THEORIE DE PICARD-VESSIOT DES SYSTEMES REGULIERS (OU BILINEAIRES)

Michel FLIESS
Laboratoire Des Signaux et Systèmes
C.N.R.S. - E.S.E.
Plateau du Moulon
91190 Gif-sur-Yvette

Christophe REUTENAUER
Laboratoire d'Informatique
Théorique et Programmation
Institut de Programmation
Université Paris VI
4, place Jussieu
75230 Paris Cedex 05

RÉSUMÉ Le comportement entrée-sortie d'un système régulier (ou bilinéaire) est, comme on le sait, décrit par une série génératrice non commutative rationnelle. Nous montrons d'abord que cette rationalité équivaut à une équation différentielle linéaire, à coefficients dépendant des entrées et de leurs dérivées, dont la sortie du système est solution. Interviennent alors le corps de rupture et le groupe de Galois différentiels de cette équation et, par définition, du système et de sa série génératrice. Ce groupe est un groupe algébrique connexe que nous pouvons caractériser simplement ainsi que son algèbre de Lie. Comme application, nous montrons que la résolubilité du groupe de Galois correspond au fait remarquable suivant : la sortie du système s'obtient par un nombre fini d'intégrations et d'exponentiations.

SUMMARY As we know, the input-output behaviour of a regular (or bilinear) system may be described by its non-commutative generating power series which is rational. We show first that this rationality is equivalent to a linear differential equation with coefficients depending of the inputs and their derivatives, the solution of which is the output of the system. This allows us to introduce the splitting field and the differential Galois group of the equation and, by definition, of the system and its generating series. This group is a connected algebraic group which we simply characterize, together with its Lie algebra. As an application we show that the solvability of the Galois group corresponds to the solvability of the system in the following sense : the output may be obtained by a finite number of integrations and exponentiations.

INTRODUCTION

L'origine de ce travail est double :

- Etant donné un système régulier (ou bilinéaire), il est, en général, assez pénible, pour des entrées non fixées une fois pour toute, de l'intégrer numériquement. Il apparaît donc nécessaire d'isoler des sous-classes, où cette intégration serait plus aisée.

- On connait, à travers la théorie des séries génératrices non commutatives, les liens entre systèmes réguliers et automates finis (cf. [9]). En 1965, Schützenberger [30] avait caractérisé les langages dits apériodiques ou

"star-free", qui sont reconnus par des automates finis particuliers, grâce à une propriété remarquable de leur monoïde syntaxique (voir aussi Eilenberg [6] et Lallement [21]). Récemment, l'un des auteurs [25] a montré qu'il y avait possibilité d'étendre ce résultat aux séries rationnelles non commutatives par une propriété de triangularisation de la représentation linéaire. Quel est alors le lien avec les systèmes réguliers ?

Le cadre naturel pour de telles questions semble être la théorie de Picard-Vessiot des équations différentielles linéaires, qui a pour but de généraliser la théorie de Galois des équations algébriques. A leur époque, Picard [24] et Vessiot [33] avaient pour seul outil la théorie locale des groupes de Lie, qui n'était pas vraiment adaptée au but poursuivi. Il a appartenu à Kolchin [19] de montrer qu'il fallait employer les groupes algébriques linéaires.

Après des rappels indispensables sur les séries rationnelles non commutatives et leur lien avec les systèmes réguliers, nous montrons comment intervient l'algèbre différentielle. Le premier résultat significatif prouve que toute série rationnelle non commutative ou, ce qui revient au même, toute sortie d'un système régulier vérifie une équation différentielle linéaire dont les coefficients dépendent des entrées et de leurs dérivées. On peut alors définir l'extension de Picard-Vessiot correspondante : c'est un corps différentiel qui joue le même rôle que le corps de rupture en théorie de Galois. Le groupe de Galois différentiel de cette extension est un groupe algébrique que nous appelons groupe de Galois de la série et de tout système régulier l'admettant par série génératrice. Ce groupe et son algèbre de Lie, l'algèbre de Lie galoisienne de la série et du système, reçoivent des caractérisations simples grâce aux notions de représentations linéaires réduites [8] et d'algèbre associative syntaxique [25]. Par l'intermédiaire d'un résultat de [25] auquel il a déjà été fait allusion, on peut alors généraliser le théorème célèbre de Vessiot en montrant que la résolubilité du groupe de Galois équivaut à obtenir la sortie du système régulier par intégrations et exponentiations. On conclut par deux exemples élémentaires.

PLAN

CHAPITRE I – RAPPELS SUR LES SYSTEMES REGULIERS ET LES SERIES GENERATRICES RATIONNELLES (*)

I. INTRODUCTION HEURISTIQUE DES INDETERMINEES NON COMMUTATIVES

Considérons le système régulier (ou bilinéaire)

$$\begin{cases} \dot{q}(t) = \left(A_o + \sum_{i=1}^{n} u_i(t) A_i\right) q(t) \\ y(t) = \lambda q(t) \end{cases}$$

(*) On trouvera des compléments dans les cours [17] et [27].

L'état q appartient à un $\mathbb{R}$-espace vectoriel Q de dimension finie ; l'état initial q(0) est donné. Les opérateurs $A_0, A_1, \ldots, A_n : Q \to Q$, $\lambda : Q \to \mathbb{R}$ sont $\mathbb{R}$-linéaires. Les entrées $u_1, \ldots, u_n : [0, \infty[\to \mathbb{R}$ sont, pour les nécessités de ce travail, supposées indéfiniment dérivables, c'est-à-dire C^∞.

La formule de Peano-Baker permet d'écrire la sortie y de (1) sous forme de la série suivante :

$$y(t) = \lambda\left[1 + \sum_{\nu \geq 0} \sum_{j_0, \ldots, j_\nu = 0}^{n} A_{j_\nu} \ldots A_{j_0} \int_0^t d\xi_{j_\nu} \ldots d\xi_{j_0}\right] q(0) \qquad (2)$$

L'intégrale itérée $\int_0^t d\xi_{j_\nu} \ldots d\xi_{j_0}$ est définie par récurrence sur la longueur :

$$\xi_0(\tau) = \tau, \quad \xi_i(\tau) = \int_0^\tau u_i(\sigma)d\sigma \quad (i=1,\ldots,n), \quad \int_0^t d\xi_j = \xi_j(t) \quad (j=0,\ldots,n)$$

$$\int_0^t d\xi_{j_\nu} \ldots d\xi_{j_0} = \int_0^t d\xi_{j_\nu}(\tau) \int_0^\tau d\xi_{j_{\nu-1}} \ldots d\xi_{j_0},$$ où la dernière intégrale est de Stieltjes.

Introduisons l'ensemble $X = \{x_0, x_1, \ldots, x_n\}$ d'indéterminées non commutatives. En (2), remplaçons l'intégrale itérée $\int_0^t d\xi_{j_\nu} \ldots d\xi_{j_0}$ par la suite correspondante $x_{j_\nu} \ldots x_{j_0}$ de symboles. On obtient la série *génératrice*

$$\underline{g} = \lambda q(0) + \sum_{\nu \geq 0} \sum_{j_0, \ldots, j_\nu = 0}^{n} \lambda A_{j_\nu} \ldots A_{j_0} q(0) x_{j_\nu} \ldots x_{j_0} \qquad (3)$$

qui caractérise le comportement entrée-sortie de (1).

II. RATIONALITE NON COMMUTATIVE

a) Définition

On note X^* le monoïde libre engendré par X. Un élément de X^* est un mot, c'est-à-dire une suite finie $x_{j_\nu} \ldots x_{j_0}$ de symboles. Le produit est la concaténation :

$$(x_{j_\nu} \ldots x_{j_0})(x_{k_\mu} \ldots x_{k_0}) = x_{j_\nu} \ldots x_{j_0} x_{k_\mu} \ldots x_{k_0}$$

L'élément neutre, noté 1, est le mot vide.

