OFFPRINT FROM

NEW CONCEPTS AND TECHNOLOGIES IN PARALLEL INFORMATION PROCESSING

edited by

E. R. CAIANIELLO

Director of the Laboratory
of Cybernetics, CNR
Arco Felice, Italy

NATO ADVANCED STUDY INSTITUTES SERIES

Series E: Applied Sciences
Volume 9. New Concepts and Technologies in
Parallel Information Processing

NOORDHOFF – LEYDEN – 1975

SOLUTION NON COMMUTATIVE D'UNE EQUATION DIFFERENTIELLE CLASSIQUE

M.P. SCHÜTZENBERGER

(Fac. Sci. Paris et Laboratorio di Cibernetica del CNR, Arco Felice)

INTRODUCTION

Cette communication fait partie d'une série de recherches poursuivies depuis plusieurs années avec mon ami le Professeur D. Foata sur les nombres d'Euler, c'est à dire sur les coefficients de Hurwitz de la fonction $\operatorname{tg} t + 1/\cos t$.

Les rapports que peuvent avoir de semblables questions arithmétiques avec certains aspects de la cybernétique ont été brillament illustrés par les deux conférenciers qui m'ont précédé et je me bornerai donc à discuter un problème de nature purement technique, à savoir la solution de l'équation différentielle classique $y'' = y\, y'$ dans le cas non commutatif, c'est à dire, par exemple, dans le cas où la fonction inconnue y et ses dérivées y' et y'' appartiennent à un anneau de matrices dont les entrées sont des fonctions de la variable indépendante t .

Dans le cas commutatif, la solution de cette équation qui satisfait les conditions initiales $y(0) = y'(0) = 1$ est précisément la fonction génératrice exponentielle $\operatorname{tg} t + 1/\cos t$ des nombres d'Euler. (Cf (1), (4), (5)). Il me parait assez remarquable que l'on puisse en exprimer la solution dans le cas général au moyen d'une famille infinie de polynomes en les variables (non commutatives) $y(0)$ et $y'(0)$ dont les coefficients numériques dépendent assez simplement des nombres d'Euler.

Dans un premier chapitre nous rappelons quelques éléments du formalisme de la théorie des équations différentielles et, dans les deux suivants, nous appliquons ces notions au cas de $y'' = y\,y'$ Dans le dernier chapitre nous présentons une autre propriété remarquable de l'opérateur associé à cette équation.

I. GENERALITES

I.1. Pour simplifier au maximum ce rappel de notions connues nous nous bornons à considérer une équation différentielle du second ordre.

(1) $y'' = H\,(t, y, y')$

où H est un polynôme dont les coefficients appartiennent à un anneau donné $\mathcal{A}$ de caractéristique zéro. Formellement nous introduisons l'anneau $\bar{\mathcal{A}} = \mathcal{A}[y, y']$ des polynomes à coefficients dans $\mathcal{A}$ en les variables (non commutatives) y et y' et l'anneau $\bar{\mathcal{A}}(t)$ n'ayant qu'un nombre fini de termes non nuls. Par définition, une solution formelle de (1) est un élément

$$Y = \sum_{0 \le n} \frac{t^n}{n!} a_n \quad \text{de} \quad \bar{\mathcal{A}}(t)$$

satisfaisant les deux conditions suivantes :

(2) $a_0 = y \;;\; a_1 = y' \;;\; a_{n+2} \in \bar{\mathcal{A}}$ pour chaque $n \in \mathbb{N}$;

(3) $Y'' = H\,(t, Y, Y')$ où Y' et Y'' sont définies par

(4) $$Y' = \sum_{0 \le n} \frac{t^n}{n!} a_{n+1} \;;\; Y'' = \sum_{0 \le n} \frac{t^n}{n!} a_{n+2} \;.$$

Comme H est un polynome, le coefficient de t^n dans le membre de droite de (3) est pour chaque n un polynome en $a_a, a_1, \ldots, a_{n+1}$ cependant que le coefficient de t^n dans Y" est égal à $\underline{a_{n+2}}$. Il en résulte immédiatement que a_{n+2} est déterminé de façon unique par les a_i d'indices inférieurs, d'où par induction, que tous les a_n appartiennent à $\bar{\mathcal{A}}$. Autrement dit, l'équation (1) admet une et une seule solution formelle satisfaisant $Y(0) = y$, $Y'(0) = y'$.

Soit maintenant φ un morphisme de $\bar{\mathcal{A}}$ dans une algèbre normée. On peut montrer que pour chaque ε positif il existe un ε', positif lui aussi, tel que l'on ait identiquement $||a_n \varphi|| \leq n!\, \varepsilon^n$ quand $||y\varphi||$ et $||y'\varphi||$ sont inférieurs à ε'. Ceci entraine que la série $Y\varphi = \Sigma \frac{t^n}{n!} (a_n\varphi)$ converge absolument au voisinage de l'origine et montre que la solution formelle est bien la solution de (1).

I.2. Nous en venons maintenant au calcul effectif des polynomes a_n et pour cela nous rappelons qu'une dérivation d'un anneau $\mathcal{B}$ quelconque est une application β de $\mathcal{B}$ dans lui même, satisfaisant l'identité :

(5) $(ab)\beta = (a\beta) \cdot b + a \cdot (b\beta)$ pour tout $a, b \in \mathcal{B}$.

$\bar{\mathcal{A}}(t)$ des séries formelles en la variable t dont les coefficients sont dans $\bar{\mathcal{A}}$. Par définition, une solution formelle de (1) est un élément de l'anneau

Nous considérons désormais le cas où $\mathcal{B} = \bar{\mathcal{A}}_{(t)}$ et nous notons ∂ la dérivation de noyau $\bar{\mathcal{A}}$ envoyant t sur 1. On a identiquement $t^n\partial = nt^{n-1}$.

