A. PROPRIÉTÉS ALGÉBRIQUES

$\mathbf{F}_q$ — la méthode banale consistant à calculer les valeurs de $P(x)$ pour x parcourant $\mathbf{F}_q$ nécessite en moyenne près de q évaluations, en calculant l'ordre de la matrice compagnon de P on peut répondre à la question en $O(\text{Log } q)$ opérations.

Quelques ouvrages contiennent une présentation générale des suites récurrentes linéaires, d'abord le livre de E. Lucas [33], ainsi que Bachman [3], Henrici [30] chap. 7 et [29], Montel [47], Pisot [52]. Signalons aussi le livre de Dickson [22] sur l'histoire de la théorie des nombres, le chapitre XVII est consacré aux suites récurrentes linéaires.

A. PROPRIÉTÉS ALGÉBRIQUES

I. Séries rationnelles sur un corps $\mathscr{K}$

Soit une série formelle

$$\Xi(X) = \sum_{n \geqslant 0} \xi_n X^n$$

à coefficients dans un corps (commutatif) $\mathscr{K}$; nous allons étudier différents critères de rationnalité d'une telle série.

1. Supposons Ξ *rationnelle*, c'est-à-dire qu'il existe deux polynômes A et B, à coefficients dans $\mathscr{K}$, tels que

$$\Xi(X) = \frac{A(X)}{B(X)}, \qquad B(0) \neq 0. \tag{1}$$

Soient alors $\omega'_1, ..., \omega'_k$ les racines du polynôme B dans une extension algébrique convenable $\mathscr{L}$ du corps $\mathscr{K}$ et soit τ_i la multiplicité de ω'_i $(i = 1, ..., k)$.

La décomposition en éléments simples de la fraction A/B est de la forme

$$\frac{A(X)}{B(X)} = Q(X) + \sum_{i=1}^{k} \sum_{j=1}^{\tau_i} \frac{\alpha_{ij}}{(X - \omega'_i)^j}, \tag{2}$$

où $Q(X)$ est un polynôme à coefficients dans $\mathscr{K}$ (c'est le quotient de la division euclidienne de A par B) et où les α_{ij} appartiennent au corps $\mathscr{L}$.

L'identité formelle, vraie pour tout entier positif j,

$$(X - \omega)^{-j} = (-1)^j \omega^{-j} \sum_{n \geqslant 0} \binom{n+j-1}{j-1} (X \omega^{-1})^n \quad \left(\text{où } \binom{n}{0} = 1\right)$$

jointe à (1) et (2) conduit à la relation

$$\Xi(X) = Q(X) + \sum_{n \geqslant 0} \sum_{i=1}^{k} \sum_{j=1}^{\tau_i} (-1)^j \alpha_{ij} \omega_i^{n+j} \binom{n+j-1}{j-1} X^n$$

où on a posé $\omega_i = \dfrac{1}{\omega_i'}$ $(i = 1, ..., k)$.

Si Q a pour degré n_0, on a donc

$$\xi_n = P_1(n)\,\omega_1^n + ... + P_k(n)\,\omega_k^n \quad \text{pour} \quad n > n_0\,, \tag{3}$$

avec

$$P_i(n) = \sum_{j=1}^{\tau_i} (-1)^j \alpha_{ij} \omega_i^j \binom{n+j-1}{j-1}\,. \tag{4}$$

Remarque. Lorsque la caractéristique du corps $\mathscr{K}$ est nulle, chaque P_i est un polynôme (à coefficients dans le corps $\mathscr{L}$) en n de degré plus petit que τ_i, et même égal à $\tau_i - 1$ lorsque la représentation (1) est irréductible. On dit alors que l'expression (3) est un *polynôme-exponentiel.* A ce sujet voir aussi l'exemple 2) plus loin.

2. Réciproquement, supposons maintenant que les relations (3) et (4) aient lieu pour $n > n_0$.

Soit E l'opérateur de décalage (en anglais « shift operator »), qui à une suite $\xi = (\xi_n)_{n \geqslant 0}$ associe la suite $E\xi = (\xi_{n+1})_{n \geqslant 0}$. Nous allons montrer que la suite

$$(E - \omega_1 I)^{\tau_1} ... (E - \omega_k I)^{\tau_k}(\xi_n)$$

est ultimement nulle, et plus précisément que $\xi = (\xi_n)_{n \geqslant 0}$ satisfait à l'*équation aux différences finies* à coefficients constants

$$E^{n_0} \,.\, G(E)\,(\xi_n) = 0 \tag{5}$$

où

$$G(X) = \frac{X^m}{B(0)} B(X^{-1}) = \prod_{i=1}^{k} (X - \omega_i)^{\tau_i}\,. \tag{5'}$$

Du fait que les opérateurs $E - \omega_i I$ commutent entre eux, il suffit, par linéarité, de vérifier que les suites

$$(E - \omega I)^{j'} \left(\binom{n+j''-1}{j-1} \omega^n\right)$$

sont nulles pour tout triplet d'entiers naturels j, j', j'' vérifiant $j' \geqslant j \geqslant 1$

et $j'' \geqslant j$. Raisonnons par récurrence sur j'. Ce résultat est clair pour $j' = 1$. Supposons $j' > 1$ et l'assertion vraie jusqu'à l'ordre $j'-1$. La relation

$$(E-\omega I)\left(\binom{n+j''-1}{j-1}\omega^n\right) = \left(\left(\binom{n+j''}{j-1}\right)-\binom{n+j''-1}{j-1}\right)\omega^{n+1}\Big)$$
$$= \left(\binom{n+j''-1}{j-2}\omega^{n+1}\right) = \omega\left(\binom{n+j''-1}{j-2}\omega^n\right)$$

permet d'appliquer l'hypothèse de récurrence, ce qui prouve le résultat annoncé.

Si on pose en (5)

$$(6) \qquad G(X) = X^m - a_{m-1}X^{m-1} - \ldots - a_0\,, \qquad m = \sum_{i=1}^{k} \tau_i\,,$$

on a donc démontré que la suite (ξ_n) vérifie la condition

$$(7) \qquad \xi_{n+m} = a_{m-1}\,\xi_{n+m-1} + \ldots + a_0\,\xi_n \quad \text{pour} \quad n > n_0\,,$$

c'est donc — par définition — une *suite récurrente linéaire* (en abrégé: s.r.l.); le polynôme $X^{n_0}G(X)$ sera appelé *échelle de récurrence* [1]) ou *polynôme caractéristique* et l'entier (n_0+m) *ordre* de la s.r.l. (ξ_n) (il s'agit d'un abus de langage car ces objets ne sont pas uniques; voir plus avant).