Soient $\mathbb{R}\langle X\rangle$ et $\mathbb{R}\langle\langle X\rangle\rangle$ les $\mathbb{R}$-algèbres des polynômes et des séries formels, à coefficients réels, en les indéterminées non commutatives $x_j \in X$. Un élément $s \in \mathbb{R}\langle\langle X\rangle\rangle$ est noté :

$$s = \sum \{(s,w)\ w \mid w \in X^*\} \quad \text{où } (s,w) \in \mathbb{R} \tag{4}$$

Addition et produit (de Cauchy) sont définis par

$$s_1 + s_2 = \sum \{[(s_1,w) + (s_2,w)]w \mid w \in X^*\} ,$$

$$s_1 s_2 = \sum \{[\sum_{w_1 w_2 = w} (s_1,w_1)(s_2,w_2)]w \mid w \in X^*\}$$

Une série $s \in \mathbb{R}\langle\langle X\rangle\rangle$ est inversible si, et seulement si, son terme constant $(s,1)$ est non nul. Une sous-algèbre R de $\mathbb{R}\langle\langle X\rangle\rangle$ est rationnellement close si, et seulement si, l'inverse de toute série inversible de R appartient encore à R. La R-algèbre $\mathbb{R}\langle(X)\rangle$ des séries *rationnelles* est la plus petite sous-algèbre rationnellement close de $\mathbb{R}\langle\langle X\rangle\rangle$, qui contienne $\mathbb{R}\langle X\rangle$ (Schützenberger [29]).

Q désignant un $\mathbb{R}$-espace vectoriel, une représentation (linéaire) $\mu : X^* \to \mathrm{End}(Q)$ est un morphisme du monoïde X^* dans le monoïde multiplicatif $\mathrm{End}(Q)$ des endomorphismes $\mathbb{R}$-linéaires de Q. Le théorème suivant, dit de Kleene-Schützenberger, donne une caractérisation remarquable de la rationalité.

Théorème I.1. Une série $r \in \mathbb{R}\langle\langle X\rangle\rangle$ est rationnelle si, et seulement si, il existe un $\mathbb{R}$-espace vectoriel Q de dimension finie, des éléments $\gamma \in Q$, $\lambda \in {}^tQ$ (*) tels que

$$r = \sum \{(\lambda \mu w \gamma) w \mid w \in X^*\} \tag{5}$$

Le formule (3) montre alors qu'un système régulier est caractérisé par la rationalité de sa série génératrice.

b) Matrice de Hankel et réalisation (cf. [8])

A la série (4), on associe le tableau infini $\mathscr{H}(s)$, la matrice de Hankel de s, dont lignes et colonnes sont indexées par les mots de X^* :

(*) ${}^tQ$ désigne le dual de Q.

l'élément d'indice $(u,v) \in X^* \times X^*$ est le coefficient (s,uv). On montre que $\mathscr{H}(s)$ est de rang fini si, et seulement si, s est rationnelle.

Si la matrice de Hankel est de rang fini, on peut prendre, dans l'énoncé du théorème I.1, l'espace Q de dimension N. La représentation correspondante (λ,μ,γ) est de dimension N ; elle est dite *réduite* ou *minimale*, car c'est la plus petite dimension possible. Toute autre représentation de dimension N est semblable. La théorie de la réalisation des systèmes réguliers (I) en découle immédiatement.

A tout mot $w \in X^*$ associons les séries

$$\underline{\underline{g}}\circ w = \sum_{v\in X^*} (\underline{\underline{g}},wv)v, \qquad w\circ\underline{\underline{g}} = \sum_{v\in X^*} (\underline{\underline{g}},vw)v$$

Si $p = \sum \alpha_w w$ est un polynôme de $\mathbb{R}\langle X\rangle$, on pose, par linéarité,

$$\underline{\underline{g}}\circ p = \sum_{w\in X^*} \alpha_w \underline{\underline{g}}\circ w, \qquad p\circ\underline{\underline{g}} = \sum_{w\in X^*} \alpha_w w\circ\underline{\underline{g}}$$

Les ensembles $\left\{\underline{\underline{g}}\circ p \mid p \in \mathbb{R}\langle X\rangle\right\}$ et $\left\{p\circ\underline{\underline{g}} \mid p \in \mathbb{R}\langle X\rangle\right\}$ sont des $\mathbb{R}$-espaces vectoriels Λ et Γ, canoniquement isomorphes aux $\mathbb{R}$-espaces vectoriels engendrés par les lignes et les colonnes de $\mathscr{H}(g)$. Aussi peut-on énoncer :

Proposition I.2. $\underline{\underline{g}}$ est rationnelle si, et seulement si, Λ (resp. Γ) est de dimension finie. Cette dimension est égale au rang de $\mathscr{H}(\underline{\underline{g}})$.

III. PRODUIT ET MELANGE

La formule d'intégration par parties montre que l'on peut écrire le produit de deux intégrales itérées de la manière suivante

$$\left(\int_0^t d\xi_{j_\nu}\ldots d\xi_{j_0}\right)\left(\int_0^t d\xi_{k_\mu}\ldots d\xi_{k_0}\right) = \int_0^t d\xi_{j_\nu}(\tau)\left[\left(\int_0^\tau d\xi_{j_{\nu-1}}\ldots d\xi_{j_0}\right)\right.$$
$$\left.\times\left(\int_0^\tau d\xi_{k_\mu}\ldots d\xi_{k_0}\right)\right] + \int_0^t d\xi_{k_\mu}(\tau)\left[\left(\int_0^\tau d\xi_{j_\nu}\ldots d\xi_{j_0}\right)\left(\int_0^\tau d\xi_{k_{\mu-1}}\ldots d\xi_{k_0}\right)\right] \tag{6}$$

Définissons alors le *mélange*(*), noté ⧢, par récurrence sur la longueur des

(*) On dit aussi *produit de Hurwitz*. En anglais, le terme consacré est *"shuffle product"*.

mots de X^* :

$$1 \sqcup\!\sqcup 1 = 1, \quad 1 \sqcup\!\sqcup x_j = x_j \sqcup\!\sqcup 1 = x_j \quad (j = 0,\ldots,n)$$

$$(x_j w) \sqcup\!\sqcup (x_{j'} w') = x_j\left[w \sqcup\!\sqcup (x_{j'} w')\right] + x_{j'}\left[(x_j w) \sqcup\!\sqcup w'\right] \qquad (7)$$

Le produit de deux mots de X^* est donc un polynôme de $\mathbb{R}\langle X\rangle$, qui est homogène, de degré égal à la somme des longueurs des mots. On constate que les formules (6) et (7) se correspondent et donc que le mélange est l'opération algébrique qui traduit le produit (cf. [10]).

Par linéarité, le mélange s'étend aux séries de $\mathbb{R}\langle\langle X\rangle\rangle$:

$$s_1 \sqcup\!\sqcup s_2 = \sum\left\{(s_1,w_1)(s_2,w_2) w_1 \sqcup\!\sqcup w_2 \,|\, w_1, w_2 \in X^*\right\}$$

Avec l'addition et le mélange, les ensembles $\mathbb{R}\langle X\rangle$ et $\mathbb{R}\langle\langle X\rangle\rangle$ des polynômes et des séries deviennent des $\mathbb{R}$-algèbres associatives, commutatives, intègres et unifères (l'élément neutre pour le mélange est 1).

Considérons alors deux séries rationnelles

$$s_k = \sum\left\{(\lambda_k \mu_k w \gamma_k) w \,|\, w \in X^*\right\}, \quad (k = 1,2),$$

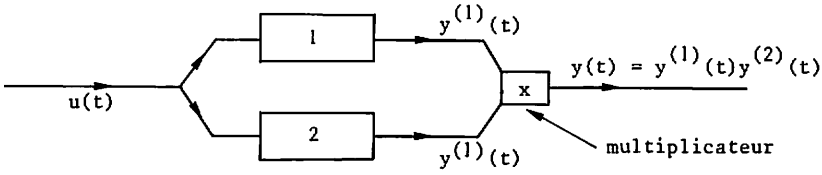
données, selon la formule (5), d'espaces vectoriels correspondants Q_k. Nous désirons prouver la rationalité de $s_1 \sqcup\!\sqcup s_2$. Pour le faire, posons $Q = Q_1 \otimes Q_2$ (où $\otimes$ désigne le produit tensoriel sur $\mathbb{R}$). La représentation $\mu : X^* \to Q$ est définie par $x_j \to \mu_1 x_j \otimes 1_2 + 1_1 \otimes \mu_2 x_j$ $(j = 0,\ldots,n)$, où $1_k \in \mathrm{End}(Q_k)$ désigne l'endomorphisme identité. Avec $\gamma = \gamma_1 \otimes \gamma_2$, $\lambda = \lambda_1 \otimes \lambda_2$ $s_1 \sqcup\!\sqcup s_2$ s'écrit comme en (5). On a montré (cf. [7]) :

Théorème I.3. Le mélange de deux séries rationnelles non commutatives est encore une série rationnelle.