Ceci entraine évidemment que β soit définie par la donnée de son action sur les générateurs de $\mathcal{B}$ et que $\beta\,\mu$ et $\mu\,\beta$ soient aussi des dérivations pour tout morphisme μ de $\mathcal{B}$ dans lui même.

Par conséquent si

$$X = \Sigma \frac{t^n}{n!} b_n$$

est une série formelle (dont les coefficients b_n sont dans $\overline{\mathcal{A}}$) nous aurons la formule habituelle

(6) $\quad X\, \partial^p = \Sigma \frac{t^n}{n!}\, b_{n+p} \qquad (p \in \mathbb{N})$

d'où l'on déduit que $b_n = X\, \partial^n\, \theta$ où θ est le morphisme de $\overline{\mathcal{A}}(t)$ sur son sous-anneau $\overline{\mathcal{A}}$, laissant ce dernier invariant et envoyant t sur 0.

En particulier notre équation différentielle peut s'écrire sous la forme $Y\, \partial^2 = H\, (t, Y, Y\, \partial)$ et les calculs d'identification des coefficients a_n de $\frac{t^n}{n!}$ dans Y effectués plus haut sont équivalents à l'ensemble des équations :

(7) $\quad Y\, \theta = y\ ;\ y\, \partial\, \theta = y' \quad ;\ Y\, \partial^{n+2}\, \theta = H\, \partial^n\, \theta$.

Nous nous proposons de mettre ces relations sous une forme plus compacte. Pour cela nous considérons une suite de nouvelles variables non commutatives $\{x_j\}$ $(j \in \mathbb{N})$, l'algèbre large $\mathcal{A}(t, \{x_j\})$, une dérivation χ de cette algèbre définie par la condition que $a\chi = 0$ pour chaque $a \in \mathcal{A}$, $t\chi = 1$ et $x_j\ \chi = x_{j+1}$ pour chaque $j \in \mathbb{N}$ et enfin le morphisme ξ laissant $\mathcal{A}(t)$ invariant et envoyant chaque x_j sur $X\partial^j$ où $X = \Sigma \frac{t^n}{n!} b_n$ $(b_n \in \mathcal{A})$.

Comme on l'a mentionné plus haut, $\xi\partial$ et $\chi\partial$ sont deux dérivations et par définition elles coincident sur $\mathcal{A}(t)$. En outre pour chaque $j \in \mathbb{N}$ on a $x_j\xi\partial = x_{j+1}\xi = x_j\chi\xi$.

Par conséquent on a

(8) $\quad K\xi\partial = K\chi\xi$

quelque soit la série formelle K en t et les x_j .

Posons maintenant $x_0 = y$, $x_1 = y'$ et définissons une dérivation η de $\bar{\mathcal{A}}(t)$ par les conditions $a\eta = 0$ pour $a \in \mathcal{A}$, $t\,\eta = 1$; $y\,\eta = y'$, $y'\,\eta = H\,(t, y, y')$.

Si $X = Y$ est la solution formelle de notre équation, nous avons l'identité

$$Y\,\partial^{n+2} = H\,(t, x_0, x_1)\,\xi\,\partial^n = H\,(t, x_0, x_1)\,\chi^n\,\xi$$

d'où en particulier $x_2\,\xi = Y\,\partial^2 = H\,(t, x_0, x_1)\,\xi$ puis par induction sur n $x_{n+2}\,\xi = Y\,\partial^{n+2} = H\,\eta^n\,\xi = y\,\eta^{n+2}\,\xi$ ce qui donne enfin d'après (7) la formule cherchée :

$a_n = Y\,\partial^n\,\theta = y\,\eta^n\,\theta$ c'est à dire

$$(9)\quad Y = \sum_{o\le n} \frac{t^n}{n!}\,(y\,\eta^n\,\theta)\ .$$

I.3. Considérons à titre d'exemple l'équation classique

$$y' = ay - yb + c \qquad (a, b, c \in \mathcal{A})$$

dont la solution remonte à Wedderburn. En raison de sa forme particulière la dérivation η se réduit au morphisme de $\bar{\mathcal{A}}(t)$ laissant $\mathcal{A}(t)$ invariant et envoyant y sur $ay - yb + c$. En outre θ se réduit à l'identité. La solution Y est donc égale à

$$y + \frac{t}{1!}\,(ay - by + c) + \dots + \frac{t^n}{n!}\,(y\,\eta^n) + \dots$$

Par induction sur n on pourrait d'ailleurs vérifier que le coefficient $a_n = y\,\eta^n$ peut s'expliciter de la façon suivante :

$$a_n = \sum_{o\le j\le n} (-1)^j \begin{bmatrix} n \\ j \end{bmatrix} a^{n-j}\,y\,b^j + \sum_{o\le j\le n-1} (-1)^j \begin{bmatrix} n-1 \\ j \end{bmatrix} a^{n-1-j} c\, b^j$$

Un autre exemple est fourni par l'équation $y'' = y\,y'$ qui nous interessera plus particulièrement ici. La dérivation η laisse $\mathcal{A}(t)$ invariant et elle envoye y sur y' et y' sur $y\,y' = H$. Les premiers termes du développement de la solution Y sont $Y = y + \frac{t}{1!}\,y' + \frac{t^2}{2!}\,(y\,y') + \dots$ et on calcule :

$$a_3 = (y\, y')\, \eta = y'\, y' + y\, y\, y'$$
$$a_4 = (y'^2 + y^2\, y')\, \eta = y\, y'\, y' + y'\, y\, y' + y'\, y\, y'$$
$$+ y\, y'\, y' + y^2\, y\, y' = (y^3 + 2\, y\, y' + 2\, y'\, y)\, y'$$
$$a_5 = a_4\, \eta = (y^4 + 3\, y^2\, y' + 5\, y\, y'\, y + 3\, y'\, y^2 + 4\, y'^2)\, y'$$
$$a_6 = a_5\, \eta = (y^5 + 4\, y^2\, y' + 9\, y^2\, y'\, y + 9\, y\, y'\, y^2 + 4\, y'\, y^2$$
$$+ 12\, y\, y'^2 + 10\, y'\, y\, y' + 12\, y'^2\, y)\, y'$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