Supposons enfin que la relation (7) ait lieu. On vérifie alors aisément que l'expression

$$\left(\sum_{n\geqslant 0} \xi_n X^n\right)(a_0X^m + a_1X^{m-1} + \ldots + a_{m-1}X - 1)$$

est un polynôme en X de degré au plus $n_0 + m$. La série $\Xi(X) = \sum_{n\geqslant 0} \xi_n X^n$ est alors une fraction rationnelle de la forme (1), ce qui achève la preuve de l'équivalence logique des trois objets considérés.

II. Quelques exemples

Ce paragraphe contient un certain nombre d'exemples variés qui illustrent les résultats généraux que nous venons de présenter. De plus de nombreux exemples figurent dans tout bon livre sur le calcul aux différences finies ou sur la combinatoire (entre autres [21], [26], [29], [30], [46]).

1) L'exemple le plus populaire de s.r.l. et aussi le plus ancien (il date de 1202) est la suite (F_n) de Fibonacci définie par les conditions

$$F_0 = 0\,, \quad F_1 = 1\,, \quad F_{n+2} = F_{n+1} + F_n \quad \text{pour} \quad n \geqslant 0$$

---

[1]) C'est la terminologie de E. Lucas [33].

de sorte que ses valeurs successives sont

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Dans ce cas la formule (3) s'écrit

$$F_n = \frac{\omega_1^n - \omega_2^n}{\omega_1 - \omega_2} \quad \text{où} \quad \omega_1 = \frac{1+\sqrt{5}}{2} \quad \text{et} \quad \omega_2 = \frac{1-\sqrt{5}}{2}$$

en effet pour $n = 0$ et 1 le membre de droite vaut 0 et 1 et comme $\omega_i^2 = \omega_i + 1, i = 1, 2$, le membre de droite vérifie la même relation de récurrence que F_n.

2) Si $\xi = (\xi_n)_{n \geqslant 0}$ est une s.r.l. alors toute section de ξ, c'est-à-dire toute suite $\eta = (\xi_{an+b})_{n \geqslant 0}$, où a et b sont deux entiers $\geqslant 0$ fixés, est une s.r.l.; de plus si $G(X) = \prod_{i=1}^{k} (X - \omega_i)^{r_i}$ est le polynôme caractéristique de ξ alors le polynôme $\prod_{i=1}^{k} (X - \omega_i^a)^{r_i}$ est un polynôme caractéristique de la suite η. [En caractéristique zéro, ceci résulte du fait que $n \mapsto \xi_{an+b}$ est un polynôme exponentiel; en particulier, lorsque les ω_i sont rationnels on a pour tout n

$$\prod_{i=1}^{k} (E - \omega_i^a I)(\xi_{an+b}) = 0,$$

ξ_{an+b} étant exprimé comme combinaison des ω_j^{an}. Il en résulte que cette formule est vraie pour des ω_i appartenant à un anneau unitaire quelconque. C'est le « principe de prolongement des identités algébriques », voir [11], chap. V, § 2, scholie au théorème 3.]

3) Soient $\xi = (\xi_n)$ et $\eta = (\eta_n)$ deux s.r.l. de polynômes caractéristiques respectifs G et H. Alors leur somme $\xi + \eta = (\xi_n + \eta_n)$ est une s.r.l. admettant GH comme polynôme caractéristique.

[Preuve: $(GH)(E)(\xi + \eta) = H(E)[G(E)\xi] + G(E)[H(E)\eta] = 0$].

Par exemple, la suite $(\xi_n + \alpha)_{n \geqslant 0}$, α fixe, est une s.r.l. admettant $(X-1)\,G(X)$ comme échelle. On peut noter aussi que $(\theta_n) = (\xi_{n+1} - a\xi_n)$ a la même échelle $G(X)$ que (ξ_n) si $G(a) \neq 0$ mais l'échelle $G(X)/(X-a)$ dans le cas contraire. Plus généralement, si $G(X) = P(X)\,Q(X)$ et si $\xi = (\xi_n)$ est une s.r.l. d'échelle G, la suite $P(E)\,.\,\xi$ est une s.r.l. qui admet Q comme échelle.

4) Soit a un entier $\geqslant 2$ et $\xi^{(0)}, \ldots, \xi^{(a-1)}$ des s.r.l.; alors la suite $\xi = (\xi_n)$ définie par $\xi_n = \xi_q^{(r)}$ où $n = aq + r$, $0 \leqslant r < a$, est une s.r.l.; de plus,

si G_i est le polynôme caractéristique de $\xi^{(i)}$, $0 \leqslant i < a$, alors ξ admet le polynôme $G(X) \equiv G_0(X^a) \ldots G_{a-1}(X^a)$ comme polynôme caractéristique. [D'après l'exemple précédent, il suffit de considérer le cas où une seule à la fois des $\xi^{(i)}$ n'est pas nulle; le résultat est alors évident.]

5) Soient $\xi = (\xi_n)$ et $\eta = (\eta_n)$ deux s.r.l. et $G = \prod_{i=1}^{k} (X-\omega_i)^{r_i}$ et $H = \prod_{j=1}^{h} (X-\sigma_j)^{s_j}$ leurs polynômes caractéristiques; alors le *produit de Hadamard* $\theta = (\xi_n \eta_n)_{n \geqslant 0}$ de ξ et η est une s.r.l. dont le polynôme caractéristique est $\prod_{i,j} (X-\omega_i\sigma_j)^{r_i+s_j-1}$. [En caractéristique zéro, $n \mapsto \xi_n\eta_n$ est un polynôme exponentiel donc θ est une s.r.l.; le cas général s'en déduit par le principe énoncé plus haut.] Par contre, si on considère le produit $\xi * \eta = \zeta$ où $\zeta_n = \sum_{i=0}^{n} \binom{n}{i} \xi_i \eta_{n-i}$, on trouve que ζ est une s.r.l. dont le polynôme caractéristique est $\prod_{i,j} (X-(\omega_i+\sigma_j))^{r_i+s_j-1}$ [voir plus loin A IV 1].

6) Avec les notations de l'exemple précédent, le *produit de Cauchy* $\theta_n = \sum_{i=0}^{n} \xi_i \eta_{n-i}$ de ξ et η est aussi une s.r.l. dont le polynôme caractéristique est GH [C'est le développement du produit de deux fractions rationnelles]. Ainsi, si $\eta_n = 1$ pour tout n, on voit que $n \mapsto \xi_0 + \xi_1 + \ldots + \xi_n$ est une s.r.l. admettant $(X-1) \cdot G(X)$ comme échelle de récurrence.

7) Si $A(X)$ est un polynôme sur $\mathscr{K}$, non nul et de degré h et si $\xi = (A(n))_{n \geqslant 0}$, alors ξ est une s.r.l. admettant $(X-1)^{h+1}$ comme polynôme caractéristique.

8) Soit A comme dans l'exemple précédent et soit ξ une s.r.l. de polynôme caractéristique G; toute suite η solution de l'équation $A(E)\eta = \xi$ est une s.r.l. admettant $A(X) \cdot G(X)$ comme polynôme caractéristique. [Preuve: $(AG)(E)\eta = G(E)[A(E)\eta] = G(E)\xi = 0$].