Pour traduire cette propriété fondamentale dans le langage des systèmes réguliers, prenons deux tels systèmes, de mêmes entrées, donnés comme en (1) :

$$\begin{cases} \dot{q}^{(k)} = \left\{A_o^{(k)} + \sum_{i=0}^{n} u_i(t) A_i^{(k)}\right\} q^{(k)}(t) \\ y^{(k)} = \lambda^{(k)} q^{(k)}(t) \end{cases} \qquad (k = 1,2)$$

Le système ayant mêmes entrées que les précédents et pour sortie le produit des sorties, selon le schéma



peut d'après ce qui précède être encore mis sous la forme d'un système régulier (cf. [9]) :

$$\begin{cases} \dot{q}(t) = \left[A_o^{(1)} \otimes 1_2 + 1_1 \otimes A_o^{(2)} + \sum_{i=1}^{n} u_i(t)\left(A_i^{(1)}(t) \otimes 1_2 + 1_1 \otimes A_i^{(2)}(t)\right)\right] q(t) \\ y(t) = \lambda^{(1)} \otimes \lambda^{(2)}(t) q(t) \qquad\qquad q(0) = q^{(1)}(0) \otimes q^{(2)}(0) \end{cases}$$

CHAPITRE II - INTRODUCTION DE L'ALGEBRE DIFFERENTIELLE

I. GENERALITES

a) Présentation heuristique

L'algèbre différentielle reprend, *grosso modo* , l'étude des structures de l'algèbre commutative en y ajoutant des opérations de dérivations obéissant aux règles habituelles : $D(ab) = D(a)b + aD(b)$, où D est une dérivation. C'est avant tout la création du mathématicien américain Ritt [28]. Le livre de Kolchin [20] en donne un panorama très complet, peut-être difficile à déchiffrer. Il en existe une excellente introduction, due à Kaplansky [18], à laquelle il suffit de renvoyer pour nos besoins.

Regardons comment algèbre différentielle et séries génératrices s'interpénètrent. La dérivée par rapport au temps de l'intégrale itérée $\int_o^t d\xi_{j_\nu} \ldots d\xi_{j_o}$ est donné par :

$$\frac{d}{dt} \int_o^t d\xi_{j_\nu} \ldots d\xi_{j_o} = \begin{cases} \int_o^t d\xi_{j_{\nu-1}} \ldots d\xi_{j_o} & \text{si } j_\nu = 0 \\ u_{j_\nu}(t) \int_o^t d\xi_{j_{\nu-1}} \ldots d\xi_{j_o} & \text{sinon} \end{cases}$$

De même, la dérivée de la série Peano-Baker (2) est

$$\lambda\Big(A_o+\sum_{i=1}^{n} u_i(t)A_i\Big)\Big(1+\sum_{\nu\geq 0}\sum_{j_o,\ldots,j_\nu=0}^{n} A_{j_\nu}\ldots A_{j_o}\int_o^t d\xi_{j_\nu}\ldots d\xi_{j_o}\Big)q(0) \tag{8}$$

On voit qu'avec la dérivation on sort du domaine des intégrales itérées. Pour algébriser cela, commençons par introduire la $\mathbb{R}$-algèbre $\mathbb{R}\{u\}$ des polynômes différentiels en $u_1,\ldots,u_n$, c'est-à-dire des polynômes en les variables u_i $(i = 1,\ldots,n)$ et leurs dérivées successives $\dot{u}_i$, $\ddot{u}_i$,$\ldots$,$u_i^{(k)}$,$\ldots$ Soit $\mathbb{R}(\{u\})$ son corps de fractions. Formons la $\mathbb{R}$-algèbre commutative $\mathbb{R}(\{u\})\otimes \mathbb{R}\langle(X)\rangle$ produit tensoriel de $\mathbb{R}(\{u\})$ et de l'algèbre des séries rationnelles relativement au mélange. Un élément s'écrit :

$$\alpha = \sum_{\text{fini}} m\otimes r \qquad (m \in \mathbb{R}(\{u\}),\ r \in \mathbb{R}\langle(X)\rangle)$$

Remarquons que $\mathbb{R}(\{u\})$ et $\mathbb{R}\langle(X)\rangle$ s'injectent canoniquement dans $\mathbb{R}(\{u\})\otimes \mathbb{R}\langle(X)\rangle$.

Par définition, la dérivée de α est :

$$\dot{\alpha} = \sum \dot{m}\otimes r + m\otimes(r\circ x_o) + \sum_{i=1}^{n} mu_i\otimes(r\circ x_i)$$

En particulier, si $\underline{\underline{g}} \in \mathbb{R}\langle(X)\rangle$, il vient :

$$\dot{\underline{\underline{g}}} = \underline{\underline{g}}\circ x_i + \sum_{i=1}^{n} u_i\otimes \underline{\underline{g}}\circ x_i$$

On retrouve ainsi (8). Soit κ le corps de fractions de $\mathbb{R}\{u\}\otimes \mathbb{R}\langle(X)\rangle$, qui est aussi un corps différentiel qui va jouer un grand rôle par la suite.

Remarque : Dans $\mathbb{R}\langle\langle X\rangle\rangle$ considérée relativement au mélange, on vérifie immédiatement que, pour tout $x_j \in X$, les applications $s \to s\circ x_j$ et $s \to x_j\circ s$ sont des dérivations. En effet, on a :

$$(s \sqcup\!\sqcup s')\circ x_j = (s\circ x_j) \sqcup\!\sqcup s' + s \sqcup\!\sqcup (s'\circ x_j) \ ,$$

$$x_j\circ(s \sqcup\!\sqcup s') = (x_j\circ s) \sqcup\!\sqcup s' + s \sqcup\!\sqcup (x_j\circ s')$$

Les dérivations $s \to s\circ x_j$ et $s \to x_j\circ s$ sont respectivement notées R_{x_j} et L_{x_j}.

b) Constantes de κ

Dans un corps différentiel, une constante est un élément de dérivée nulle. L'ensemble des constantes est un sous-corps que, très souvent, il importe de déterminer. En [14], il a été prouvé ,

Lemme II.1. Le corps des constantes de κ est $\mathbb{R}$.

II. EQUATIONS DIFFERENTIELLES LINEAIRES

a) Propriété fondamentale (cf. [14])

Théorème II.2. Soit $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$ une série rationnelle dont la matrice de Hankel a pour rang N. Alors $\underline{g}, \dot{\underline{g}}, \ldots, \overset{(N-1)}{\underline{g}}$ sont $R(\{u\})$ -linéairement indépendants et g vérifie une équation différentielle de la forme :

$$\overset{(N)}{\underline{g}} + C_1 \otimes \overset{(N-1)}{\underline{g}} + \ldots + C_N \otimes \underline{g} = 0 \qquad (9)$$

où $C_1, \ldots, C_N$ appartiennent à $\mathbb{R}\{\{u\}\}$.