L'expression des coefficients est passablement compliquée et sera donnée (de façon indirecte) dans la section suivante.Les polynomes a_n ont été définis dans un tout autre contexte (où ils sont dénotés par D_{n+1}). Leurs valeurs pour $y = y' = 1$ sont les nombres d'Euler.

II. L'EQUATION $y'' = y\, y'$

II.1. Nous gardons les notations utilisées dans l'exemple ci-dessus et nous nous proposons d'expliciter les polynomes $a_n = y\, \eta^n \in \overline{\mathcal{A}} = \mathcal{A}[y, y']$ au moyen d'un changement de variable. Pour cela nous considérons deux nouvelles variables x et z et l'anneau $\overline{\mathcal{B}} = \mathcal{A}[x, z]$ de leurs polynomes non commutatifs. Nous définissons le morphisme φ, l'anneau de polynomes et la dérivation σ de $\overline{\mathcal{B}}$ par les conditions suivantes :

(10.1) $x\varphi = y$; $z\varphi = - y^2 + 2\, y'$;

(10.2) $x\, \sigma = x^2 + z$; $z\, \sigma = 0$.

Nous établissons d'abord la remarque (11) :

Pour chaque $\eta \in \mathbb{N}$ on a $a_{n+1} = b_n\, \varphi\, y'\, 2^{-n}$ où les b_n sont des polynomes de $\overline{\mathcal{B}}$ définis par la récurrence

$$b_o = 1 \;\; ; \;\; b_{n+1} = b_n\, \sigma + x\, b_n + b_n\, x \;\; (= b_n\, \lambda).$$

Preuve : On a $a_o = y$ et d'après $y\, \eta = y'$ $y'\, \eta = y\, y'$, il existe pour chaque $\eta \in \mathbb{N}$ un polynome a'_n tel que $a_{n+1} = a'_n y'$.

Comme $a'_{n+1} y' = a_{n+1} = a_n \eta = a'_n y' \eta = a'_n \eta y' + a'_n (y' \eta)$ $= a'_n \eta y' - a'_n yy'$, on a la récurrence $a'_{n+1} = a'_n \eta + a'_n y$ avec $a'_o = 1$.

Notons maintenant que φ est un isomorphisme dont l'inverse ψ est définie par $y \psi = x$ et $y' \psi = \frac{1}{2} (x^2 + z)$.
Posant $b_n = a'_n \psi . 2^n$ nous aurons donc $b_o = 1$ et $a_n = b_n \varphi . y'$ pour chaque n positif. De plus les b_n satisferont la relation de récurrence

$$b_{n+1} = a'_{n+1} \psi . 2^{n+1} = 2 (a'_n \eta \psi . 2^n + a'_n . y \psi . 2^n)$$
$$= 2 (b_n \varphi \eta \psi + b_n x) .$$

Maintenant, comme φ est un isomorphisme l'application linéaire $\bar{\eta} = \varphi \eta \psi$ est une dérivation de $\mathcal{B}$ dont l'action sur les générateurs x et z est donnée par le calcul

$$x \bar{\eta} = y \eta \psi = y' \psi = \frac{1}{2} (x^2 + z) = \frac{1}{2} x \sigma \ ;$$
$$z \bar{\eta} = (2 y' - y^2) \eta \psi = (2 y y' - y y' - y' y) \psi$$
$$= (y y' - y' y) \psi = x \frac{1}{2} (x^2 + z) - \frac{1}{2} (x^2 + z) x$$
$$= \frac{1}{2} (x z - z x) .$$

Ceci permet d'écrire $\bar{\eta} = \frac{1}{2} (\sigma + \rho)$ où ρ est la dérivation envoyant x sur 0 et z sur $x z - z x$, et nous avons donc $b_{n+1} = b_n \sigma + b_n \rho + 2 b_n x$.

Il suffit désormais de montrer que pour tout monôme u en x et z on a identiquement $u \rho + 2 u x = x u + u x$. Or ceci est trivial quand $u = x^n$ puisque $x^n \rho = 0$ et $x^n x = \frac{1}{2} (x x^n + x^n x)$.

Supposons donc ce résultat établi pour le monome v et prenons $u = v z x^n$. On a :

$$u\,\rho + 2\,u\,x = v\,\rho\,.\,z\,x^n + v\,(x\,z - z\,x)\,x^n + 2\,v\,z\,x^{n+1}$$
$$= x\,v\,z\,x^n - v\,x\,z\,x^n + v\,x\,z\,x^n - v\,z\,x^{n+1} + 2\,v\,z\,x^{n+1}$$
$$= x\,u + u\,x \qquad \text{Q.E.D.}$$

Dans ce qui suit nous nous bornerons au calcul des polynômes $b_n = 1\,\lambda^n$ dont les premiers sont

$b_o = 1$; $b_1 = b_o\lambda = x1 + 1\,x = 2\,x$;
$b_2 = 2\,x\,\lambda = 2\,(x^2 + z) + x\,.\,2\,x + 2\,x\,.\,x = 6\,x^2 + 2\,z$;
$b_3 = 24\,x^3 + 8\,(x\,z + z\,x)$;
$b_4 = 120\,x^4 + 40\,(x^2\,z + x\,z + z\,x^2) + 16\,z^2$;

Notre résultat principal est résumé par les formules 17 et 22 ci-dessous. Notant M le monoïde libre engendré par $\{x, z\}$, c'est à dire l'ensemble des monômes en x et z nous écrirons chaque polynôme b de B comme une somme finie $\Sigma\,\{\langle b, m\rangle\, m : m \in M\}$ dont les coefficients $\langle b, m\rangle$ appartiennent à $\mathcal{A}$. L'application $\langle\,,\,\rangle$ sera étendue de façon naturelle à une application bilinéaire de $\mathcal{B} \times \mathcal{B}$ dans $\mathcal{A}$.