9) Soit $A = (a_{ij})$ une matrice carrée à coefficients dans $\mathscr{K}$; posons $A^n = (a_{ij}(n))$, alors, pour tout couple (i,j) fixé, la suite $n \mapsto \xi_n = a_{ij}(n)$ est une s.r.l. admettant le polynôme minimal G de A comme polynôme caractéristique. [En développant la relation $G(A) \cdot A^n = 0$ on obtient $G(E)\xi = 0$]. (A ce sujet, voir aussi [14].)

10) Inversement toute s.r.l. ξ est obtenue à partir des puissances successives d'une matrice. Soit

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{m-1} \end{pmatrix}$$

la matrice-compagnon du polynôme caractéristique $G(X) = X^m - a_{m-1} - \dots - a_0$; alors si on pose

$$U_n = \begin{pmatrix} \xi_n \\ \cdot \\ \cdot \\ \cdot \\ \xi_{n+m-1} \end{pmatrix}$$

on a la relation

$$U_{n+1} = A\,U_n \quad \text{pour} \quad n \geqslant 0,$$

donc $U_n = A^n U_0$. Il en résulte que, pour n fixé, on peut calculer U_n — donc en particulier ξ_n — en $O(\operatorname{Log} n)$ opérations. [C'est un truc bien connu: on écrit n en binaire, $n = \Sigma\, e_i 2^i$, et $A^n = \prod_{\substack{i \\ e_i \neq 0}} A^{2^i} \dots$].

11) Soit $T = (t_{ij})_{i,\,j \geqslant 0}$, où $t_{ij} = \binom{i}{j}$, la matrice de Pascal infinie; alors, pour chaque j fixé, la j-ième colonne de T est la $(j+1)$-ième s.r.l. fondamentale (voir plus avant) d'échelle $(X-1)^{j+1}$.

12) L'exemple précédent est un cas particulier de celui-ci. Soit $H = (h_{ij})$ où

$$h_{ij} = h_{ij}(X_0, \dots, X_k) = \begin{cases} \displaystyle\sum_{i_0 + \dots + i_k = n-k} X_0^{i_0} \dots X_k^{i_k} & \text{si} \quad n \geqslant k \\ 0 & \text{sinon} \end{cases}$$

est le polynôme homogène élémentaire de degré $n - k$ en les variables $X_0, \dots, X_k$. Alors vaut pour H un résultat analogue au précédent avec cette fois le polynôme $G_{k+1} = \prod_{i=0}^{k} (X - X_i)$ comme échelle de récurrence. En particulier:

a) si $X_i = 1$ pour tout i, $H = T$.

b) si $X_i = n$, n entier fixé, alors $H = T^n$.

c) si $X_i = q^i$ alors H est le triangle des coefficients q-nomiaux (ou coefficients de Gauss)

$$h_{ij} = \binom{i}{j}_q = \begin{cases} \dfrac{(i)_q!}{(j)_q!(i-j)_q!} & \text{si} \quad i \geqslant j \\ 0 & \text{si} \quad i < j, \end{cases}$$

où $(0)_q! = 1$, $(i)_q! = \prod_{s=1}^{n} (s)_q$ et $(s)_q = 1 + q + \ldots + q^{s-1}$.

d) si $X_i = i$ alors H est la matrice des nombres de Stirling de seconde espèce $h_{ij} = S(i,j)$ pour $i \geqslant j$, $h_{ij} = 0$ pour $i < j$, définis par la formule

$$X^i = \sum_{j=0}^{i} S(i,j)\, X(X-1)\ldots(X-k+1)$$

(voir [15]).

13) Soit $\xi = (\xi_n)$ une s.r.l. d'échelle $G(X) = X^m - a_{m-1}X^{m-1} - \ldots - a_0$; on peut regarder son terme ξ_n en tant que polynôme en les variables $a_0, \ldots, a_{m-1}$. Alors la suite donnée par

$$\eta_n = \frac{\partial^h \xi_n}{\partial_{a_0}^{h_0} \ldots \partial_{a_{m-1}}^{h_{m-1}}}$$

est une s.r.l. d'échelle G^{h+1}.

III. Espaces de s.r.l. sur $\mathscr{K}$

Dans *I* nous avons étudié une suite particulière $\xi = (\xi_n)$ à valeurs dans $\mathscr{K}$ et donné différentes conditions équivalentes pour que ξ soit une s.r.l. Ici, nous étudions des espaces de suites et nous utilisons la structure d'espace vectoriel de l'ensemble des suites à valeurs dans $\mathscr{K}$.

1. Nous considérons l'ensemble $\mathscr{K}[X]$ des polynômes à coefficients dans $\mathscr{K}$ et l'ensemble $\mathscr{K}[[X]]$ des séries formelles sur $\mathscr{K}$, tous deux avec leur structure de $\mathscr{K}$-espace vectoriel. Nous identifierons implicitement $\mathscr{K}[X]$ à l'espace $\mathscr{K}^{(\mathbf{N})}$ des suites à valeurs dans $\mathscr{K}$ ultimement nulles et $\mathscr{K}[[X]]$ à l'espace $\mathscr{K}^{\mathbf{N}}$ des suites quelconques à valeurs dans $\mathscr{K}$ (rappelons que $\mathscr{K}^{\mathbf{N}}$ est le dual linéaire de $\mathscr{K}^{(\mathbf{N})}$).

2. Etant donné une s.r.l. ξ, l'ensemble de toutes les échelles de récurrence qu'elle vérifie est un idéal de l'anneau $\mathscr{K}[X]$ il admet donc un générateur unitaire unique que l'on appelle le *polynôme minimal* de ξ. On appellera *rang* de ξ le degré du polynôme précédent. Evidemment, une suite d'ordre m

possède un rang au plus égal à m (contrairement au rang, l'ordre d'une s.r.l. fixée n'est pas défini de manière unique).

3. Soit G un polynôme fixé à coefficients dans $\mathscr{K}$. On écrira encore

$$G(X) = X^m - a_{m-1} X^{m-1} - \ldots - a_0 = \prod_{i=1}^{k} (X-\omega_i)^{r_i},\ \omega_i \in \mathscr{L}\ .$$

Nous considérons l'ensemble S_G de toutes les s.r.l. d'échelle G. Un élément ξ de S_G est uniquement déterminé par ses m premiers termes $\xi_0, \xi_1, \ldots, \xi_{m-1}$; chaque autre terme ξ_n dépend linéairement de ceux-ci. Il en résulte que S_G est un sous-espace vectoriel de dimension m de $\mathscr{K}^{\mathbf{N}}$. Les m éléments $\xi^{(i)} = (\xi_n^{(i)})_{n\geqslant 0}$, $i = 0, \ldots, m-1$, constituent une base de S_G si et seulement si le déterminant

$$\det\left((\xi_j^{(i)})\ 0 \leqslant i, j \leqslant m-1\right)$$

est non nul.

