 \sqcup\!\sqcup\, x_0 \sqcup\!\sqcup\, x_0 - x_1x_0x_1x_0 - x_1x_0x_0x_1 \\ & - x_0x_0x_1x_1 - x_0x_1x_0x_1 - x_0x_1x_1x_0 \end{aligned} \tag{4.7}$$

les mots x_0, x_1 et $x_0x_0x_1x_1$ sont des mots de Lyndon et les mots $x_1x_0x_1x_0$, $x_1x_0x_0x_1$, $x_0x_1x_0x_1$ et $x_0x_1x_1x_0$ ont déjà été décomposés (4.6, 4.5, 4.3 et 4.4).

$\diamondsuit$

4.9.4 Base duale

Supposons connue, pour chaque élément Q_w de la base $PBWL$, un polynôme S_{Q_w} que l'on note simplement S_w de $\mathbb{Q}\langle X\rangle$, et supposons vérifiées les conditions :

$$\forall\, Q_{w'} \in PBWL, \quad \langle S_w | Q_{w'}\rangle \;=\; \delta_{Q_w}^{Q_{w'}} \;=\; \begin{cases} 1 & \text{si } Q_w = Q_{w'} \\ 0 & \text{sinon} \end{cases}$$

Tout polynôme $P \in \mathbb{Q}\langle X\rangle$ peut s'écrire sous la forme

$$P \;=\; \sum_{Q_w \in PBWL} \alpha_w\, Q_w$$

$\alpha_w \in \mathbb{Q}$. On obtient alors, pour $Q_w \in PBWL$:

$$\langle S_w | P\rangle \;=\; \sum_{Q_{w'} \in PBWL} \alpha_{w'}\, \langle S_w | Q_{w'}\rangle \;=\; \alpha_w$$

Le coefficient α_w est donc obtenu par un simple produit scalaire.

On a donc tout intérêt à pouvoir calculer une fois pour toute les polynômes S_w, qui forment la “base duale” de $PBWL$.

Algorithme :

On fait d'abord les remarques suivantes :

1) Tout élément $Q_w \in PBWL$ est *multihomogène* : il est combinaison linéraire de mots qui ont tous le même nombre de x_0 et le même nombre de x_1.
2) En conséquence, on pourra imposer que pour tout $Q_w \in PBWL$, S_w soit un polynôme multihomogène de même *multidegré* que Q_w.
3) Pour chaque multidegré fixé, les équations de définition $\langle S_w | Q_{w'}\rangle = \delta_{Q_w}^{Q_{w'}}$ vont définir un système d'équations linéaires, dont les coefficients du polynôme S_w sur les mots u (de même multidegré que Q_w) forment une matrice *triangulaire inversible.*

La remarque 3) est le point crucial de la construction de la base duale. Nous n'allons pas le démontrer. Nous allons simplement faire fonctionner, à la main, l'algorithme pour des multidegrés petits. Le multidegré (n,m) signifie que x_0 apparaît n fois et x_1 apparaît m fois.

Multidegré $(0,0)$ S_ε est calculé directement :

$$\begin{aligned} \langle S_\varepsilon | \varepsilon\rangle &= 1 \\ \langle S_\varepsilon | Q_w\rangle &= 0 \quad \text{pour tout } Q_w \in PBWL \setminus \{\varepsilon\} \end{aligned}$$

On en déduit que $S_\varepsilon = \varepsilon$.

Multidegré $(1,0)$ On va calculer S_{x_0} :

$$\begin{aligned} \langle S_{x_0} | \varepsilon\rangle &= 0, \\ \langle S_{x_0} | x_0\rangle &= 1, \\ \langle S_{x_0} | x_1\rangle &= 0 \end{aligned}$$

et $\langle S_{x_0} | Q_w\rangle = 0$ si le multidegré de Q_w n'est pas $(1,0)$, c'est-à-dire si Q_w est multihomogène de degré > 2. Donc : $S_{x_0} = x_0$

Multidegré (0,1) On trouve de même que $S_{x_1} = x_1$.
Multidegré (2,0) On trouve de même que $S_{x_0x_0} = x_0x_0$.
Multidegré (1,1) On trouve de même que $S_{x_0x_1} = x_0x_1$.
Multidegré (0,2) On trouve de même que $S_{x_1x_1} = x_1x_1$.
Multidegré (3,0) On trouve de même que $S_{x_0x_0x_0} = x_0x_0x_0$.
Multidegré (0,3) On trouve de même que $S_{x_1x_1x_1} = x_1x_1x_1$.
Multidegré (2,1) Pour ce multidegré, il y a dans *PBWL* les éléments :

$$[x_0, [x_0, x_1]], \quad [x_0, x_1] \cdot x_0 \quad \text{et } x_1 \cdot x_0 \cdot x_0$$