Le degré $|m|$ d'un mot $m \in M$ sera par définition $|m|_x + 2\,|m|_z$ où, comme d'usage, $|m|_x$ (resp. $|m|_z$) dénote le nombre d'occurence de x (resp. z) dans m .

On vérifie sans difficulté que chacun des termes d'un polynôme $m\,\lambda$ $(m \in M)$ est de degré $|m| + 1$.

Comme $b_o = 1$ est homogène de degré zéro, il en résulte que chaque $b_n = 1\,\lambda^n$ est homogène de degré n . Ceci entraine en particulier que chaque mot m ait le même coefficient dans $b_{|m|}$ et dans la série formelle $B = \sum_{o\le n} b_n$. Ceci nous permettra d'utiliser la notation $\langle B, m\rangle$ au lieu de $\langle b_{|m|}, m\rangle$.

III. CALCUL DES POLYNOMES b_n

III.1. Nous désignerons par μ la transposée de $\lambda\dagger$ de λ, c'est à dire l'application linéaire de $\mathcal{P}$ telle que pour chaque paire $m, m' \in M$ le coefficient de m dans $m'\mu$ soit égal au coefficient de m' dans $m\lambda$. On vérifie facilement que chaque $m'\mu$ est un polynôme. Par définition on a la formule

(12) $b\lambda = \Sigma \langle b, m\mu\rangle m$

pour tout polynôme (ou série formelle) b. En particulier
(13) $\langle B, m\rangle = \langle b, m\mu\rangle$ identiquement.

Comme λ est rationnelle au sens de Eilenberg, un théorème de cet auteur que nous nous bornerons à appliquer donne une technique générale pour calculer M. Pour cela nous écrivons $\sigma = \sigma_x + \sigma_z$ où σ_x est la dérivation envoyant x sur x^2 et σ_z la dérivation envoyant x sur z, les noyaux de ces deux dérivations étant les polynômes qui ne contiennent pas la variable x. La transposée μ de λ est la somme des transposées des applications linéaires σ_x, σ_z, $m \longrightarrow m\,x$ et $m \longrightarrow x\,m$.

En ce qui concerne ces deux dernières, ce sont les applications $m \longrightarrow m\,x^{-1}$ et $m \longrightarrow x^{-1}\,m$ où, comme d'usage, la notation $m\,x^{-1}$ (resp. $x^{-1}\,m$) désigne le monome m' tel que $m'\,x = m$ (resp. $x\,m' = m$) s'il en éxiste un et 0 autrement. En ce qui concerne $\sigma_z\dagger$ c'est l'application envoyant chaque $m \in M$ sur la somme des produits $m_1\,x\,m_2$ où $m_1, m_2 \in M$ satisfont $m_1\,z\,m_2 = m$.

Enfin $m\,\sigma_x\dagger$ est la somme des monômes $m_1\,x\,m_2$ étendue à toutes les paires $m_1, m_2 \in M$ telles que $m_1\,x\,x\,m_2 = m$.
On voit sans peine que $x^{-1}\,m + m\,x^{-1} + m\,\sigma_z\dagger$ a tous ses coefficients 0 ou 1 et qu'aucun mot du support de $m\,\sigma_z\dagger$ (c'est à

dire de l'ensemble des mots ayant un coefficient non nul dans ce polynôme) n'appartient au support de m $m\,\sigma_x^{-1}$.

Par contre, si $m = m_1 x^n m_2$ où $n \geq 2$ et où les mots m_1 et m_2 satisfont la condition $m_1 \notin M_x$, $m_2 \notin x M$ (c'est à dire, pour abréger si x^n est un x^* – facteur maximal de m), le mot $m' = m_1 x^{n-1} m_2$ apparait dans $m\,\sigma_x \dagger$ avec la multiplicité $n-2$. Si en outre $m_1 = 1$, le même mot m' apparait dans $x^{-1} m$ ce qui fait que son coefficient dans $m\mu$ devient $n-1$. La même remarque vaut quand $m_2 = 1$.

A titre d'application nous calculons

(14) Pour chaque $n \in \mathbb{N}$, le coefficient $< B, x^n >$ est égal à $(n + 1)!$.

Preuve : Ceci est vrai pour $n = 0$, puisque $b_o = 1 = (0 + 1)!$. Soit donc n positif. On a $x^n \sigma_z \dagger = 0$ et par conséquent

$$x^n \mu = x^n \sigma_x \dagger + x^{-1} x^n + x^n x^{-1} = (n-1)\, x^{n-1} + x^{n-1} + x^{n-1}$$
$$= (n + 1)\, x^{n-1} \; .$$

Comme $< B, x^n > \; = \; < B, x^n \mu >$ d'après (13) le résultat en découle par induction. Q.E.D.

