SUITES RÉCURRENTES LINÉAIRES Propriétés algébriques et arithmétiques

Autor(en): **Cerlienco, L. / Mignotte, M. / Piras, F.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **33 (1987)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **01.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-87887

L'Enseignement Mathématique, t. 33 (1987), p. 67-108

SUITES RÉCURRENTES LINÉAIRES
PROPRIÉTÉS ALGÉBRIQUES ET ARITHMÉTIQUES

par L. CERLIENCO [1]), M. MIGNOTTE [2]) et F. PIRAS [1])

INTRODUCTION

Les suites récurrentes linéaires sont nées en 1202 avec l'exemple donné par Fibonacci [25] de la suite 1, 1, 2, 3, 5, 8, 13 ... . De ce fait une littérature très abondante leur a été consacrée et il est pratiquement impossible de réaliser une bibliographie à peu près complète sur ce sujet. Leur grand âge a encore pour conséquence fâcheuse que les suites récurrentes linéaires sont considérées comme des choses vieillotes, voire peu intéressantes. Cet article a pour but de montrer que l'étude de ces suites est encore active et pose certains problèmes fascinants — par exemple celui de savoir si une suite récurrente linéaire donnée possède ou non un zéro (plus précisément de construire un algorithme répondant à la question — ou de prouver qu'un tel algorithme général n'existe pas).

Ce travail est partagé en deux parties, l'étude des propriétés algébriques puis celle des propriétés arithmétiques. Chacune de ces parties comporte une collection d'exemples qui montrent les nombreux liens qui existent entre les suites récurrentes linéaires et des domaines mathématiques très variés. Nous ne voulons pas recopier ici la liste de toutes les questions qui sont abordées dans la suite; il nous semble plus intéressant de citer quelques exemples importants mais qui ne sont pas traités ici. Auparavant nous tenons à souligner que les choix que nous avons dus faire sont en grande partie subjectifs et reflètent à l'évidence les intérêts des auteurs.

Voici donc une liste (sans doute incomplète) de sujets importants où interviennent encore les suites récurrentes linéaires.

A.M.S. Subject Classification: 10 A 35.
Mots-Clés: Suites récurrentes linéaires.
[1]) Travail partiellement financé par les « Fondi ministeriali per la Ricerca 40% e 60% ».
[2]) Travail réalisé durant un séjour à Cagliari comme « Professore a conttrato ».

En informatique, les suites récurrentes linéaires interviennent dans divers domaines théoriques ou pratiques. Elles apparaissent d'abord comme un objet fondamental en théorie des langages; elles interviennent directement dans l'étude des morphismes itérés sur un monoïde (DOL-systems... voir [5]) et la théorie des séries rationnelles en variables non commutatives — sujet fondé essentiellement par M. P. Schützenberger — en est une généralisation naturelle et féconde (voir [7]). L'étude de la période d'une suite récurrente linéaire à valeurs dans un corps fini est à peine effleurée ici, alors qu'il s'agit d'un problème essentiel pour l'utilisation des suites récurrentes linéaires dans le domaine des communications (voir [27] ou [34]), elles correspondent au fonctionnement des registres à décalage (shift-registers).

Parmi les nombreuses propriétés arithmétiques des suites récurrentes linéaires, plusieurs ne sont pas traitées ici. Par exemple, les propriétés remarquables de divisibilité des suites de Lucas et de Lehmer; nous renvoyons le lecteur à l'article de Stewart [57], qui contient de nombreuses références, ainsi qu'à [28]. Une autre question, difficile, est celle de l'inversion du produit de Hadamard (i.e. étant données trois suites d'entiers (a_n), (b_n) et (c_n) telles que les suites (b_n) et (c_n) soient récurrentes linéaires et que $a_n b_n = c_n$ pour tout n, la suite (a_n) est-elle aussi récurrente linéaire?); Cantor a montré que c'est vrai lorsque la série formelle associée à (b_n) possède une seule singularité, puis G. Pathiaux [50] a étendu ce résultat au cas où cette série possède au plus deux singularités, nous ne connaissons pas de preuve satisfaisante du cas général.