Calculons $S_{x_0x_0x_1}$.

$$\begin{aligned}
\langle S_{x_0x_0x_1} | [x_0, [x_0, x_1]] \rangle = \langle S_{x_0x_0x_1} | x_0x_0x_1 - 2\, x_0x_1x_0 + x_1x_0x_0 \rangle &= 1, \\
\langle S_{x_0x_0x_1} | [x_0, x_1] \cdot x_0 \rangle = \langle S_{x_0x_0x_1} | x_0x_1x_0 - x_1x_0x_0 \rangle &= 0 \\
\langle S_{x_0x_0x_1} | x_1 \cdot x_0 \cdot x_0 \rangle = \langle S_{x_0x_0x_1} | x_1x_0x_0 \rangle &= 0
\end{aligned}$$

On en déduit

$$S_{x_0x_0x_1} = x_0x_0x_1$$

Calculons $S_{x_0x_1 \cdot x_0}$.

$$\begin{aligned}
\langle S_{x_0x_1 \cdot x_0} | [x_0, [x_0, x_1]] \rangle &= 0, \\
\langle S_{x_0x_1 \cdot x_0} | [x_0, x_1] \cdot x_0 \rangle &= 1, \\
\langle S_{x_0x_1 \cdot x_0} | x_1 \cdot x_0 \cdot x_0 \rangle &= 0
\end{aligned}$$

On en déduit

$$S_{x_0x_1 \cdot x_0} = 2\, x_0x_0x_1 + x_0x_1x_0$$

Calculons $S_{x_1 \cdot x_0 \cdot x_0}$.

$$\begin{aligned}
\langle S_{x_1 \cdot x_0 \cdot x_0} | [x_0, [x_0, x_1]] \rangle &= 0, \\
\langle S_{x_1 \cdot x_0 \cdot x_0} | [x_0, x_1] \cdot x_0 \rangle &= 0, \\
\langle S_{x_1 \cdot x_0 \cdot x_0} | x_1 \cdot x_0 \cdot x_0 \rangle &= 1
\end{aligned}$$

On en tire successivement

$$\begin{aligned}
\langle S_{x_1 \cdot x_0 \cdot x_0} | x_0x_1x_0 \rangle &= 1 \\
\langle S_{x_1 \cdot x_0 \cdot x_0} | x_0x_0x_1 \rangle &= 2 - 1 \ = \ 1 \\
S_{x_1 \cdot x_0 \cdot x_0} &= x_0x_0x_1 + x_0x_1x_0 + x_1x_0x_0
\end{aligned}$$

Multidegré (1,2) Des calculs analogues donnent :

$$\begin{aligned}
S_{x_0x_0x_1} &= x_0x_1x_1 \\
S_{x_1 \cdot x_0x_1} &= x_1x_0x_1 + 2\, x_0x_1x_1 \\
S_{x_1 \cdot x_1 \cdot x_0} &= x_0x_1x_1 + x_1x_0x_1 + x_1x_1x_0
\end{aligned}$$

Le théorème suivant qui définit de manière générale et récursive les S_w, $w \in X^*$.

Théorème 4.11 *La base duale de la base PBWL est définie par :*

1. $S_\varepsilon = \varepsilon$.
2. *Si* $l = xw \in \mathcal{L}yndon(X)$ *alors* $S_l = x \cdot S_w$.
3. *Si la factorisation en produit décroissant de mots de Lyndon de* w *est* $l_1^{\alpha_1} l_2^{\alpha_2} \ldots l_n^{\alpha_n}$, *alors* $S_w = \dfrac{1}{\alpha_1!\alpha_2!\cdots\alpha_n!} S_{l_1}^{\sqcup\!\sqcup\,\alpha_1} \sqcup\!\sqcup\, S_{l_2}^{\sqcup\!\sqcup\,\alpha_2} \sqcup\!\sqcup\, \ldots \sqcup\!\sqcup\, S_{l_n}^{\sqcup\!\sqcup\,\alpha_n}$

4.10 Illustration

On va voir comme illustration les directions tangentes à la sphère. En chaque point sur la sphère, on peut considérer les deux *vecteurs vitesses* suivants :

$\vec{M}$ avancer à 100 km/h en suivant le méridien du nord vers le sud.

$\vec{P}$ avancer à 100 km/h en suivant le parallèle vers l'est.