Nous établissons maintenant un énoncé technique essentiel pour la suite. Pour abréger nous notons $\mathcal{M}$ la relation dans $M \times M$ telle que $(m', m) \in \mathcal{M}$ ssi m appartient au support de $m'\,\sigma_x + x\,m' + m'\,\bar{x}$ et nous étendons $\mathcal{M}$ à une relation $\overline{\mathcal{M}}$ dans $\mathcal{B} \times \mathcal{B}$ en posant $(b', b) \in \overline{\mathcal{M}}$ ssi il existe une bijection α entre les supports des polynômes b' et b telle que pour tout monôme m' ou ait d'une part $(m', m'\alpha) \in \mathcal{M}$ et d'autre part $< b', m' > \; = \; < b, m'\alpha >$.

Propriété 15 : Soient $(m', m) \in \mathcal{M}$. On a $(m'\mu, m\mu - m') \in \overline{\mathcal{M}}$

Preuve : La vérification que $(m'\sigma_z\dagger, m\sigma_z\dagger) \in \overline{\mathcal{M}}$ est facile. Pour le reste, nous distinguons trois cas, et comme le résultat résulte immédiatement de (14) quand m et m' sont des puissances de x nous pouvons supposer que $|m|_z$ est positif.

Cas i : $m = x\, m'$.
Nous pouvons écrire $m' = x^n z\, m''$ $(n \in \mathbb{N},\ m'' \in M)$ et comme $m' = x^{-1} m$ il nous suffira de vérifier d'une part $(m' x^{-1}, m\, x^{-1}) \in \overline{\mathcal{M}}$ ce qui est trivial et d'autre part $(m'\sigma_x\dagger + x^{-1} m', m\sigma_x\dagger) \in \mathcal{M}$.

Soit S l'ensemble des paires (m_1, m_2) telles que $m_1\, x\, x\, m_2 = m$. Le sous ensemble S_1 de celles pour lesquelles $|m_1|_z$ est positif, est en correspondance biunivoque par $m_1 \longrightarrow x^{-1} m_1$ avec l'ensemble correspondant pour m'. En outre l'ensemble $S \setminus S_1$ est formé de n paires $(x^i, x^{n-i-1} z\, m'')$ $(o \le i \le n-1)$ ce qui fait que $x^n z\, m''$ a le coefficient n dans $m\sigma_x\dagger$.

On peut donc se limiter au cas de n positif et on vérifie de même que $x^{n-1} z\, m''$ a le coefficient $(n-1) + 1$ dans $m'\sigma_x\dagger + x^{-1} m'$ ce qui établit le résultat dans ce cas.

Cas ii : $m = m'\, x$.
Le même raisonnement s'applique par symétrie.

Cas iii : $m \neq m'\, x,\ x\, m'$.
On peut écrire $m' = m''\, z\, x^n\, z\, m'''$ où z est positif et l'on a $m = m''\, z\, x^{n+1}\, z\, m'''$. Il est clair que $(x^{-1} m' + m' x^{-1}, x^{-1} m + m x^{-1})$ est dans $\overline{\mathcal{M}}$. Comme ci-dessus le sous ensemble $S_1 \subset S$ des paires (m_1, m_2) telles que $m_1\, x\, x\, m_2 = m$ qui satisfont la condition supplémentaire que $|m_1|_z \neq |m''|_z$ est en correspondance biunivoque avec le sous ensemble correspondant pour m'. En ce

qui concerne les autres paires elles produisent le mot m' avec la multiplicité n et par conséquent le coefficient de m' dans $m\,\sigma_x\dagger - m'$ est $n-1$. Le mot correspondant $m''\,z\,x^{n-1}\,z\,m''$ a le coefficient $n-1$ dans $m'\,\sigma_x\dagger$ et le résultat est donc établi dans tous les cas. Q.E.D.

(16) <u>Corollaire</u> : Soit $(m', m) \in \mathcal{M}$. On a
$< B, m > \; = \; < B, m' > . \; (|m| + 1)$.

<u>Preuve</u> : Si $|m| = 1$, on a $m = x$ et il existe un seul m' , à savoir 1 tel que $(m', m) \in \mathcal{M}$. Comme $< B, x > = 2$ ainsi qu'on l'a vu dans (14), la formule vérifiée dans ce cas et nous pouvons procéder par induction sur le degré de m .
D'après (13) nous avons
$< B, m> \; = \; < B, m\mu >$ et $< B, m' > \; = \; < B, m'\mu >$.

De plus d'après (15) $m\,\mu$ est la somme de m' et d'un polynôme b tel que $(m'\mu, b) \in \mathcal{M}$. Comme b est homogène de degré $|m|-1$, il en résulte par l'hypothèse d'induction que
$< B, b > \; = \; < B, m'\mu > . \; |m|$. Par conséquent
$< B, m > \; = \; < B, m' > + < B, m'\mu > |m|$ où
$< B, m'> \; = \; < B, m'\mu >$ ce qui est le résultat cherché. Q.E.D.

Considérons maintenant un mot quelconque $m \in M$. On peut l'écrire sous la forme

$$m = x^{n_o}\, z^{p_1}\, x^{1+n_1}\, z^{p_2} \ldots x^{1+n_{k-1}}\, z^{p_k}\, x^{n_k}$$

où les p_i sont positifs et où k et les n_i sont non négatifs.

Désignons par $\hat{m}$ le mot $z^{p_1}\, x\, z^{p_2} \ldots x\, z^{p_k}$ (et par conséquent $\hat{m} = 1$ ssi $m = x^{n_o}$).

(17) Pour tout $m \in M$, on a $< B, m > \; = \; < B, \hat{m}> \dfrac{(1 + |m|)!}{(1 + |\hat{m}|)!}$

Preuve : Par induction sur $|m| - |\hat{m}|$ en observant que si $m \neq \hat{m}$, il existe au moins un m_1 tel que $(m_1, m) \in \mathcal{M}$ et que pour tout m_i satisfaisant cette dernière relation on a $\hat{m}_i = \hat{m}$.