Démonstration. (i) Soit $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$ avec une matrice de Hankel de rang N. Supposons qu'elle vérifie la relation

$$B_1 \otimes \overset{(N-1)}{\underline{g}} + \ldots + B_N \otimes \underline{g} = 0 \qquad (10)$$

où $B_1, \ldots, B_N \in \mathbb{R}(\{u\})$. L'application $\mathbb{R}$-linéaire $\mathbb{R}\langle\langle X\rangle\rangle \to \mathbb{R}(X)$, $r \to p \circ r$ $(p \in \mathbb{R}\langle X\rangle)$ se prolonge en un endomorphisme $\mathbb{R}\{\{u\}\}$-linéaire de $\mathbb{R}(\{u\}) \otimes \mathbb{R}\langle\langle X\rangle\rangle$ par la formule

$$p \circ (\textstyle\sum m \otimes r) = \sum m \otimes (p \circ r)$$

et commute à la dérivation. Avec (10), il vient

$$B_1 \otimes (p \circ \overset{(N-1)}{\underline{g}}) + \ldots + B_N \otimes (p \circ \underline{g}) = 0 \ .$$

D'après la proposition I.2, il existe N séries $\mathbb{R}$-linéairement indépendantes de la forme $p \circ \underline{g}$ ce qui contredit le fait suivant, classique en algèbre différentielle (cf. Kaplansky [18]) :

Lemme II.3. Soit K un corps différentiel et k son corps des constantes. Alors l'équation différentielle

$$\alpha_o \eta^{(N)} + \ldots + \alpha_N \eta = 0 \qquad (\alpha_i \in K) \tag{11}$$

possède au plus N solutions k-linéairement indépendantes.

(ii) En vertu de la proposition I.2, la dimension du $\mathbb{R}$-espace vectoriel $\underset{=}{g}_o \mathbb{R}\langle X\rangle$ est N, de même que celle du $\mathbb{R}(\{u\})$-espace vectoriel

$$V = \mathbb{R}(\{u\}) \otimes (\underset{=}{g}_o \mathbb{R}\langle X\rangle)$$

V contient toutes les dérivées de $\underset{=}{g}$. Comme $\underset{=}{g}, \ldots, \underset{=}{g}^{(N-1)}$ sont $\mathbb{R}(\{u\})$-linéairement indépendants et constituent, ainsi, une base de V, $\underset{=}{g}^{(N)}$ s'exprime comme combinaison $\mathbb{R}(\{u\})$-linéaire de $\underset{=}{g}, \dot{\underset{=}{g}}, \ldots, \underset{=}{g}^{(N-1)}$.

Le théorème précédent a une traduction immédiate en terme de systèmes réguliers.

Théorème II.2.bis. La sortie y d'un système régulier dont la matrice de Hankel de la série génératrice a pour rang N satisfait à une équation différentielle linéaire d'ordre N

$$y^{(N)} + C_1 y^{(N-1)} + \ldots + C_N y = 0 \tag{9bis}$$

où $C_1, \ldots, C_N$ sont des fractions rationnelles des entrées $u_1, \ldots, u_n$ et de leurs dérivées. Aucune équation différentielle linéaire d'ordre inférieur à N n'est satisfaite par y.

Remarque : Des réciproques aux théorèmes II.2 et II.2.bis sont démontrées en [14], où il est aussi observé que les équations (9) et (9bis) fournissent des généralisations non linéaires des formes auto-régressives.

b) Extension de Picard-Vessiot

Etant donnée une équation algébrique, on définit un corps de rupture en adjoignant ses solutions au corps des coefficients et l'on peut alors appliquer la théorie de Galois (voir, par exemple, Lang [22]).

Avec les équations différentielles linéaires, la notion d'extension de Picard-Vessiot joue ce rôle. Pour en rappeler la définition (cf.

Kaplansky [18]), reprenons l'équation (11). Un corps différentiel K', contenant K est une extension de Picard-Vessiot pour l'équation considérée si, et seulement si,

1) K' est engendré par N solutions linéairement indépendantes sur le corps des constantes,
2) K' a même corps des constantes que K.

Soit $\underline{\underline{g}} \in \mathbb{R}\langle\langle X\rangle\rangle$ une série rationnelle. Notons E le $\mathbb{R}$-espace vectoriel formé par les séries $p \circ \underline{\underline{g}} \circ q$, où $p, q \in \mathbb{R}\langle X\rangle$. Si le rang de la matrice de Hankel de g est N, alors $\dim(E) \leq N^2$. Choisissons, en effet, $p_1,\ldots,p_N$, $q_1,\ldots,q_N \in \mathbb{R}\langle X\rangle$ de sorte que $p_i \circ \underline{\underline{g}}$ et $\underline{\underline{g}} \circ q_j$ forment des bases de Γ et Λ (cf. proposition I.2). Alors, tout élément de E est combinaison linéaire des $p_i \circ \underline{\underline{g}} \circ q_j$.

Soit $\mathcal{F}$ le plus petit sous-corps différentiel de κ contenant $\mathbb{R}\langle X\rangle \circ \underline{\underline{g}}$. Une démonstration utilisant des techniques analogues à celles du théorème II.2 permet d'établir le

Théorème II.3. $\mathcal{F}$ est une extension de Picard-Vessiot de $\mathbb{R}(\{u\})$ relativement à l'équation (9). Il est égal au sous-corps de κ engendré par $\mathbb{R}\{u\} \otimes E$.

Passons à la traduction en terme de systèmes réguliers. A (1), associons la représentation $\mu : \mathbb{R}\langle X\rangle \to \mathrm{End}(Q)$ ($\mathbb{R}\langle X\rangle$ avec le produit de Cauchy), $x_j \mapsto A_i$. Pour $p, q \in \mathbb{R}\langle X\rangle$, définissons les systèmes réguliers

- (1^p), identique à (1) à ceci près que l'état initial est $\mu(p)q(o)$,
- (1_q), identique à (1) à ceci près que la forme de sortie est $\lambda\mu(q)$,
- (1^p_q), identique à (1) à ceci près que l'état initial est $\mu(p)q(o)$ et la forme de sortie $\lambda\mu(q)$.

Notons y^p, y_q, y^p_q les sorties de (1^p), (1_q) et (1^p_q). Soient $\mathbb{R}\{u\}$ et $\mathbb{R}(\{u\})$ l'algèbre et le corps différentiel engendrés par les entrées $u_1,\ldots,u_n$ et leurs dérivées. Alors, le sur-corps différentiel $\mathcal{F}$ de $\mathbb{R}(\{u\})$ engendré par y_q ($q \in \mathbb{R}\langle X\rangle$) est extension de Picard-Vessiot de $\mathbb{R}(\{u\})$ relativement à (9bis). Soit E le $\mathbb{R}$-espace vectoriel engendré par les y^p_q. $\mathcal{F}$ est égal au corps engendré par $\mathbb{R}\{u\} \otimes E$.

$\mathcal{F}$ sera dit *corps différentiel de rupture* de g et (1).

CHAPITRE III - THEORIE DE GALOIS DIFFERENTIELLE

I. GROUPE DE GALOIS DIFFERENTIEL

Soient $\underline{\underline{g}} \in \mathbb{R}\langle\langle X\rangle\rangle$ une série rationnelle de $\mathcal{F}$ son corps différentiel de rupture. Considérons le groupe G des automorphismes de $\mathcal{F}$ qui laissent invariant tout élément de $\mathbb{R}(\{u\})$ et commutent à la dérivation. C'est, par définition, le groupe de Galois différentiel de l'extension de Picard-Vessiot $\mathcal{F}$ (cf. Kaplansky [18]) que nous appellerons *groupe de Galois (différentiel)* de $\underline{\underline{g}}$ et de tout système régulier admettant $\underline{\underline{g}}$ pour série génératrice.

Ce groupe va jouer le même rôle que le groupe de Galois d'une équation algébrique (cf. Lang [22]). Seulement, il n'a plus nécessairement un nombre fini d'éléments : c'est un groupe algébrique (cf. Kaplansky [18], chapitre IV). Un groupe algébrique est un groupe qui est aussi une variété algébrique, c'est-à-dire dont les éléments satisfont des équations polynomiales. Leur étude est un sujet important. Le premier traité les concernant est dû à Chevalley [2]. Depuis, il y a eu bien des livres avec des points de vue variés, par exemple celui des schémas de Grothendieck (Demazure et Gabriel [5]), celui des fonctions représentatives et des bigèbres (Hochschild [16], Abe [1]). Comme I.Kupka l'a fait observer à l'un des auteurs, ce dernier formalisme pourrait être ici intéressant et profitable si l'on rappelle que le mélange des séries non commutatives qui, comme on l'a constaté, joue un rôle essentiel, s'interprête à travers les bigèbres (cf. Sweedler [31]). Mentionnons enfin le cours de Northcott [23] qui a l'avantage de donner de façon claire les notions indispensables de géométrie algébrique.