Suivant les cas, il est utile de prendre une base de S_G de l'un des types suivants:

a) la base constituée par les s.r.l. dites *fondamentales*

$$\zeta^{(i)} = (\zeta_n^{(i)})_{n\geqslant 0},\ i = 0, \ldots, m-1$$

définies par les conditions initiales $\zeta_j^{(i)} = \delta_j^i$, $0 \leqslant j \leqslant m-1$ (δ_j^i est le symbole de Kronecker, $\delta_j^i = 1$ si $i = j$ et 0 sinon). Sur cette base, un élément ξ de S_G s'écrit tout simplement

$$\xi = \xi_0\, \zeta^{(0)} + \ldots + \xi_{m-1}\, \zeta^{(m-1)}\ ; \tag{8}$$

b) la base formée par les suites

$$(\omega_i^n)_{n\geqslant 0},\ \left(\binom{n}{1}\, \omega_i^{n-1}\right), \ldots, \left(\binom{n}{r_i-1}\, \omega_i^{n-r_i+1}\right)_{n\geqslant 0},\ i = 1, \ldots, k\ ,$$

ce qui correspond aux formules (3) et (4);

c) enfin une base de la forme $\varphi, E\varphi, \ldots, E^{m-1}\varphi$ où φ est une s.r.l. quelconque admettant G comme polynôme minimal (par exemple les suites $\zeta^{(0)}$ et $\zeta^{(m-1)}$ de la base a)).

4. Si à une suite $\xi = (\xi_n)_{n\geqslant 0}$ quelconque, on associe la *matrice de Hankel*

$$H(\xi) = \begin{pmatrix} \xi_0 & \xi_1 & \xi_2 & \ldots & \xi_n & \ldots \\ \xi_1 & \xi_2 & \xi_3 & \ldots & \xi_{n+1} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \xi_p & \xi_{p+1} & \xi_{p+2} & \ldots & \xi_{n+p} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix} \tag{9}$$

alors on vérifie facilement que

(i) la suite ξ est une s.r.l. si et seulement si il existe un entier m tel que tout mineur d'ordre plus grand que m extrait de $H(\xi)$ soit nul;

(ii) si ξ est une s.r.l. de rang m alors son polynôme minimal est donné par le déterminant

$$G(X) = \begin{vmatrix} 1 & X & X^2 & \dots & X^m \\ \xi_0 & \xi_1 & \xi_2 & \dots & \xi_m \\ \xi_1 & \xi_2 & \xi_3 & \dots & \xi_{m+1} \\ \dots & \dots & \dots & \dots & \dots \\ \xi_{m-1} & \xi_m & \xi_{m+1} & \dots & \xi_{2m-1} \end{vmatrix} \tag{10}$$

5. De (5) résulte, comme nous l'avons déjà observé, que chaque élément de S_G admet un multiple quelconque de G comme polynôme caractéristique; autrement dit, l'espace S_G est l'orthogonal de l'idéal (G) engendre par G (regardé en tant que sous-espace de $\mathscr{K}[X]$):

$$S_G = (G)^{\perp} . \tag{11}$$

La dualité sous-entendue dans la formule précédente peut être décrite de manière plus explicite. Identifions la variable X à l'application linéaire

$$\begin{aligned} \text{« } X \text{ »}: \mathscr{K}[X] &\to \mathscr{K}[X] \\ A(X) &\mapsto X \,.\, A(X) \end{aligned}$$

(tout simplement la multiplication par X); alors l'application duale est l'opérateur de décalage E. Ainsi, à l'application de multiplication par $G(X)$: $A(X) \mapsto G(X)\, A(X)$ — dont l'image est (G) — correspond par dualité l'opérateur $G(E)$ — dont le noyau est S_G. La relation $(\mathrm{Im} f)^{\perp} = \mathrm{Ker} f^*$, valable pour une application linéaire quelconque f de duale f^*, équivaut à la relation (11) dans le cas considéré.

6. Le lien que nous avons indiqué entre le sous-espace S_G et l'idéal (G) peut être étendu en un lien entre l'espace S de toutes les s.r.l. et l'espace $\mathscr{K}[X]$, ceci en ayant recours à la notion de *bialgèbre.*

Une étude détaillée de la structure usuelle de bialgèbre sur $\mathscr{K}[X]$ et de sa bialgèbre duale est contenue en [51]. Pour un développement général sur la structure de bialgèbre et de coalgèbre, nous renvoyons à [59] et [1]. Pour la commodité du lecteur, nous indiquons ici les notions utilisées dans le présent article.

Nous noterons par V un espace vectoriel sur $\mathscr{K}$ et par $(b^{(i)})$, ou plus simplement (b^i), une base de cet espace. On considère ici une structure d'algèbre comme un triplet $\mathscr{A} = (V, m, n)$ avec la condition que l'application linéaire

$$m: V \otimes V \to V$$
$$b^i \otimes b^j \mapsto \sum_h t^{ij}\, b^h$$

[autrement dit, m correspond à la multiplication et on a $b^i b^j = \sum_h t_h^{ij}\, b^h$]

et le plongement

$$u: \mathscr{K} \to V$$
$$1 \mapsto \Sigma\, e_i\, b^i$$

rendent commutatifs les diagrammes

$$\begin{array}{ccc} V \otimes V \otimes V & \xrightarrow{I \otimes m} & V \otimes V \\ \downarrow{\scriptstyle m \otimes I} & & \downarrow{\scriptstyle m} \\ V \otimes V & \xrightarrow{m} & V \end{array}$$

et

$$\begin{array}{ccccc} \mathscr{K} \otimes V & \xrightarrow{u \otimes I} & V \otimes V & \xrightarrow{I \otimes u} & V \otimes \mathscr{K} \\ & \searrow & \downarrow{\scriptstyle m} & \swarrow & \\ & & V & & \end{array}$$

(Le premier diagramme exprime tout simplement l'associativité de la multiplication; dans le second — qui ne fait que traduire que u est unité — les flèches doubles représentent les isomorphismes canoniques). En termes des constantes de structure, ces conditions s'expriment par les formules

$$\sum_h t_h^{ij}\, t_k^{hl} = \sum_h t_h^{jl}\, t_k^{ih}$$

et

$$\sum_i e_i\, t_h^{ij} = \sum_i e_i\, t_h^{ji} = \delta_h^j \text{(le symbole de Kronecker).}$$

La définition d'une coalgèbre $\mathscr{C} = (V, \Delta, \varepsilon)$ s'obtient par dualisation de la précédente; maintenant les deux applications linéaires

$$\Delta : V \to V \otimes V \quad \text{(diagonalisation ou comultiplication)}$$
$$b^h \mapsto \sum_{i,j} \tau_{ij}^h \, b^i \otimes b^j$$

et

$$\varepsilon : V \to \mathscr{K} \qquad \text{(counité)}$$
$$b^h \mapsto \varepsilon^h$$

doivent rendre commutatifs les diagrammes

$$\begin{array}{ccc} V & \xrightarrow{\Delta} & V \otimes V \\ \Delta \downarrow & & \downarrow \Delta \otimes I \\ V \otimes V & \xrightarrow{I \otimes \Delta} & V \otimes V \otimes V \end{array} \qquad \text{(coassociativité)}$$

et

$$\begin{array}{ccccc} \mathscr{K} \otimes V & \xleftarrow{\varepsilon \otimes I} & V \otimes V & \xrightarrow{I \otimes \varepsilon} & V \otimes \mathscr{K} \\ & \searrow & \uparrow \Delta & \swarrow & \\ & & V & & \end{array}$$

(On renverse les flèches des diagrammes précédents.)