Q.E.D.

(18) Quelques soient l'entier n et le polynome homogène a on a
$$< B, a x^n > = < B, a > \frac{(|a| + n + 1)!}{(|a| + 1)!} = < B, x^n a > .$$

Preuve : Ceci résulte immédiatement de (17) et de ce que $\hat{m}_1 = \hat{m}$ pour chaque m_1 de la forme $m x^n$ ou $x^n m$. Q.E.D.

III.2. Le résultat principal

Définissons d'abord une suite infinie de nombres rationnels (d_k) par la récurrence

(20) $d_o = 1$; $d_{k+1} = (2k + 3)^{-1} \sum_{o \leq j \leq k} d_j \, d_{k-j}$.

Nous vérifions d'abord

(21) pour chaque entier positif k et chaque mot $g \in \{1\} \cup M x$ on a $< B, g z^k > = < B, g x^{2k} > d_k$.

Preuve : Le résultat est facilement vérifié pour $|g z^k| \leq 2$ et nous pouvons procéder par induction sur le degré.

Considérons d'abord le cas de $g = 1$. On a
$$z^{k+1} \mu = z^{k+1} \sigma_z{}^{\dagger} = \sum_{o \leq j \leq k} z^{k-j} x z^j .$$

D'après l'hypothèse d'induction et (17) on a
$$< B, z^{k-j} x z^j > = < B, z^{k-j} x^{2j+1} > d_j$$
$$= < B, z^{j-j} > d_j \frac{(2k + 2)!}{(2k - 2j + 1)!}$$
$$= < B, x^{2k-2j} > d_j \frac{(2k + 2)!}{(2k - 2j + 1)!}$$

$= d_{k-j} \cdot d_j \, (2k + 2) = (2k + 3)^{-1} < B,\ x^{2k+2} > .$

Par conséquent nous avons bien

$$< B,\ z^{k+1} > = <B,\ x^{2k+2}> . (2k + 3)^{-1} \sum_{o \leq j \leq k} d_j \, d_{k-j} \ .$$

Supposons maintenant que g soit différent de 1, c'est à dire que $g = f x$ $(f \in M)$. On vérifie facilement que $g\, z^{k+1}\, \mu$ est la somme de $b = g\, (z^{k+1}\, \mu)$ et d'un autre polynôme c qui est égal à z^{k+1} si $f = 1$ et à $(f\, \mu)\, x\, z^{k+1}$ si $f \neq 1$.

D'après l'hypothèse d'induction, on trouve que

$$b = < B,\ g\, x^{2k+1} > \sum_{o \leq j \leq k} d_j \, d_{k-j}$$

$$= < B,\ g\, x^{2k+1} > (2k + 3)\, d_{k+1} \quad ;$$

D'autre part $c = d_{k+1}$ si $f = 1$ et sinon, utilisant l'hypothèse d'induction et (17), on trouve

$$c = < B,\ g\, x^{2k+1} > (\,|f| + 1)\, d_{k+1} \quad .$$

Par conséquent dans tous les cas

$$< B,\ g\, z^{k+1} > = < B,\ b > + < B,\ c >$$

$$= < B,\ g\, x^{2k+1} > \ (|g| + 2k + 3)\, d_{k+1}$$

ce qui est bien égal à $< B,\ g\, x^{2k+2} > d_{k+1}$. Q.E.D.

Nous sommes maintenant à même d'énoncer notre résultat principal :

(22) Si $m = x^{n_o}\, z^{p_1}\, x^{n+n_1} \ldots z^{p_k}\, x^{n_k}$

$(p_1,\ p_2,\ \ldots,\ p_k \geq 1\ )$ on a

$< B,\ m > = (1 + |m|.\,)!\, d_{p_1}\ ,\ d_{p_2} \ldots d_{p_k}$

<u>Preuve</u> : Pour $k = 0$ ceci est la formule (14). Le cas général s'en déduit par induction sur k au moyen de (22) et (17) . Q.E.D.

On notera que comme tous les coefficients intervenant dans λ sont des entiers non négatifs, il en est de même des coefficients $< B, m >$ des polynômes $b_n = 1\ \lambda^n$ ($n \in \mathbb{N}$) bien que les d_k soient des nombres fractionnaires.

III.3. Relations avec les nombres d'Euler.

Soit Y_o la solution de $y'' = y\, y'$ telle que $Y_o = 0$ pour $t = 0$. Elle est obtenue en faisant $y = 0$ dans les polynômes a_n décrits dans la première section de ce chapitre. Nous noterons a_{on} ces polynômes qui sont donc des polynômes en y'.

En particulier $a_{oo} = 0$ et $a_{o1} = y'$.

Rappelant la formule $a_{n+1} = b_n\ \varphi\ .\ y'\ 2^{-n}$ utilisée pour définir les polynômes b_n au moyen du morphisme φ envoyant x sur y et z sur $-y^2 + 2y'$, nous aurons $a_{o,n+1} = b_{on}\ \varphi\ .\ y'\ 2^{-n}$ où $b_{o,n}$ est le polynôme obtenu en faisant $x = 0$ dans b_n. Comme b_n est homogène de degré n et que les degrés de x et z sont respectivement 1 et 2 nous savons que b_{on} est nul pour n impair et qu'il se réduit à $< B, z^k > z^k$ pour $n = 2k$ ($k \in \mathbb{N}$).

De plus, d'après (22) et (17) nous savons que $< B, z^k>$ est égal à $(2k + 1)!\ d_k$.