Autre exemple bien connu, les réduites du développement en fraction continue des irrationnels quadratiques ont des numérateurs et des dénominateurs qui sont les termes de suites récurrentes linéaires, ainsi les dénominateurs de la suite des réduites du développement du nombre d'or $(1+\sqrt{5})/2$ sont les nombres de Fibonacci; cet exemple n'apparaît ici que sous la rubrique de l'équation de Pell-Fermat. Comme il est expliqué en [37], on peut aussi utiliser les suites récurrentes linéaires pour construire des algorithmes en théorie algébrique des nombres, c'est un peu la version arithmétique des algorithmes d'analyse numérique où les suites récurrentes linéaires sont utilisées pour obtenir des informations sur les racines d'un polynôme (voir la partie A.IV du présent article); pour un exposé très précis des algorithmes algébriques sur les polynômes voir le livre de Knuth [1]). Voici cependant un exemple extrait de [40]: étant donné un polynôme P sur un corps $\mathbf{F}_q$ fini, savoir si P se décompose en facteurs linéaires dans

[1]) The Art of Programming, Addison Wesley.

$\mathbf{F}_q$ — 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

$a_0(\xi_{n_0-1}-\xi_{n_0+t-1}) = 0$, ce qui implique $\xi_{n_0-1} = \xi_{n_0+t-1}$, formule qui contredit la minimalité de n_0. On a donc $n_0 = 0$, autrement dit la suite ξ est bien purement périodique. □

On peut en déduire une démonstration du théorème de Kronecker.

COROLLAIRE. *Soit* θ *un entier algébrique non nul dont tous les conjugués sont de module au plus* 1, *alors* θ *est une racine de l'unité.*

Soient $\theta_1 = \theta, \theta_2, ..., \theta_d$ les conjugués de θ et $X^d - a_{d-1}X^{d-1} - ... - a_0$ son polynôme minimal sur $\mathbf{Z}$. Pour n entier $\geqslant 0$ posons $\xi_n = \theta_1^n + \theta_2^n + ... + \theta_d^n$. Alors la suite (ξ_n) vérifie

$$\xi_{n+d} = a_{d-1}\xi_{n+d-1} + ... + a_0\xi_n, \quad n \geqslant 0,$$

de plus les ξ_n sont des entiers de l'intervalle $[-d, +d]$. Enfin a_0 est non nul, la proposition implique donc que (ξ_n) est purement périodique. Soit t la période, on a $\xi_t = \xi_0$; soit $\theta_1^t + ... + \theta_d^t = d$, et comme $|\theta_i| \leqslant 1$ pour $i = 1, ..., d$, $\theta^t = 1$. □

Le cas particulier de la proposition 1 le plus intéressant est celui où $\mathscr{A} = \mathbf{F}_p(=\mathbf{Z}/p\mathbf{Z})$, p étant (comme toujours !) un nombre premier. Considérons donc une série s.r.l. ξ à valeurs dans $\mathbf{F}_p$ et vérifiant

$$\xi_{n+k} = a_{k-1}\xi_{n+k-1} + ... + a_0\xi_n, \quad n \geqslant 0 \ (a_0, ..., a_{k-1} \in \mathbf{F}_p).$$

Soit $L = \mathbf{F}_{p^d}$ la plus petite extension de $\mathbf{F}_p$ dans laquelle le polynôme $G = X^k - a_{k-1}X^{k-1} - ... - a_0$ se décompose en facteurs linéaires. Alors ξ est ultimement périodique (purement périodique si $a_0 \neq 0$) et sa période est un diviseur de $p(p^d-1)$, ce qu'on voit en utilisant les formules (3) et (4) de A.I.2 [d'une part les ρ_j appartiennent à L^* et vérifient donc $\rho_j^{p^d-1} = 1$, d'autre part les coefficients du binôme modulo p admettent p comme période]; en outre si G n'a que des racines simples alors la période divise $p^d - 1$. Le cas des suites récurrentes linéaires binaires est très simple. L'entier d ne peut alors prendre que les valeurs 1 ou 2. Plus précisément, si ξ vérifie