Rappelons que E est le $\mathbb{R}$-espace vectoriel $p \circ \underline{\underline{g}} \circ q$ ($p, q \in \mathbb{R}\langle X\rangle$). Chacune des déviations, droites ou gauches, de l'algèbre de mélange laisse E invariant. On peut montrer, et cela conduit à une caractérisation plus intrinsèque du groupe de Galois, que G est isomorphe au groupe des automorphismes de E qui commutent avec les déviations R_{x_j} et préservent les relations algébriques vérifiées, dans l'algèbre de mélange, par les séries de E.

De manière plus précise, soit $\mathcal{A}$ la sous-algèbre de l'algèbre de mélange engendrée par E. Soit S(E) la $\mathbb{R}$-algèbre symétrique de E[(*)]. Il existe un épimorphisme canonique $\nu : S(E) \to \mathcal{A}$, de noyau J ; donc $\mathcal{A}$ et S(E)/J sont

(*) Rappelons que si $\dim E = \ell$, S(E) est isomorphe à une $\mathbb{R}$-algèbre de polynômes en ℓ variables commutatives (voir, par exemple, Lang [22]).

isomorphes. Tout endomorphisme R-linéaire φ de E se prolonge de manière unique en un endomorphisme $\overline{\varphi}$ de S(E). Il est alors possible de prouver le

Théorème III.1. Soit φ un élément du groupe de Galois G de $g \in \mathbb{R}\langle\langle X\rangle\rangle$ et de tout système régulier l'admettant pour série génératrice. Alors, $\varphi(E) \subset E$. Le morphisme $\varphi \to \varphi|E$ ainsi défini est un isomorphisme de G sur le groupe des automorphismes ψ de E tels que

- $\overline{\psi}(J) \subset J$,
- pour tout $r \in E$ et tout $x_j \in X$, $\psi(R_{x_j} r) = R_{x_j}\psi(r)$.

Remarque. En terme de systèmes réguliers, si l'on prend pour E la définition donnée à la fin du paragraphe II.b du chapitre II, $\mathcal{A}$ est la $\mathbb{R}$-algèbre commutative engendrée par E.

II. ALGEBRE DE LIE GALOISIENNE

a) Structures syntaxiques

Soit $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$ une série rationnelle produite, selon la formule (5), par une représentation (λ,μ,γ) réduite, c'est-à-dire telle que la dimension de Q soit égale au rang N de la matrice de Hankel. Plusieurs structures algébriques méritent alors d'être dégagées :

- La $\mathbb{R}$-algèbre associative syntaxique $\mathcal{M}$ (cf. [25]) engendrée par les matrices $\mu(x_j)$ $(j = 0,1,\ldots,n)$, c'est-à-dire $\mathcal{M} = \mu(\mathbb{R}\langle X\rangle)$ où $\mathbb{R}\langle X\rangle$ est pris avec le produit de Cauchy.

- La $\mathbb{R}$-algèbre de Lie syntaxique $\mathcal{L}$ (cf. [11]) engendrée par les matrices $\mu(x_j)$ $(j = 0,1,\ldots,n)$.

$\mathcal{M}$ et $\mathcal{L}$ seront aussi les algèbres associatives et de Lie syntaxiques de tout système régulier admettant $\underline{g}$ pour série génératrice.

On sait (cf. [8]) que

- $\mu(\mathbb{R}\langle X\rangle)\gamma = Q$
- $\lambda\mu(\mathbb{R}\langle X\rangle) = {}^tQ$ (dual de Q)

Etudions le noyau de μ :

$$\begin{aligned}\mathrm{Ker}\ \mu &= \{p \in \mathbb{R}\langle X\rangle \mid \mu(p) = 0\}\\ &= \{p \mid {}^t Q\mu(p)Q = 0\}\\ &= \{p \mid \forall q,r \in \mathbb{R}\langle X\rangle,\ \lambda\mu(q)\mu(p)\mu(r)\gamma = 0\}\\ &= \{p \mid \forall q,r\ \ (g, qpr) = 0\}\\ &= \{p \mid \forall q,r\ \ r\circ g\circ q = 0\}\end{aligned}$$

Autrement dit, Ker μ est l'orthogonal dans $\mathbb{R}\langle X\rangle$ du sous-espace E de $\mathbb{R}\langle\langle X\rangle\rangle$. Comme, bien entendu, $\mathcal{M} = \mathbb{R}\langle X\rangle/\mathrm{Ker}\ \mu$, E s'identifie au dual de $\mathcal{M}$.

Rappelons que la notion de structure syntaxique est apparue avec les automates finis et les langages rationnels (voir, à ce propos, les livres d'Eilenberg [6] et de Lallement [21]). Un langage L est une partie d'un monoïde libre X^*. On définit par X^* la congruence $\equiv_L$, dite syntaxique, suivante

$$w \equiv_L w' \quad \text{ssi} \quad \forall \alpha,\beta \in X^* : \alpha w\beta \in L \Leftrightarrow \alpha w'\beta \in L$$

Le quotient $\mathrm{Synt}(L) = X^*/\equiv_L$ est le monoïde syntaxique de L. Il est fini si, et seulement si, L est rationnel, c'est-à-dire, d'après le théorème de Kleene, si L est reconnu par un automate fini. Bien des propriétés de L peuvent être lues dans Synt(L).

b) Caractérisation de l'algèbre de Lie galoisienne

Le groupe de Galois G de $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$ étant un groupe de Lie, possède une algèbre de Lie $\mathfrak{G}$, dite *algèbre de Lie galoisienne* de $\underline{g}$ et de tout système régulier admettant $\underline{g}$ pour série génératrice.

Rappelons qu'étant donné une algèbre de Lie continue dans End(E), il ne lui correspond pas nécessairement un groupe algébrique de GL(E). Une algèbre de Lie possédant cette propriété est dite *algébrique* (cf. Chevalley [2]). On démontre que l'intersection d'algèbres de Lie algébriques est encore algébrique.

Théorème III.2. L'algèbre de Lie galoisienne de $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$, de représentation réduite (λ,μ,γ), est la plus petite algèbre de Lie algébrique contenant l'algèbre de Lie syntaxique. Le groupe de Galois de $\underline{g}$ s'identifie à un sous-groupe algébrique d'éléments inversibles de $\mathcal{M}$ et admet pour point générique la matrice $\sum_{w\in X^*} \mu w.w$, à coefficients dans κ.

Il est impossible de rappeler ici la notion de *point générique* qui, en géométrie algébrique, généralise celle, classique, de représentation paramétrique de courbes et de surfaces (renvoyons au paragraphe 2.11 du livre de Northcott [23]). La démonstration du théorème exige le lemme suivant dû à l'un des auteurs [26] (voir aussi Hochschild [15]), que nous admettrons ici :

Lemme III.3. Le plus petit groupe algébrique dont l'algèbre de Lie contient les matrices $\mu(x)$ admet la matrice $\sum w\mu w$, à coefficients dans κ, comme point générique.

Abordons maintenant la démonstration du théorème. Comme E s'identifie au dual L de $\mathcal{M}$, $\mathcal{M}$ s'identifie au dual de E, à travers la dualité définie pour toute série $s \in E$ et tout $m \in \mathcal{M}$ par

$$(s,m) = (s,p) \quad \text{où} \quad p \in \mu^{-1}(m) \subset \mathbb{R}\langle X\rangle$$

Pour tout $\varphi \in \mathrm{End}(E)$, notons ${}^t\varphi : \mathcal{M} \to \mathcal{M}$ l'endomorphisme transposé. On a donc

$$\Big(\varphi(s),m\Big) = \Big(s,{}^t\varphi(m)\Big)$$

En vertu du théorème III.1, nous identifions le groupe de Galois G de g au groupe des automorphismes de E qu'il définit. Introduisons l'application $f : G \to \mathcal{M}$, $\varphi \to {}^t\varphi(1)$ où $1 = \mu(1)$ est l'élément neutre de $\mathcal{M}$.