Il en résulte que $a_{o,n} = 0$ pour n pair et que pour $n = 2k + 1$ on a $a_{o,2k+1} = 2^{-k}\ (2k + 1)!\ d_k\ y'^{k+1}$ et

$$Y_o = \sum_{o \leq k} \frac{t^{2k+1}}{(2k+1)!}\ a_{o,2k+1} \quad .$$

Faisons maintenant $y' = 1$ dans Y_o. La série obtenue est la solution de l'équation différentielle (ordinaire) $y'' = y\, y'$

qui, pour $t = 0$, prend la valeur 0 cependant que sa dérivée prend la valeur 1, c'est à dire comme il est bien connu, la fonction $\mathrm{tg}\,(t)$. Les nombres $2^{-k}\,(2k+1)!\,d_k$ en sont les coefficients de Hurwitz; ce sont donc les nombres d'Euler d'indice impair.

IV. UNE AUTRE APPLICATION

IV.1. Nous commençons par un complément aux généralités de I. Considérons un anneau de polynomes (non commutatifs) $\mathcal{A}[u, v, w, \ldots]$ en les variables $u, v, w, \ldots,$ son quotient $\mathcal{C}$ par la congruence $u\,v \equiv v\,u \equiv 1$ et une dérivation ζ telle que :

(23) $v\,\zeta = -\,v\,(u\,\zeta)\,v$.

<u>Remarque</u> : ζ est une dérivation de $\mathcal{C}$.

<u>Preuve</u> : Il suffit de montrer que pour tout $a, b \in \mathcal{A}[u, v, \ldots]$ on a $a\,u\,v\,b\,\zeta \equiv a\,v\,u\,b\,\zeta \equiv a\,b\,\zeta$.

Calculons $a\,u\,v\,b\,\zeta$. On a

$a\,u\,v\,b\,\zeta = (a\,\zeta)\,u\,v\,b + a\,u\,v\,(b\,\zeta) + a\,(u\,\zeta)\,v\,b + a\,u\,(v\,\zeta)\,b$.

La somme des deux premiers termes est congrue à $(a\,\zeta)\,b + a\,(b\zeta)$ c'est à dire à $a\,b\,\zeta$. La somme des deux derniers termes est congrue à 0 puisque

$a\,u\,(v\,\zeta)\,b = -\,a\,u\,v\,(u\,\zeta)\,v\,b \equiv -\,a\,(u\,\zeta)\,b\,v$.

Un calcul analogue vaut pour $a\,v\,u\,b\,\zeta$. Q.E.D.

Il résulte de ceci que $(u\,v)\,\zeta = (v\,u)\,\zeta = 1\,\zeta = 0$, donc que $(u\,v)\,\zeta^n = (v\,u)\,\zeta^n = 0$ pour tout n positif. Or, comme ζ est une dérivation, on a identiquement

$(a\,b)\,\zeta^n = \sum\limits_{o \le j \le n} (a\,\zeta^j)\,(b\,\zeta^{n-j}) \begin{bmatrix} n \\ j \end{bmatrix}$ quelque soient a, b et $n \geq 0$.

Divisant par $n!$ on en déduit l'identité

(24) $$\sum_{o\le j\le n} \frac{u\,\zeta^j}{j!} \cdot \frac{v\,\zeta^{n-j}}{(n-j)!} = 0 \quad \text{pour chaque } n \text{ positif.}$$

Introduisant une nouvelle variable t commutant avec u et v et posant

$$U = \sum_{o\le n} \frac{t^n}{n!} \cdot u\,\zeta^n \quad ; \quad V = \sum_{o\le n} \frac{t^n}{n!} \cdot v\,\zeta^n$$

il en résulte finalement la relation

(25) $U\,V = V\,U = 1$

par identification des coefficients de t^n et (24) .

IV.2. Nous revenons aux notations de II.1. et nous adjoignons à $\bar{\mathcal{A}}(t)$ une nouvelle variable v satisfaisant $y'\,v = v\,y' = 1$ (ce qui entraine $v\,t = t\,v$ puisque $t\,y' = y'\,t$)

En conformité avec (23), nous étendons la dérivation η (définie par $y\,\eta = y'$, $y'\,\eta = y\,y'$) en posant $v\,\eta = -\,v\,(y'\,\eta)\,v$ ce qui donne $v\,\eta = -\,v\,y\,y'\,v = -\,v\,y$.

D'après (25) les deux séries formelles

$$Y' = \sum_{o\le n} \frac{t^n}{n!}\,(y'\,\eta^n) \qquad \text{et} \qquad V = \sum_{o\le n} \frac{t^n}{n!}\,(v\,\eta^n)$$

sont inverses l'une de l'autre et nous proposons de calculer directement les coefficients $v\,\eta^n$ de V .

Remarque 26 : Pour chaque $n \in \mathbb{N}$ on a

$$2\,v\,\eta^n = v\,(C_n\,\varphi)$$

où les C_n sont des polynomes dans $\overline{\mathcal{B}}$ définis par la récurrence

$$C_o = 2 \quad ; \quad C_{n+1} = \frac{1}{2}\,(C_n\,\sigma - x\,C_n - C_n\,x) = C_n\,\nu.$$

Preuve : C'est essentiellement la même que celle de la remarque 11 dont nous utilisons les notations.

Nous avons $v\,\eta^0 = v$ et par conséquent nous pouvons prendre $C_0 = 2 \in \bar{\mathcal{B}}$

Supposons maintenant que $2\,v\,\eta^n = v\,(C_n\,\varphi)$ où $C_n \in \bar{\mathcal{B}}$.