$$\xi_{n+2} = a_1\xi_{n+1} + a_0\xi_n, \quad n \geqslant 0, \quad a_0, a_1 \in \mathbf{F}_p, \quad a_0 \neq 0,$$

posons $\Delta = a_1^2 + 4a_0$ et supposons p impair. Le symbole de Legendre permet de caractériser les cas $d = 1$ ou 2: on a

$$d = 2 \quad \text{si et seulement si} \quad \left(\frac{\Delta}{p}\right) = -1 .$$

Ainsi, on a les trois possibilités suivantes:

(i) Δ est un résidu quadratique modulo p, alors la période t divise $p-1$,

(ii) Δ n'est pas un résidu quadratique modulo p, alors t divise p^2-1,

(iii) $\Delta = 0$, alors t divise $p(p-1)$.

On peut raffiner l'assertion (ii) de la manière suivante. Supposons $\left(\frac{\Delta}{p}\right) = -1$. Soient ρ_1 et ρ_2 les racines du polynôme $X^2 - a_1X - a_0$ dans le corps $\mathbf{F}_{p^2}$ et soit σ l'automorphisme de Frobenius de ce corps $(\sigma(\alpha)=\alpha^p)$. On a d'une part

$$\xi_n = \alpha_1\rho_1^n + \alpha_2\rho_2^n , \quad \alpha_1, \alpha_2 \in L ,$$

et d'autre part

$$\rho_1^p = \rho_2 , \ \rho_2^p = \rho_1 \quad \text{et} \quad \rho_1\rho_2 = -a_0 .$$

D'où

$$\rho_1^{p+1} = \rho_2^{p+1} = \rho_1\rho_2 = -a_0 ,$$

ce qui prouve l'assertion suivante.

(ii)′ Soit e l'ordre de $-a_0$ dans le corps $\mathbf{F}_p$, alors si Δ n'est pas résidu quadratique modulo p, la période divise $e(p+1)$.

Exemple 1: Reprenons la suite de Fibonacci. On a alors,

$$F_{n+2} = F_{n+1} + F_n , \quad \Delta = 5 , \quad e = 2$$

et les trois cas précédents sont

(i) $p = 5k \pm 1$, la période divise $p-1$,

(ii) $p = 5k \pm 2$, la période divise $2(p+1)$ (c'est encore vrai pour $p = 2$)

(iii) $p = 5$, la période est égale à 20.

On en déduit aussitôt les propriétés de divisibilité suivantes:

si $p = 5k \pm 1$ alors p divise F_n lorsque $p-1$ divise n,

si $p = 5k \pm 2$ alors p divise F_n lorsque $p+1$ divise n,

[en effet, $F_n = \dfrac{\rho_1^n - \rho_2^n}{\rho_1 - \rho_2}$ donc $F_{p+1} = \dfrac{\rho_1\rho_2 - \rho_1\rho_2}{\rho_1 - \rho_2} = 0$],

enfin si $p = 5$ on vérifie directement que 5 divise F_n si et seulement si 5 divise n.

Exemple 2: Le critère de Lucas peut être obtenu comme corollaire de l'étude précédente. Soit $\omega = \dfrac{1+\sqrt{5}}{2}$ le nombre d'or. On considère la suite d'entiers $r_m = \omega^{2^m} + \omega^{-2^m}$, $m = 1, 2, 3, \ldots$, ainsi $r_m = 3, 7, 47, \ldots$, et on peut calculer aisément les r_m grâce à la relation évidente $r_{m+1} = r_m^2 - 2$. En fait si (L_n) est la s.r.l. — dite de Lucas — définie par $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$ pour $n \geqslant 0$, on a $r_m = L_{2^m}$. On a alors le critère de primalité suivant.