Une application $f : V \to V$ est un morphisme d'algèbre (resp. de coalgèbre) si elle est linéaire et vérifie $f \circ m = m \circ (f \otimes f)$ et $f \circ u = u$ (respectivement: $\Delta \circ f = (f \otimes f) \circ \Delta$ et $\varepsilon \circ f = \varepsilon$).

A chaque coalgèbre $\mathscr{C} = (V, \Delta, \varepsilon)$ est associée son algèbre duale $\mathscr{C}^* = (V^*, \Delta^*, \varepsilon^*)$, où V^* est le dual linéaire de V et Δ^*, ε^* les applications linéaires respectivement duales de Δ et ε. Sur la (pseudo-)base (b_i) duale de (b^i), i.e. $b_i(b^j) = \delta_i^j$, les constantes de l'algèbre $\mathscr{C}^*$ coïncident avec celles de $\mathscr{C}$.

Le passage de l'algèbre $\mathscr{A} = (V, m, n)$ à sa coalgèbre duale $\mathscr{A}^\circ = (V^\circ, m^\circ, u^\circ)$ est défini d'une manière analogue en dimension finie (on a alors $V^\circ = V^*, m^\circ = m^*$ et $u^\circ = u^*$); par contre, si la dimension de V est infinie, alors l'ensemble V° sous-jacent à $\mathscr{A}^\circ$ est un sous-ensemble strict de V^* [car $m^* : V^* \to (V \otimes V)^*$ mais $V^* \otimes V^* \subset (V \otimes V)^*$]. Il est bien connu

qu'on doit prendre pour V° l'espace des *fonctions linéaires représentatives*, c'est-à-dire des formes linéaires $f: V \to \mathscr{K}$ telles que Ker f contienne un idéal J de V de codimension finie.

La structure $\mathscr{B} = (V, m, \Delta, u, \varepsilon)$ est une *bialgèbre* si (V, m, u) est une algèbre, (V, Δ, ε) une coalgèbre et si Δ et ε sont des morphismes d'algèbre (ou, ce qui est équivalent, si m et u sont des morphismes de coalgèbre). Ceci se traduit évidemment en termes de constantes de structures (voir [16], formule (5) à (8)).

Le passage à la bialgèbre duale $\mathscr{B}^\circ = (V^\circ, \Delta^\circ, m^\circ, \varepsilon^\circ, u^\circ)$ ne représente pas de problème puisque $\Delta^*(V^\circ \otimes V^\circ) \subseteq V^\circ$ (Δ° et ε° sont définies respectivement comme les restrictions à V° de Δ^* et ε^*).

En ce qui nous concerne, les deux exemples suivants sont fondamentaux.

1) L'espace vectoriel $\mathscr{K}[X]$ des polynômes possède une structure naturelle de bialgèbre $\mathscr{B} = \mathscr{K}[X], m, \Delta, u, \varepsilon)$ dont les applications linéaires sont définies par

$$m(X^i \otimes X^j) = X^{i+j}, \quad \Delta(X) = X \otimes 1 + 1 \otimes X,$$
$$u(1) = 1 \quad \text{et} \quad \varepsilon(X^i) = \delta_0^i \quad \text{(le symbole de Kronecker)}.$$

Plus simplement: m est la multiplication usuelle des polynômes, Δ associe à $P(X)$ le polynôme $P(X+Y)$ [ici on identifie $X^i \otimes X^j$ à $X^i Y^j$] et enfin ε associe à $P(X)$ son terme constant $P(0)$.

2) L'espace S de toutes les s.r.l. possède lui aussi une structure naturelle de bialgèbre $\mathscr{S} = (S, \tilde{m}, \tilde{\Delta}, \tilde{u}, \tilde{\varepsilon})$

$$\tilde{u}: \mathscr{K} \to S, \quad 1 \mapsto (\delta_n^0)_{n \geq 0}$$
$$\tilde{\varepsilon}: S \to \mathscr{K}, \quad (\xi_n)_{n \geq 0} \mapsto \xi_0$$
$$\tilde{m}: S \otimes S \to S, \quad \xi \otimes \eta \mapsto \xi * \eta$$
(c'est le produit défini en A II 5))

et

$$\tilde{\Delta}: S \to S \otimes S, \quad \xi \mapsto H(\xi)$$

(dans ce dernier cas on identifie $\mathscr{K}^{\mathbf{N}} \otimes \mathscr{K}^{\mathbf{N}}$ avec l'espace des matrices infinies de type $\omega \times \omega$ et $H(\xi)$ désigne la matrice de Hankel de ξ).

Le lien entre les structures ci-dessus est fourni par le résultat fondamental suivant [51]:

THÉORÈME (Peterson-Taft, 1980). *La bialgèbre $\mathscr{S}$ des s.r.l. est la bialgèbre duale de celle des polynômes.*

IV.

Dans ce paragraphe nous montrons comment la théorie des s.r.l. permet d'obtenir des algorithmes utiles pour la résolution de certains problèmes algébriques et numériques relatifs à $\mathscr{K}[X]$. Le contenu de la fin du paragraphe précédent fournit une justification théorique générale à la méthode utilisée ici.

En général, nous utiliserons sans les rappeler les notations introduites plus haut.

1. *Quelques problèmes d'élimination*

Premier problème. Soient donnés $n+2$ polynômes $G_i(X_i)$, $i = 0, ..., n$, et $Z = Z(X_0, ..., X_n)$; déterminer — rationnellement en fonction des coefficients des G_i et de Z — un polynôme $G(X)$ dont les racines sont toutes les valeurs $Z(\omega_{0,j_0}, \omega_{1,j_1}, ..., \omega_{n,j_n})$ où les ω_{i,j_i} parcourent les racines de G_i.