Les deux vecteurs $\vec{M}$ et $\vec{P}$ sont portés par des directions, c'est-à-dire par des droites tangentes à la sphère. Ils sont situés entièrement dans le plan tangent à la sphère au point considéré. Ils ne sont pas sur la sphère, mais ils s'en "décollent" (voir la figure 4.1).

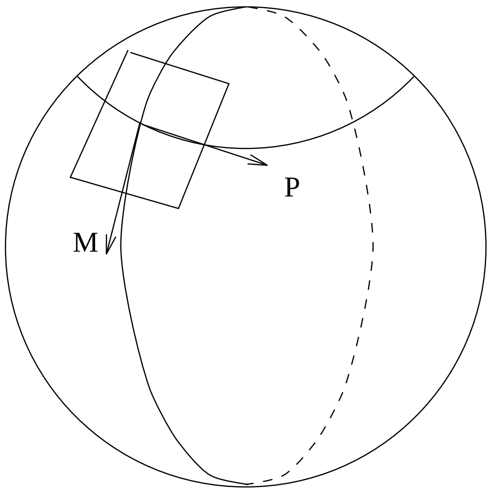


FIG. 4.1 – *Les deux vecteurs vitesses dans le plan tangent*

Par contre, ils indiquent un *mouvement* qui se fait sur la sphère : celui qui est obtenu en faisant une *intégration* de la fonction vitesse. Mathématiquement, cela se traduit par des *exponentielles.*

Le mouvement le long de la sphère, suivant le méridien, pendant 1 heure sera représenté par l'exponentielle e^M. Le mouvement pendant 1 heure suivant le méridien suivi du mouvement pendant 1 heure suivant le parallèle sera représenté par le produit : $e^P e^M$.

Or la direction PM (chemin suivant $\vec{M}$ puis suivant $\vec{P}$) et la direction MP (chemin suivant $\vec{P}$ puis suivant $\vec{M}$) ne sont pas égales, comme on peut s'en rendre compte par un simple dessin (voir la figure 4.2).

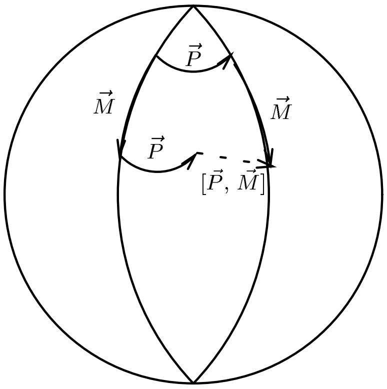


FIG. 4.2 – *Illustration de la nouvelle direction définie par* $[\vec{P}, \vec{M}]$

Par contre, on peut se convaincre que la différence

$$[P, M] \;=\; PM - MP$$

représente une nouvelle direction de mouvement (un nouveau vecteur vitesse).

Sur les véritables mouvements (les exponentielles), on va tester la composition indiquée par le dessin :

$$e^P e^M e^{-P} e^{-M}$$

(on chemine "à l'envers" suivant $\vec{M}$, puis suivant $\vec{P}$, puis on chemine à l'endroit suivant $\vec{M}$, puis suivant $\vec{P}$).

Le cheminement composé obtenu aura lieu suivant une direction de mouvement qui n'est autre que $[\vec{P}, \vec{M}]$. Vérifions ce fait pour des cheminements durant un temps ε petit.

$$\begin{aligned} e^{\varepsilon P} &= 1 + \varepsilon P + \frac{\varepsilon^2}{2!}P^2 + \mathcal{O}(\varepsilon^3) \\ e^{\varepsilon M} &= 1 + \varepsilon M + \frac{\varepsilon^2}{2!}M^2 + \mathcal{O}(\varepsilon^3) \\ e^{-\varepsilon P} &= 1 - \varepsilon P + \frac{\varepsilon^2}{2!}P^2 + \mathcal{O}(\varepsilon^3) \\ e^{-\varepsilon M} &= 1 - \varepsilon M + \frac{\varepsilon^2}{2!}M^2 + \mathcal{O}(\varepsilon^3) \end{aligned}$$

Dans le produit $e^{\varepsilon P} e^{\varepsilon M} e^{-\varepsilon P} e^{-\varepsilon M}$ beaucoup de termes s'en vont. Il faut calculer soigneusement car le produit n'est pas commutatif. On obtient finalement :

$$e^{\varepsilon P} e^{\varepsilon M} e^{-\varepsilon P} e^{-\varepsilon M} \;=\; 1 + \varepsilon^2 [P, M] + \mathcal{O}(\varepsilon^3)$$

C'est donc bien la direction de mouvement portée par le vecteur $[P, M] = PM - MP$ qui est apparue. Ce nouveau vecteur vitesse est encore un vecteur tangent à la sphère.

Index