PROPOSITION 2. *Soit p un nombre premier de la forme $4n + 3$ et soit $M = M_p = 2^p - 1$, le $p^{ième}$ nombre de Mersenne. Alors M est premier si, et seulement si, $r_{p-1} \equiv 0 \pmod M$.*

Supposons d'abord M premier, $M = 8 \cdot 16^n - 1 \equiv 2 \pmod 5$, donc $\omega^{M+1} \equiv -1 \pmod M$, ce qui implique bien

$$r_{p-1} = (\omega^{M+1} + 1)\,\omega^{-2^{p-1}} \equiv 0 \pmod M .$$

Inversement, supposons $r_{p-1} \equiv 0 \pmod M$. On a alors

(*) $\omega^{2^p} \equiv -1 \pmod M$ [comme deux lignes plus haut]

donc

(**) $\omega^{2^{p+1}} \equiv 1 \pmod M$.

Supposons que M se décompose sous la forme

$$M = \Pi\, p_i \cdot \Pi\, q_j$$

où les p_i sont des nombres premiers de la forme $5a \pm 1$ et les q_j sont des nombres premiers de la forme $5a \pm 2$, et on a

$$\omega^{p_i - 1} \equiv 1 \pmod{p_i}, \qquad \omega^{2(q_j+1)} \equiv 1 \pmod{q_j} .$$

Comme les congruences (*) et (**) sont valables pour tout diviseur de M, on voit que l'ordre de ω modulo chaque diviseur premier de M est exactement 2^{p+1}. Donc les p_i et les q_j sont respectivement de la forme

$$p_i = 2^{p+1} h_i + 1 \quad \text{et} \quad q_j = 2^p k_j - 1 .$$

Le premier cas est impossible puisqu'on aurait $p_i > M$; le second cas n'est possible que pour $k_j = 1$ et on a donc $M = q_j$, M est bien premier! □

Ce test s'applique par exemple pour $p = 7$ et montre que 127 est premier, de la même manière (mais après plus de calculs!) on peut montrer que M_{127} est aussi premier.

D'autres tests de primalité sur les nombres de Mersenne et de Fermat figurent dans l'ouvrage de Sierpinski [56], chap. X.

2. *L'équation de Pell-Fermat*

Soit Γ une « conique » définie sur $\mathbf{Z}$, elle peut alors être caractérisée par une équation à coefficients entiers de la forme

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0.$$

En multipliant cette équation par a, on a la forme équivalente (si $a \neq 0$)

$$(ax+by+d)^2 + (ac-b^2)y^2 + 2(ac-bd)y + af - d^2 = 0.$$

Si $a = 0$ et $c \neq 0$ on obtient une écriture analogue.

Si $a = c = 0$ alors b est non nul (sinon Γ est une droite) et en posant $x' = x + y$, $y' = x - y$ on peut mettre l'équation de Γ sous la forme

$$2bx'^2 - 2by'^2 + 2(d+e)x' + 2(d-e)y' + f = 0,$$

ce qui nous ramène au cas précédent.

Ainsi, par un changement convenable de coordonnées, on peut se limiter à l'étude de l'équation

$$x'^2 + c'y'^2 + 2d'y' + f' = 0;$$

— pour $c' > 0$, Γ est une ellipse qui, bien entendu, n'a qu'un nombre fini de coordonnées entières (que l'on peut calculer facilement),

— pour $c' = 0$, Γ est une parabole, nous n'étudierons pas ce cas (on peut encore déterminer facilement les points entiers de Γ),

— pour $c' < 0$, Γ est une hyperbole et par un nouveau changement de coordonnées on peut mettre l'équation sous la forme

$$(E) \qquad X^2 - DY^2 = k, \quad \text{avec} \quad D > 0.$$

Nous excluons encore le cas trivial où k est nul. Nous sommes donc ramenés à l'étude de cette équation, dite de Pell-Fermat. Si $D = u^2$ est le carré d'un entier on a la décomposition

$$(X-uY)(X+uY) = k$$

et Γ n'a qu'un nombre fini de points que l'on trouve de manière évidente. On supposera donc désormais que D n'est pas un carré.