Comme pour tout $x_j \in X$ et tout $s \in E$, on a

$$\varphi(s\circ x_j) = \varphi(R_{x_j}s) = R_{x_j}\varphi(s) = \varphi(s)\circ x_j$$

Il vient pour tout $m \in \mathcal{M}$, $p \in \mu^{-1}(m)$

$$\begin{aligned}\Big(s,{}^t(\varphi(x_j)m)\Big) &= \Big(\varphi(s),\mu(x_j)m\Big) = \Big(\varphi(s),x_jp\Big)\\ &= \Big(\varphi(s)\circ x_j,p\Big) = \Big(\varphi(s\circ x_j),p\Big)\\ &= \Big(\varphi(s\circ x_j),m\Big) = \Big(s\circ x_j,{}^t\varphi(m)\Big)\end{aligned}$$

Posons ${}^t\varphi(m) = \mu(q)$, où $q \in \mathbb{R}\langle X\rangle$. Alors

$$\Big(s,{}^t\varphi(\mu(x_j)m)\Big) = (s,x_jq) = \Big(s,\mu(x_jq)\Big) = \Big(s,\mu(x_j){}^t\varphi(m)\Big)$$

Comme cela est vrai pour tout $s \in E$, on a ${}^t\varphi\Big(\mu(x_j)m\Big) = \mu(x_j){}^t\varphi(m)$. Donc

pour tout $m' \in \mathcal{M}$, il vient

$$ {}^t\varphi(m'm) = m' {}^t\varphi(m) $$

Par suite, si $\psi \in G$, on a ${}^t(\varphi\circ\psi)(1) = {}^t\psi\circ{}^t\varphi(1) = {}^t\psi({}^t\varphi(1).1)$

$$ = {}^t\varphi(1)\,{}^t\psi(1) $$

c'est-à-dire $f(\varphi\circ\psi) = f(\varphi)f(\psi)$. Comme $f(id) = {}^t id(1) = 1$, f est un morphisme de G dans le groupe des éléments inversibles de $\mathcal{M}$. Par ailleurs, f est injective : si ${}^t\varphi(1) = {}^t id(1) = 1$, alors ${}^t\varphi(m) = m^t(1) = m$, dont $\varphi = id$.

Quelle est l'image de f ? Remarquons que puisque E est le dual de $\mathcal{M}$, l'algèbre symétrique S(E) est isomorphe à l'algèbre des fonctions polynômes sur $\mathcal{M}$. Pour $U \in S(E)$, $m \in \mathcal{M}$, notons U(m) la valeur de la fonction polynôme U en m ; en particulier, si $U \in E$, on a $U(m) = (U,m)$.

Avec ces conventions, nous montrons que pour tout élément inversible $m \in \mathcal{M}$,

$$ m \in \varphi(G) \Leftrightarrow \forall U \in J,\ U(m) = 0 $$

où J est l'idéal de S(E) défini au paragraphe I de ce chapitre. Rappelons que $\mathcal{A}$ désigne l'algèbre de mélange engendrée par E, ν l'épimorphisme canonique $S(E) \to A$, et, pour tout $\varphi \in End(E)$, $\overline{\varphi}$ le prolongement canonique de φ à S(E). Avec ces notations, pour tout $U \in S(E)$, on a

$$ U\circ f(\varphi) = \left(\nu\circ\overline{\varphi}(U),1\right) $$

En effet, écrivons, sous forme abrégée, $U = \sum s_1 \ldots s_p$ où $s_i \in E$. Alors,

$$ \begin{aligned} U\circ f(\varphi) &= \sum\left(s_1, f(\varphi)\right)\ldots\left(s_p, f(\varphi)\right) \\ &= \sum\left(s_1, {}^t\varphi(1)\right)\ldots\left(s_p, {}^t\varphi(1)\right) \\ &= \sum\left(\varphi(s_1),1\right)\ldots\left(\varphi(s_p),1\right) \\ &= \sum\left(\varphi(s_1)\ \sqcup\ldots\sqcup\varphi(s_p),1\right) \\ &= \left(\nu(\sum\varphi(s_1)\ldots\varphi(s_p)),1\right) \\ &= \left(\nu\circ\overline{\varphi}(U),1\right) \quad . \end{aligned} $$

Par conséquent, si $m \in \varphi(G)$, $m = {}^t\varphi(1)$, avec $\varphi \in G$, alors pour tout $U \in J$, $U(m) = U_o f(\varphi) = (\nu_o \overline{\varphi}(U), 1) = 0$, puisque $\overline{\varphi}(U) \in J = \mathrm{Ker}\ \nu$.

Réciproquement, soit $\varphi \in \mathrm{Aut}(E)$ le transposé de l'automorphisme de $\mathcal{M}$: $m' \to m'm$. Donc, $m = {}^t\varphi(1)$. Alors, pour tout $s \in E$, $m' \in \mathcal{M}$, $p \in \mu^{-1}(m)$, $q \in \mu^{-1}(m')$, $x_j \in X$.

$$\begin{aligned}
\left(\varphi(R_{x_j} s), m'\right) &= \left(R_{x_j} s, {}^t\varphi(m')\right) \\
&= (R_{x_j} s, m'm) = (R_{x_j} s, qp) \\
&= (s, x_j qp) \quad = \left(s, \mu(x_j)\ (q)\, {}^t\varphi(1)\right) \\
&= \left(s, {}^t\varphi(\mu(x_j)\mu(q))\right) = \left(\varphi(s), \mu(x_j)\mu(q)\right) \\
&= \left(\varphi(s), x_j q\right) = \left(R_{x_j}\varphi(s), q\right) \\
&= \left(R_{x_j}\varphi(s), m'\right)
\end{aligned}$$

Par suite, $\varphi(R_{x_j} s) = R_{x_j}\varphi(s)$.

En outre, si $U \in J$, on a

$$\left(\nu_o \overline{\varphi}(U), 1\right) = U_o f(\varphi) = U_o {}^t\varphi(1) = U(m) = 0.$$

L'application $E \to E$, $s \to R_{x_j} s$ se prolonge en une dérivation de $S(E)$. De plus, $R_{x_j} \mathcal{A} \subset \mathcal{A}$. Alors, pour tout $U \in S(E)$,

$$\nu(R_{x_j} U) = R_{x_j} \nu(U)$$

Par conséquent, $U \in J$ implique $R_{x_j} U \in J$. De même, pour tout mot $w = x_j \ldots x_{j_o} \in X^*$ on définit $R_w : E \to E$ par

$$R_w = R_{x_j} \circ \ldots \circ R_{x_{j_o}}$$

et l'on a

$$U \in J \Rightarrow R_w U \in J$$

$$\nu(R_w U) = R_w \nu(U)$$

$$\overline{\varphi}(R_w U) = R_w \overline{\varphi}(U)$$

On en déduit que $(\nu_\circ\overline{\varphi}(U),w) = 0$ pour tout mot $w \in X^*$. Donc $\nu_\circ\overline{\varphi}(U) = 0$ et $\overline{\varphi}(U) \in \mathrm{Ker}\ \nu = J$.

Cela montre que le groupe de Galois G s'identifie au groupe des éléments inversibles m de $\mathcal{M}$ vérifiant, pour tout $U \in J$, $U(m) = 0$.

Si le rang de la matrice de Hankel de g est N, on peut considérer tout $\mu(w) \in \mathrm{End}(Q)$ comme une matrice $\in \mathbb{R}^{N\times N}$. Les coefficients M_{ij} $(1 < i,j \leq n)$ de la matrice

$$M = \sum w\mu w$$

engendrent E. En effet, si $p,q \in \mathbb{R}\langle X\rangle$, on a

$$p_\circ g_\circ q = \sum_w (g,qwp)w = \sum \lambda\mu g\mu w\mu p\gamma w = \lambda\mu q M\mu p\gamma$$

qui est la combinaison linéaire des M_{ij}. Pour i, j fixés, il existe $p,q \in \mathbb{R}\langle X\rangle$ tels que, d'après ce qui a été écrit au paragraphe I de ce chapitre, $M_{ij} = p_\circ g_\circ q$.