Algorithme 1. Il comporte les pas suivants:

a) construire $n+1$ s.r.l. $\xi^{(i)}$, où $\xi^{(i)}$ admet G_i comme polynôme minimal;

b) construire la s.r.l. $\eta = (\eta_m)_{m \geqslant 0}$ donné par

$$\eta_m = \sum_{m_0, ..., m_n} Z^{(m)}_{m_0 ... m_n} \xi^{(0)}_{m_0} \xi^{(1)}_{m_1} ... \xi^{(n)}_{m_n}$$

où on a posé

$$[Z(X_0, ..., X_n)]^m = \sum_{m_0 ... m_n} Z^{(m)}_{m_0 ... m_n} X_0^{m_0} ... X_n^{m_n}$$

c) le polynôme cherché est l'échelle de la suite η et on peut le calculer grâce à la formule (10).

Second problème. Il s'agit d'une généralisation du précédent. Soient $n+1$ polynômes $G_i(X_i)$, $i = 1, ..., n$ et $Z(X_0, ..., X_n)$, déterminer rationnellement un polynôme $H(Y)$ ayant pour racines toutes les valeurs ω_j satisfaisant à une équation du type

$$Z(\omega_j; \omega_{1,j_1}, ..., \omega_{n,j_n}) = 0$$

les ω_{i,j_i} parcourant encore l'ensemble des racines de G.

Algorithme 2.

a) Posons $G_0(X_0) = X_0 - Y$; on utilise l'algorithme 1 pour déterminer le polynôme $G(X)$ (Y étant considéré momentanément comme une constante);

b) le polynôme $H(Y)$ cherché est donné par le terme constant de $G(X)$. (Cf. [19].)

2. *Résultant et p.p.c.m. des polynômes $F(X)$ et $G(X)$*

Soient $\eta^{(i)}$, $i = 1, ..., l$, et $\xi^{(j)}$, $j = 1, ..., m$ des bases pour les espaces S_F et S_G et soit

$$A = \begin{pmatrix} \eta_1^{(1)} & \cdots & \eta_{l+m}^{(1)} \\ \cdots & & \\ \eta_1^{(l)} & \cdots & \eta_{l+m}^{(l)} \\ \cdots & & \\ \xi^{(1)} & \cdots & \xi_{l+m}^{(1)} \\ \cdots & & \\ \xi^{(m)} & \cdots & \xi_{l+m}^{(m)} \end{pmatrix}.$$

Le déterminant de A est égal au résultant de F et G, à une constante multiplicative non nulle près. [Preuve: $S_F \cap S_G \neq \{0\}$ ssi $\det A = 0$.]

De plus, si s est le rang de la matrice A et si $i_1, ..., i_{s-l}$ sont des indices tels que les s.r.l. $\eta^{(1)}, ..., \eta^{(l)}, \xi^{(i_1)}, ..., \xi^{(i_{s-l})}$ soient linéairement indépendantes, le p.p.c.m. de F et G est donné par le déterminant dont la première ligne est $1, X, ..., X^s$ et dont les autres sont les $s + 1$ premières valeurs des suites précédentes. (Voir aussi [12].)

3. *Division par un polynôme $G(X)$ fixé*

Les applications r et q de $\mathscr{K}[X]$ dans lui-même qui associent au polynôme quelconque $P(X)$ son reste $r(P)$ et son quotient $q(P)$ dans la division euclidienne par $G(X)$: $P = G \,.\, q(P) + r(P)$, sont linéaires et donc représentables par des matrices R_G et Q_G de type (ω, ω). Ces matrices peuvent être facilement décrites en termes de s.r.l.; en effet, la première est la matrice ayant pour ses $m = \deg(G)$ premières lignes les s.r.l. fondamentales $\zeta^{(0)}, ..., \zeta^{(m-1)}$ d'échelle G et les autres nulles (par commodité on supprime ces dernières), tandis que la seconde est formée par la seule $\zeta^{(m-1)}$ (précédée, dans la s-ième ligne, par $s + 1$ termes nuls; $s = 0, 1, 2, ...$)

$$R_G = \begin{pmatrix} 1 & 0 \ldots 0, & \zeta_m^{(0)} & , & \zeta_{m+1}^{(0)} & , & \cdots \\ 0 & 1 \ldots 0, & \zeta_m^{(1)} & , & \zeta_{m+1}^{(1)} & , & \cdots \\ \cdots & & & & & & \\ 0 & 0 \ldots 1, & \zeta_m^{(m-1)} & , & \zeta_{m+1}^{(m-1)} & , & \cdots \end{pmatrix}$$

$$Q_G = \begin{pmatrix} 0 & 0 \ldots 0, & 1, & \zeta_m^{(m-1)}, & \zeta_{m+1}^{(m-1)}, & \zeta_{m+2}^{(m-1)} & \ldots \\ 0 & 0 \ldots 0, & 0, & 1 \quad , & \zeta_m^{(m-1)}, & \zeta_{m+1}^{(m-1)} & \ldots \\ 0 & 0 \ldots 0, & 0, & 0 \quad , & 1 \quad , & \zeta_m^{(m-1)} & \ldots \\ \ldots\ldots & & & & & & \\ \ldots\ldots & & & & & & \end{pmatrix}$$

La matrice R_G du reste fournit diverses autres informations sur le polynôme $G(X)$. A titre d'exemple citons les suivantes:

a) la matrice formée avec les colonnes j-ième, ..., $(j+m-1)$-ième de R_G est la puissance j-ième M^j de la matrice-compagnon M du polynôme $G(X)$;

b) la suite des sommes diagonales des entrées de R_G est la suite des sommes des puissances des racines des G:

$$\zeta_n^{(0)} + \zeta_{n+1}^{(1)} + \ldots + \zeta_{n+m-1}^{(m-1)} = r_1 \omega_1^n + \ldots + r_m \omega_k^n = \text{Trace de } M^n$$

(ceci équivaut à la formule de Newton);

c) si on donne encore un polynôme $F(X)$, le déterminant de la matrice $F(M)$ — qui peut être calculé en utilisant a) — est la forme de Kronecker pour le résultant des polynômes G et F (cf. [13]).

4. *Recherche des diviseurs quadratiques d'un polynôme*

Dans ce paragraphe on considère des polynômes à coefficients réels.

Notons par $\Phi(u, v)$ et $\Psi(u, v)$ deux fonctions réelles qui s'annulent au point (u_0, v_0) et par (u, v) un point voisin de (u_0, v_0) et rappelons que la méthode de Newton donne les expressions

$$(12) \qquad h(u,v) = \frac{\Psi \dfrac{\partial \Phi}{\partial v} - \Phi \dfrac{\partial \Psi}{\partial v}}{\dfrac{\partial \Phi}{\partial u}\dfrac{\partial \Psi}{\partial v} - \dfrac{\partial \Phi}{\partial v}\dfrac{\partial \Psi}{\partial u}}, \qquad k(u,v) = \frac{\Phi \dfrac{\partial \Psi}{\partial u} - \Psi \dfrac{\partial \Phi}{\partial u}}{\dfrac{\partial \Phi}{\partial u}\dfrac{\partial \Psi}{\partial v} - \dfrac{\partial \Phi}{\partial v}\dfrac{\partial \Psi}{\partial u}}$$

pour les corrections à apporter à u et v, respectivement, afin d'obtenir une meilleure approximation.