Nous avons :

$$\begin{aligned} 2\,v\,\eta^{n+1} &= (v\,(C_n\,\varphi))\,\eta = v\,\eta\,.\,(C_n\,\varphi) + v\,(C_n\,\varphi\,\eta) \\ &= -\,v\,y\,(C_n\,\varphi) + v\,(C_n\,\varphi\,\psi\,\bar{\eta}\,\varphi\,) \\ &= -\,v\,x\,\varphi\,(C_n\,\varphi) + v\,(C_n\,\bar{\eta}\,\varphi)\;. \end{aligned}$$

Mettant v en facteur nous obtenons donc $2\,v\,\eta^{n+1} = v\,C_{n+1}$ où $C_{n+1} = -\,x\,C_n + C_n\,\bar{\eta}$ appartient à $\bar{\mathcal{B}}$ par induction.

Il ne reste plus qu'à vérifier que cette équation peut se mettre sous la forme plus simple

$$C_{n+1} = \frac{1}{2}\,(C_n\,\sigma\, - x\,C_n - C_n\,x) = C_n\,\nu$$

ce qui est facile compte tenu de $\bar{\eta} = \sigma + \rho$ et des propriétés de ρ établies dans la preuve de la remarque 11; Q.E.D.

On trouve pour les premiers termes

$C_0 = 2$; $C_1 = -\,2\,x$; $C_2 = x^2 - z$; $C_3 = x\,z + z\,x$;

On a les formules suivantes :

(27) $C_{2k} = (-1)^k\,(z^k - x\,z^{k-1}\,x)$ pour $k \geq 1$;

$C_{2k+1} = (-1)^{k+1}\,(x\,z^k + z^k\,x)$ pour $k \geq 0$.

<u>Preuve</u> : On vérifie directement que $C_1 = -\,2\,x$.

Supposant maintenant que C_{2k+1} a la forme (27), on trouve :

$$\begin{aligned} &2\,(-1)^{k+1}\,C_{2k+2} = 2\,(-1)^{k+1}\,C_{2k+1}\,\nu \\ &= (x^2 + z)\,z^k + z^k\,(x^2 + z) - x^2\,z^k - x\,z^k\,x - x\,z^k\,x - z^k\,x^2 \\ &= 2\,(z^{k+1} - x\,z^k\,x)\;. \end{aligned}$$

De même supposant que C_{2k} $(k \geq 1)$ a la forme (27) on obtient

$$2\,(-1)^k\, C_{2k+1} = 2\,(-1)^k\, C_{2k}\, \nu = -\,(x^2 + z)\, z^{k-1}\, x$$

$$-\, x\, z^{k-1}\,(x^2 + z) - x\, z^k + x^2\, z^{k-1}\, x - z^k x + x\, z^{k-1}\, x^2$$

$$= -\,2\,(x\, z^k + z^k\, x)\ .\qquad \text{Q.E.D.}$$

Posant $C = \sum_{o \leq n} t^n\, C_n$ les formules précédentes peuvent être résumées par la formule unique

(28) $C = 1 + (t - t\,x)\,(1 + t\,z)^{-1}\,(1 - t\,x)$

où, comme d'usage, $(1 + t\,z)^{-1}$ est une abréviation pour $\sum_{o \leq n} (-1)^n\, t^n\, z^n$ ce qui donnerait facilement l'expression de $\sum_{o \leq n} t^n\,(v\,\eta^n)$ en appliquant le morphisme φ . Il me parait très remarquable que cette dernière fonction se trouve ainsi être une <u>fonction rationnelle</u> en tous ses arguments.

IV.3. Nous terminons en montrant que la fonction V de t est la solution de l'équation différentielle

(29) $V'' = V'\, V^{-1}\, V' - 1$

où $V' = V\,\partial$, $V'' = V'\,\partial$

et où ∂ est la dérivation de noyau $\overline{\mathcal{P}}$ envoyant t sur 1 qui a été définie et utilisée dans le chapitre I .

Tout d'abord, nous avons par hypothèse $Y'' = Y\, Y'$ d'où $Y''' = Y\, Y'' + Y'^2$ ce qui donne $Y = Y''\, Y'^{-1}$ et $Y''' = Y''\, Y'^{-1} Y'' + Y'^2$

ce qui peut se réécrire

$$Y'^{-1}\, Y''' Y'^{-1} = Y'^{-1}\, Y''\, Y'^{-1}\, Y''\, Y'^{-1} + 1\ .$$

Maintenant d'après (25) nous avons $V = Y'^{-1}$ d'où d'après (23)

$V' = -\, V\, Y''\, V$ puis $V'' = -\, V'\, Y''\, V - V\, Y'''\, V - V\, Y''\, V'$

$= 2\, V\, Y''\, V\, Y''\, V - V\, Y'''\, V$ ce qui est égal à $V\, Y''\, V\, Y''\, V - 1$

d'après l'expression trouvée plus haut pour

$$Y'^{-1} \; Y''' \; Y'^{-1} = V \, Y''' \, V$$

et le résultat s'en déduit en utilisant la relation

$$V \, Y'' \, V = - V' \quad .$$

Q.E.D.

REFERENCES

[1] D. André. Developpements de Sec x et tang x . C.R. Acad. Sc. Paris 88 (1879) - 965 - 967 .

[2] S. Eilenberg. Theory of Automata. (Sous presse)

[3] D. Foata et M. P. Schützenberger. Nombres d'Euler et permutations alternantes. In a Survey of Combinatorial Theory (J. N. Stivastaver Ed) Amsterdam 1973 .

[4] N. Nielsen. Traite élementaire des nombres de Bernoulli. Paris 1923 .

[5] I. Riordan. Combinatorial Identities. N. Y. 1970 .

[6] Wedderburn. Lectures on Matrices. Am. Math. Soc. Colloq. Publi. 17 1934 .