Soient $\mathbb{R}[t_{i,j}]$ la $\mathbb{R}$-algèbre des fonctions polynomiales de $\mathbb{R}^{N\times N}$ et $\rho : \mathbb{R}[t_{ij}] \to \mathcal{A}$, $t_{ij} \mapsto M_{ij}$ le morphisme canonique. Pour tout $m \in \mathcal{M}\cap GL_N(\mathbb{R})$, on a

$$\forall U \in J : U(m) = 0 \Leftrightarrow \forall P \in \mathrm{Ker}\ \rho,\ P(m) = 0$$

Donc

$$m \in f(G) \Leftrightarrow \forall P \in \mathrm{Ker}\ \rho,\ P(m) = 0$$

La démonstration s'achève en appliquant le lemme III.3.

c) Quelques corollaires

Il est clair que la sous-algèbre associative de $\mathcal{M}$ engendrée par l'algèbre de Lie galoisienne $\mathcal{G}$ est égale à $\mathcal{M}$. D'autre part, on sait que $\mathcal{G}$ est contenu dans la sous-algèbre de $\mathcal{M}$ engendrée par G (cf. Chevalley [2], chapitre II, paragraphe 8, proposition 6). Il vient donc :

Corollaire III.4. Le groupe de Galois d'une série rationnelle, et de tout système régulier l'admettant pour une série génératrice, engendre la $\mathbb{R}$-algèbre associative syntaxique.

Dans la démonstration du théorème III.2, il a été prouvé :

Corollaire III.5. La $\mathbb{R}$-algèbre des fonctions polynômes sur le groupe de Galois G de $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$, et de tout système régulier l'admettant pour série génératrice, est isomorphe à $\mathcal{A}$.

En géométrie algébrique, on utilise très souvent une topologie, dite de Zariski, où les ensembles fermés sont les zéros de systèmes d'équations algébriques (cf. Kaplansky [18], chapitre IV, Northcott [23], paragraphe 2.3). Alors, un ensemble irréductible est un ensemble qui ne peut s'exprimer comme union de deux sous-ensembles propres fermés (cf. [23], chapitre 3). On démontre qu'un ensemble algébrique est irréductible si, et seulement si, l'anneau des fonctions polynomiales est intègre (cf. [23], chapitre 3, théorème 9). Comme $\mathcal{A}$ est intègre, il vient :

Corollaire III.6. Le groupe de Galois d'une série rationnelle, et de tout système régulier l'admettant, pour série génératrice, est irréductible, donc connexe, pour la topologie de Zariski.

III. LE CAS RESOLUBLE

a) Analogue du théorème de Vessiot

Observons d'abord que tous les raisonnements et les calculs concernant les séries rationnelles non commutatives restent valables avec des coefficients pris dans tout corps commutatif(*). En particulier, on peut prendre le corps $\mathbb{C}$ des complexes qui jouit de la propriété supplémentaire, dont nous avons ici besoin, d'être algébriquement clos.

Un groupe (resp. une algèbre de Lie) est dite résoluble si, et seulement si, les groupes dérivés (resp. les algèbres de Lie dérivées) sont nuls à partir d'un certain rang (cf. Chevalley [2], chapitre V).

Corollaire III.7. Soit $\underline{g} \in \mathbb{C}\langle\langle X\rangle\rangle$ une série rationnelle à coefficients complexes. Le groupe de Galois G de $\underline{g}$ est résoluble si, et seulement si, $\underline{g}$ appartient à la $\mathbb{C}$-algèbre de Cauchy engendrée par les $x_j \in X$ $(j = 0,\ldots,n)$ et les séries rationnelles de la forme

$$\left(1 - \sum_{j=0}^{n} \alpha_j x_j\right)^{-1} \qquad (\alpha_j \in \mathbb{C}) \qquad (**)$$

(*) Cela n'a évidemment pas de sens avec les systèmes réguliers. Que signifierait un tel système à coefficients dans un corps fini ?

(**) C'est-à-dire dont le rang de la matrice Hankel est un.

Démonstration. (i) Supposons G résoluble. Comme, en vertu du corollaire III.6, G est connexe, on peut appliquer un théorème classique dû à Lie (théorème 4.11 de [18]) et mettre les éléments de G sous forme de matrices triangulaires. D'après le corollaire III.4, il en va de même pour l'algèbre associative syntaxique $\mathcal{M}$. La conclusion découle alors de la proposition III.4.4 de [25].

(ii) Réciproquement, supposons $\underline{\underline{g}}$ de la forme cherchée. D'après la proposition III.4.4 de [25], $\mathcal{M}$ peut se mettre sous forme de matrices triangulaires, donc également G qui est, ainsi, résoluble.

Il importe de comprendre la signification de ce résultat pour les systèmes réguliers. On sait qu'à une lettre $x_j \in X$ correspond $\int_0^t d\xi_j = \xi_j(t)$ où $\xi_o(t) = t$, $\xi_i(t) = \int_0^t u_1(\tau)d\tau \quad (i = 1,\ldots,n)$.

Lemme III.8. La sortie correspondante à la série génératrice $\left(1 - \sum_{j=0}^{n} \alpha_j x_j\right)^{-1}$ est $\exp\left(\alpha_o t + \sum_{1\leq i\leq n} \alpha_i \int_0^t u_i(\tau)d\tau\right)$.

Démonstration. Si l'on écrit

$$\exp\left(\alpha_o t + \sum_{i=1}^{n} \alpha_i \int_0^t u_i(\tau)d\tau\right) = \exp\left(\sum_{j=0}^{n} \alpha_i \int_0^t d\xi_j\right),$$

il vient

$$\exp\left(\sum_{j=0}^{n} \alpha_j \int_0^t d\xi_j\right) = 1 + \sum_{\nu\geq 0} \sum_{j_o,\ldots,j_\nu=0}^{n} \alpha_{j_\nu}\ldots\alpha_{j_o} \int_0^t d\xi_{j_\nu}\ldots d\xi_{j_o}$$

La série génératrice correspondante est

$$1 + \sum_{\nu\geq 0} \sum_{j_o,\ldots,j_\nu=0}^{n} \alpha_{j_\nu}\ldots\alpha_{j_o}\, x_{j_\nu}\ldots x_{j_o} = \left(1 - \sum_{j=0}^{n} \alpha_j x_j\right)^{-1}.$$

Comme la concaténation correspond à itérer l'intégration, il en résulte :

Lemme III.9. La sortie correspondant à une série génératrice $r_{j_\nu}\ldots r_{j_o}$ où les r_{j_o} sont soit égaux à x_j soit à $\left(1 - \sum \alpha_j x_j\right)^{-1}$, est $\int_0^t d\eta_{j_\nu}\ldots d\eta_{j_o}$ où r_{j_o} est soit égal à $\xi_j(\tau)$ soit à $\exp\left(\sum_{j=0}^{n} \alpha_j \xi_j(\tau)\right)$.

On peut donc énoncer l'analogue suivant du théorème de Vessiot :

Théorème III.10. Le groupe de Galois d'un système régulier est résoluble si, et seulement si, sa sortie est combinaison $\mathbb{C}$-linéaire d'intégrales itérées de la forme $\int_0^t d\eta_{j_\nu} \ldots d\eta_{j_0}$, où les $\eta_{j_0}(\tau)$ sont égaux soit à $\xi_j(\tau)$, soit à $\exp\left(\sum \alpha_j \xi_j(\tau)\right)$ $(\alpha_j \in \mathbb{C})$

Si l'on revient au corps $\mathbb{R}$ des réels, apparaissent, bien entendu, les lignes trigonométriques élémentaires.

Corollaire III.11. Le groupe de Galois d'un système régulier est résoluble si, et seulement si, sa sortie est combinaison $\mathbb{R}$-linéaires d'intégrales itérées de la forme $\int_0^t d\eta_{j_\nu} \ldots d\eta_{j_0}$, où les $\eta_{j_0}(\tau)$ sont égaux soit à $\xi_j(\tau)$, soit à $\exp\left(\sum \alpha_j \xi_j(\tau)\right)\sin\left(\sum \beta_j \xi_j(\tau)\right)$ ou $\exp\left(\sum \alpha_j \xi_j(\tau)\right)\cos\left(\sum \beta_j \xi_j(\tau)\right)$ $(\alpha_j, \beta_j \in \mathbb{R})$.

Remarques. (i) Les liens du groupe de Galois avec l'algèbre associative syntaxique (corollaire III.4) montre qu'il est résoluble si, et seulement si, l'algèbre de Lie syntaxique l'est. Or, ce dernier objet est d'un usage plus courant en théorie de la commande (cf. [11]).