La méthode de Bairstow pour la recherche des valeurs approchées des coefficients d'un facteur quadratique $G_0(X) = X^2 - u_0 X - v_0$ d'un polynôme donné $P(X) = b_n X^n + \ldots + b_0$ fait usage de (12) relativement aux fonctions $\Phi(u, v)$ et $\Psi(u, v)$ telles que

$$R(X) = \alpha(n, v) + \beta(u, v)X = \Phi(u, v)X + \big(\Psi(u, v) - u\Phi(u, v)\big)$$

soit le reste de la division de $P(X)$ par un polynôme $G(X) = X^2 - uX - v$ proche de $G_0(X)$. Ce choix de Φ et Ψ trouve sa justification dans le fait

qu'on peut alors exprimer — grâce à l'algorithme connu sous le nom de « division synthétique » — les valeurs en (u, v) de ces fonctions et de leurs dérivées partielles premières et donc appliquer les formules (12).

Cependant — en calculant $R(X)$ par la méthode exposée en 3) — il est facile de vérifier que ces conditions sont satisfaites par des fonctions plus générales Φ et Ψ obtenues comme combinaisons linéaires indépendantes arbitraires des coefficients du reste

$$R(X): \Phi(u, v) = \Phi_1\alpha(u, v) + \Phi_2\beta(u, v),\ \Psi(u, v) = \Psi_1\alpha(n, v) + \Psi_2\beta(u, v)$$

(où les coefficients Φ_i et Ψ_i peuvent dépendre ou non des paramètres u, v et vérifient $\Phi_1\Psi_2 - \Phi_2\Psi_1 \neq 0$). De plus: grâce à la linéarité de notre algorithme et à quelques propriétés élémentaires des s.r.l., on peut opérer une transformation des formules (12) qui permet d'exprimer les corrections h et k sous forme de quotients de formes quadratiques sur un espace de dimension quatre évaluées au point $\hat{R} \,.\, P$, reste de P modulo G^2 (où on a posé $\hat{R} = R_{G^2}$):

$$(13)\quad h(u, v) = \frac{(\vec{\Psi} \,.\, \hat{R} \,.\, P)\left(\frac{\partial\vec{\Phi}}{\partial v} \,.\, \hat{R} \,.\, P\right) - (\vec{\Phi} \,.\, \hat{R} \,.\, P)\left(\frac{\partial\vec{\Psi}}{\partial v} \,.\, \hat{R} \,.\, P\right)}{\left(\frac{\partial\vec{\Phi}}{\partial u} \,.\, \hat{R} \,.\, P\right)\left(\frac{\partial\vec{\Psi}}{\partial v} \,.\, \hat{R} \,.\, P\right) - \left(\frac{\partial\vec{\Phi}}{\partial v} \,.\, \hat{R} \,.\, P\right)\left(\frac{\partial\vec{\Psi}}{\partial u} \,.\, \hat{R} \,.\, P\right)} = \frac{{}^t(\hat{R}P) \,.\, H \,.\, (\hat{R}P)}{{}^t(\hat{R}P) \,.\, L \,.\, (\hat{R}P)}$$

$$(13')\quad k(u, v) = \frac{(\vec{\Phi} \,.\, \hat{R} \,.\, P)\left(\frac{\partial\vec{\Psi}}{\partial u} \circ \hat{R} \,.\, P\right) - (\vec{\Psi} \,.\, \hat{R} \,.\, P)\left(\frac{\partial\vec{\Phi}}{\partial u} \,.\, \hat{R} \,.\, P\right)}{{}^t(\hat{R}P) \,.\, L \,.\, (\hat{R}P)} = \frac{{}^t(\hat{R}P) \,.\, K \,.\, (\hat{R}P)}{{}^t(\hat{R}P) \,.\, L \,.\, (\hat{R}P)}$$

où $\vec{\Phi} = \left(\Phi_1, \Phi_2, \Phi_3 = v\Phi_1 + u\Phi_2, \Phi_4 = uv\Phi_1 + (u^2 + v)\Phi_2\right)$ et $\vec{\Psi}$ est un vecteur avec une expression analogue et où H, K, L sont des matrices 4×4 données par

$$H = \vec{\Psi} * \frac{\partial\vec{\Phi}}{\partial v} - \vec{\Phi} * \frac{\partial\vec{\Psi}}{\partial v}, \qquad K = \vec{\Phi} * \frac{\partial\vec{\Psi}}{\partial u} - \vec{\Psi} * \frac{\partial\vec{\Phi}}{\partial u},$$

$$L = \frac{\partial\vec{\Phi}}{\partial u} * \frac{\partial\vec{\Psi}}{\partial v} - \frac{\partial\vec{\Phi}}{\partial v} * \frac{\partial\vec{\Psi}}{\partial u}$$

ayant noté par $(x_1, x_2, x_3, x_4) * (y_1, y_2, y_3, y_4)$ la matrice de coefficients $z_{ij} = \frac{1}{2}(x_i y_j + x_j y_i)$.

Nous soulignons que la complication des formules précédentes est purement apparente. Ainsi, par exemple, si on choisit $\Phi = \beta$ et $\Psi = \alpha + u\beta$ comme dans la méthode de Bairstow, (13) et (13′) deviennent

$$h(u, v) = \frac{u(x_1)^2 - ux_1x_2 + x_0x_3 - x_1x_2}{(x_1)^2 - x_0x_2}$$

$$k(u, v) = \frac{v(x_1)^2 + (x_2)^2 - vx_0x_2 - x_1x_3}{(x_1)^2 - x_0x_2}$$

où $x_i = b_0\sigma_i + b_1\sigma_{i+1} + \ldots + b_n\sigma_{i+n}$, (σ_i) étant la quatrième des s.r.l. fondamentales associées à G^2.

On remarque encore que cette méthode peut être reprise presque telle quelle dans la recherche des corrections $\tilde{h}(t, \rho)$ et $\tilde{k}(t, \rho)$ relatives au cosinus t de l'argument et au module ρ des racines de $G = X^2 - nX - v = X^2 - 2\rho tX + \rho^2$, enfin on peut facilement généraliser l'algorithme au cas des diviseurs de degré supérieur à deux (cf. [18]).

5. *Recherche approchée des racines d'un polynôme*

L'algorithme qu'on réfère ici contient comme cas particulier celui de Bernoulli et, dans le sens précisé à la fin de ce paragraphe, l'algorithme de Aitken et le Q.D. algorithme (cf. [23], [29]).

Soit $\xi = (\xi_n)$ une s.r.l. ayant $G(X)$ pour polynôme minimal (par exemple, $\xi = \zeta^{(1)}$ ou $\xi = \zeta^{(m)}$). On pose $G(X) = \prod_{i=1}^{m} (X - \rho_i)$ avec $|\rho_1| \geqslant \ldots \geqslant |\rho_m|$, sans exclure le cas de racines multiples. On considère la matrice formée par les m premières lignes de la matrice de Hankel $H(\xi)$ et ses mineurs d'ordre j

$$H_{j,n} = \begin{vmatrix} \xi_n & \xi_{n+1} & \cdots & \xi_{n+j-1} \\ \cdots & \cdots & \cdots & \cdots \\ \xi_{n+j-1} & \xi_{n+j} & \cdots & \xi_{n+2j-2} \end{vmatrix}, \quad n \geqslant 0.$$

On construit ensuite, pour chaque $j \leqslant m$, la suite $\theta_j = (\theta_{j,n})_{n \geqslant 0}$ où $\theta_{j,n} = H_{j,n+1}/H_{j,n}$. On distingue les deux cas suivants:

Cas (I_j): La suite $(\theta_{j,n})_{n \geqslant 0}$ converge et alors sa limite est égale au produit des j premières racines de G et $|\rho_j| > |\rho_{j+1}|$. Si ça arrive pour chaque j

on obtient ainsi successivement les produits $\rho_1, \rho_1\rho_2, ..., \rho_1\rho_2 ... \rho_j$ et donc chacune des ρ_i.

Cas (II_j): Si la suite θ_j ne converge pas alors $|\rho_j| = |\rho_{j+1}|$. Si, plus précisément, on a la suite d'éventualités: $(I_s), (II_{s+1}), ... (II_{s+t-1}), (I_{s+t})$, alors

$$|\rho_s| > |\rho_{s+1}| = ... = |\rho_{s+t}| > |\rho_{s+t+1}|$$

et

$$\frac{\lim\limits_{n\to\infty} \Theta_{s+t,n}}{\lim\limits_{n\to\infty} \Theta_{s,n}} = \frac{\rho_1\rho_2 \cdots \rho_{s+t}}{\rho_1\rho_2 \cdots \rho_s} = \rho_{s+1}\,\rho_{s+2} \cdots \rho_{s+t}\,.$$

(Un cas particulier apparaît en [39]).

Cet algorithme doit être précisé (voir [17]) dans les deux cas suivants:

a) la suite $(H_{j,n})_{n\geqslant 0}$ contient des termes nuls;

b) $G(X)$ admet au moins un couple de racines réelles et opposées sans avoir d'autres racines du même module que celles-ci.

Remarquons qu'on peut calculer les déterminants de Hankel $H_{j,n}$ à l'aide de la relation de récurrence bien connue

$$H_{j,n}\,H_{j,n+2} - H_{j+1,n}\,H_{j-1,n+2} = (H_{j,n+1})^2\,.$$

Notons enfin que:

i) Si au lieu de $G(X)$ on utilise $\tilde{G}(X)$, le polynôme quadratfrei qui a les mêmes racines que G, et la s.r.l. associée introduite en 3.b) (dont le polynôme minimal est précisément $\tilde{G}$) alors notre algorithme se réduit à celui de Aitken.

ii) Rappelons que le Q.D.-schéma utilise les suites $e_n^{(j)}, q_n^{(j)}, j, n \geqslant 0$, construites en utilisant les relations de récurrence

$$(14)\qquad e_n^{(j)} = (q_{n+1}^{(j)} - q_n^{(j)}) + e_{n+1}^{(j-1)}, \qquad q_n^{(j+1)} = q_{n+1}^{(j)}\,(e_{n+1}^{(j)}/e_n^{(j)})\,.$$

Notre algorithme donne la formule explicite suivante:

$$(15)\qquad e_n^{(j)} = \frac{H_{j+1,n}\,H_{j-1,n+1}}{H_{j,n}\,H_{j,n+1}}, \qquad q_n^{(j)} = \frac{H_{j,n+1}\,H_{j-1,n}}{H_{j,n} - H_{j-1,n+1}}\,.$$

Contrairement à ce qui peut se produire avec la formule (14), ces dernières formules permettent dans tous les cas de poursuivre la construction du schéma Q.D.; en effet, s'il se présente un zéro dans la suite $(\theta_{j,n})$, cela n'empêche pas de calculer les $\theta_{j',n}$ pour $j' > j$. De plus, les formules (15)

ramènent le problème de la recherche de conditions nécessaires et suffisantes pour l'existence du Q.D.-schéma à celui de la distribution des zéros dans les s.r.l. $H_{j,n}$. (Ce problème — relativement à une s.r.l. arbitraire — a été étudié en [6].)

B. ÉTUDE ARITHMÉTIQUE

> La théorie des suites récurrentes est une mine inépuisable qui renferme toutes les propriétés des nombres; en calculant les termes consécutifs de telles suites, en décomposant ceux-ci en facteurs, en recherchant par l'expérimentation les lois de l'apparition et de la reproduction des nombres premiers, on fera progresser d'une manière systématique l'étude des propriétés des nombres et de leurs applications dans toutes les branches des Mathématiques.
>
> Edouard LUCAS *(Théorie des Nombres)*

I. MÉTHODES ÉLÉMENTAIRES

1. *Propriétés de périodicité*

Le premier résultat de ce type est dû à Lagrange, la proposition suivante est essentiellement due à Carmichael.

PROPOSITION. *Soit* ξ *une suite à valeurs dans un anneau* $\mathscr{A}$ *et vérifiant la relation de récurrence linéaire (à coefficients dans* $\mathscr{A}$*)*

$$\xi_{n+k} = a_{k-1}\,\xi_{n+k-1} + a_{k-2}\,\xi_{n+k-2} + \ldots + a_0\,\xi_n, n \geqslant 0\,.$$

On suppose que ξ *ne prend qu'un nombre fini de valeurs; alors* ξ *est ultimement périodique. De plus, lorsque* a_0 *n'est pas un diviseur de zéro, la suite* ξ *est purement périodique.*

Considérons la suite $(\xi_n, \xi_{n+1}, \ldots, \xi_{n+k-1})_{n\geqslant 0}$ des k-uples de valeurs successives de ξ. Si ξ ne prend qu'un nombre fini de valeurs alors ces k-uples ne prennent aussi qu'un nombre fini de valeurs, il existe donc $n_0 \geqslant 0$ et $t > 0$ tels que

$$(\xi_n, \xi_{n+1}, \ldots, \xi_{n+k-1}) = (\xi_{n+1+t}, \ldots, \xi_{n+t+k-1}) \quad \text{pour} \quad n = n_0\,.$$

Grâce à la relation de récurrence cette égalité reste vraie pour tout $n \geqslant n_0$ et on a donc $\xi_{n+t} = \xi_n$ pour $n \geqslant n_0$. C'est la première assertion.

Supposons en outre a_0 non diviseur de zéro et que n_0 a été choisi minimal. Si on a $n_0 \geqslant 1$ alors la relation de récurrence montre que