(ii) Il est instructif de comparer ce qui précède avec les approches de Wei et Norman [34] et de Terashima et Akashi [32].

b) Deux exemples

α) Supposons l'algèbre de Lie syntaxique de $\underline{g} \in \mathbb{R}\langle\langle X\rangle\rangle$, ou de tout système régulier l'admettant pour série génératrice, nilpotente (cf. Chevalley [2], chapitre IV, paragraphe 1.2), donc résoluble. Alors, les liens entre intégrales itérées et formule de Baker-Campbell-Hausdorff permettent de montrer que la sortie du système est fonction d'un nombre fini d'intégrales itérées (cf. [13]).

β) Considérons le système régulier

$$\begin{cases} \dot{q}(t) = \left(A_0(t) + u_1(t)A_2(t)\right)q(t) \\ y(t) = \lambda q(t) \end{cases} \tag{12}$$

identique à (1) à ceci près qu'il n'y a qu'une seule entrée. Crouch [4] a

montré l'intérêt qu'il y avait à regarder le cas où le développement de Volterra de (12) est fini.

Proposition III.12. Si le développement de Volterra du système (12) est fini, son algèbre de Lie syntaxique est résoluble.

Démonstration. Supposons (12) réduit. Alors, l'algèbre de Lie syntaxique $\mathcal{L}$ est engendrée par A_0 et A_1. Si l'ordre le plus élevé du noyau de Volterra apparaissant dans le développement de (12) est m, un raisonnement classique sur les matrices de Hankel (cf. [8]) montre que tout élément de l'algèbre dérivée d'ordre m+1 est nul puisque y apparaissent au moins m+1 occurrences de A_1.

CONCLUSION

Une conséquence souhaitable de ce travail serait d'isoler des dispositifs physiques décrits par des systèmes réguliers à algèbres de Lie syntaxiques résolubles. Il faudrait alors déduire de sa structure une architecture de microprocesseurs permettant de calculer en temps réel son comportement entrée-sortie.

Il n'est peut-être pas inintéressant de voir si la théorie ici développée a un pendant pour les systèmes en temps discret. Comme le produit de deux systèmes réguliers n'est plus nécessairement régulier, il faudrait les remplacer par les systèmes à état-affine, où les entrées peuvent apparaître de façon polynomiale, et qui sont, eux, fermés pour le produit (cf. [12]). Quant à l'algèbre différentielle, elle devrait être remplacée par l'algèbre aux différences (cf. Cohn [3]).

BIBLIOGRAPHIE

[1] E. ABE. Hopf Algebras (traduit du japonais), Cambridge University Press, Cambridge, 1980.

[2] C. CHEVALLEY. Théorie des Groupes de Lie (Groupes algébriques. Théorèmes généraux sur les algèbres de Lie), Hermann, Paris, 1951.

[3] R.M. COHN. Difference Algebra, Interscience Publishers, New York, 1965.

[4] P.E.CROUCH. Dynamical realizations of finite Volterra series, SIAM J. Control Optimiz., 19, 177-202, 1981.

[5] M. DEMAZURE et P. GABRIEL. Groupes Algébriques, t. 1, Masson, Paris, et North-Holland, Amsterdam, 1970.

[6] S. EILENBERG. Automata, Languages and Machines, vol. A et B, Academic Press, New York, 1974 et 1976.

[7] M. FLIESS. Sur divers produits de séries formelles, Bull. Soc. Math., France, 102, 181-191, 1974.

[8] M. FLIESS. Matrices de Hankel, J. Math. Pures Appl., 53, 197-222, 1974.

[9] M. FLIESS. Un outil algébrique : les séries formelles non commutatives, in "Mathematical Systems Theory" (G. Marchesini and S.K. Mitter, eds.) Lect. Notes Econom. Math. Syst. 131, p. 122-148, Springer-Verlag, Berlin, 1976.

[10] M. FLIESS. Fonctionnelles causales non linéaires et indéterminées non commutatives, Bull. Soc. Math. France, 109, 3-40, 1981.

[11] M. FLIESS. Réalisation locale des systèmes non linéaires, algèbres de Lie filtrées transitives et séries génératrices non commutatives, Inventiones Math., 1983.

[12] M. FLIESS et D. NORMAND-CYROT. Vers une approche algébrique des systèmes non linéaires en temps discret, in "Analysis and Optimization of Systems" (A. Bensoussan and J.L. Lions, eds.), Lect. Notes Control Informat. Sci. 28, p. 594-603, Springer-Verlag, Berlin, 1980.

[13] M. FLIESS et D. NORMAND-CYROT, Algèbres de Lie nilpotentes, intégrales itérées de K.T. Chen et formule de Baker-Campbell-Hausdorff, in "Séminaires de Probabilités XVI 1980/81" (J. Azéma et M.Yor, réd.), Lect. Notes Math. 920, p. 257-265, Springer-Verlag, Berlin, 1982.

[14] M. FLIESS et C. REUTENAUER. Une application de l'algèbre différentielle aux systèmes réguliers (ou bilinéaires), in "Analysis and Optimization of Systems" (A. Bensoussan and J.L. Lions, eds), Lect. Notes Control Informat. Sci. 44, p. 99-107, Springer-Verlag, Berlin, 1982.

[15] G.P. HOCHSCHILD. Representation Theory of Lie Algebras, The University of Chicago, Summer Course 1959.

[16] G.P. HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebra, Springer-Verlag, New York, 1981.

[17] G. JACOB. Réalisation des systèmes réguliers (ou bilinéaires) et séries génératrices non commutatives, in "Outils et Modèles Mathématiques pour l'Automatique, l'Analyse de Systèmes et le Traitement du Signal" (I.D. Landau, réd.), t. 1, p. 325-357, C.N.R.S., Paris, 1981.

[18] I. KAPLANSKY. An Introduction to Differential Algebra, Hermann, Paris, 1957.

[19] E.R. KOLCHIN. Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, Ann. of Math., 49, 1-42, 1948.

[20] E.R. KOLCHIN. Differential Algebras and Algebraic Groups, Academic Press, New York, 1973.

[21] G. LALLEMENT. Semigroups and Combinatorial Applications, Wiley, New York, 1979.

[22] S. LANG, Algebra, Addison-Wesley, Reading, MA, 1965.

[23] D.G. NORTHCOTT. Affine Sets and Affine Groups, Cambridge University Press, Cambridge, 1980.

[24] E. PICARD. Traité d'Analyse, t. 3, chap. 17, Gauthier-Villars Paris, 1898 (Reimpression : Analogie entre la théorie des équations différen-

tielles linéaires et la théorie des équations algébriques, Gauthier-Villars, Paris, 1936).

[25] C. REUTENAUER. Séries formelles et algèbres syntactiques. J. Algebra, 66, 448-483, 1980.

[26] C. REUTENAUER. Point générique du plus petit groupe algébrique dont l'algèbre de Lie contient plusieurs matrices données, C.R. Acad. Sc. Paris I-293, 577-580, 1981.

[27] C. REUTENAUER. Non commuting variables, I (finite automata), II (rational generating series), III (realization of bilinear systems), in "Encyclopedia of Systems and Control" (M.D. Singh, ed.), Pergamon Press, Oxford, à paraître.

[28] J.F. RITT. Differential Algebra, Amer. Math. Soc., New York, 1950.

[29] M.P. SCHÜTZENBERGER. On the definition of a family of automats, Informat. Control. 4, 245-270, 1961.

[30] M.P. SCHÜTZENBERGER. On finite monoids having only trivial subgroups, Informat. Control., 8, 190-194, 1965.

[31] M.E. SWEEDLER. Hopf Algebras, Benjamin, New York, 1969.

[32] K. TERASHIMA et H. AKASHI. Lie algebraic approach to explicit solution of bilinear stochastic differential equations, Math. Japonica, 27, 603-608, 1982.

[33] E. VESSIOT. Méthodes d'intégrations élémentaires, in "Encyclopédie des Sciences Mathématiques Pures et Appliquées", t. 2, vol. 3, fasc. 1, p. 58-70, 1910.

[34] J. WEI et E. NORMAN. Lie algebraic solution of linear differential equations, J. Math. Physics, 4, 575-581, 1963.