La théorie de l'équation de Pell-Fermat est bien connue. On montre (cf. par exemple Borevitch et Schafarevitch [10], chap. II, § 5, Th. 1) qu'il existe un nombre fini de solutions $(x^{(1)}, y^{(1)}), \ldots, (x^{(k)}, y^{(k)})$ qui peuvent être calculées effectivement, telles que toute solution (x, y) vérifie

$$x + \sqrt{D}\, y = (x^{(i)} + \sqrt{D}\, y^{(i)})\, \varepsilon^s,$$

où $1 \leqslant i \leqslant k$, $s \in \mathbf{Z}$, et ε est l'unité fondamentale de l'anneau $\mathbf{Z}[\sqrt{D}]$ dont la norme est égale à 1.

On a donc les formules

$$x = x_s^{(i)} = \frac{1}{2}\left((x^{(i)} + \sqrt{D}\, y^{(i)})\, \varepsilon^s + (x^{(i)} - \sqrt{D}\, y^{(i)})\, \varepsilon^{-s}\right)$$

et

$$y = y_s^{(i)} = \frac{1}{2}\left((x^{(i)} + \sqrt{D}\, y^{(i)})\, \varepsilon^s - (x^{(i)} - \sqrt{D}\, y^{(i)})\, \varepsilon^{-s}\right).$$

Ceci montre qu'il existe un nombre fini de suites récurrentes binaires $\xi^{(1)}, \ldots, \xi^{(k)}, \eta^{(1)}, \ldots, \eta^{(k)}$ admettant toutes $X^2 - (\varepsilon + \varepsilon^{-1})X - 1$ comme échelle telles que les solutions de l'équation (E) soient exactement les couples $(\xi_n^{(i)}, \eta_n^{(i)})$, $1 \leqslant i \leqslant k$ et $n \geqslant 0$.

Exemple 1 : Considérons l'équation

$$X^2 - 5Y^2 = 1, \quad \text{avec } X \text{ et } Y \text{ positifs}.$$

On sait que l'unité fondamentale du corps $\mathbf{Q}(\sqrt{5})$ est le nombre d'or $\omega = \dfrac{1+\sqrt{5}}{2}$, de conjugué $\dfrac{1-\sqrt{5}}{2} = -\omega^{-1}$. D'autre part l'anneau des entiers de ce corps est principal, donc si x, y est une solution avec $x > 0$ et $y \geqslant 0$, il existe $n \geqslant 0$ tel que

$$x + \sqrt{5}\, y = \pm\left(\frac{1 \pm \sqrt{5}}{2}\right)^{2n}.$$

On voit aussitôt que les deux signes doivent être $+$, donc

$$x + \sqrt{5}\, y = \left(\frac{1+\sqrt{5}}{2}\right)^{2n} = \left(\frac{3+\sqrt{5}}{2}\right)^{n}.$$

Ensuite, on constate que n doit être multiple de trois, soit

$$x + \sqrt{5}\, y = (9+4\sqrt{5})^s, \quad s \geqslant 0.$$

Les solutions sont donc $(x_s, y_s) = (1, 0), (9, 4), (161, 72), \ldots$ et elles vérifient

$$x_{s+2} = 18x_{s+1} - x_s, \quad y_{s+2} = 18y_{s+1} - y_s \quad \text{pour} \quad s \geqslant 0.$$

On peut exprimer ces nombres en fonction des nombres de Fibonacci et de Lucas,

$$x_s = \frac{1}{2} L_{3s}, \quad y_s = \frac{1}{2} F_{3s}.$$

[On a plus généralement $L_n^2 - 5\, F_n^2 = (-1)^n 4$ pour tout $n \geqslant 0$].

Exemple 2: Considérons l'équation $\dfrac{x(x+1)}{2} = 3 \cdot 2^k - 5$ où x et k sont inconnus (et entiers!). Posons $X = 2x + 1$; l'équation devient

$$X^2 - 3 \cdot 2^n = -39, \quad \text{où} \quad n = k + 3.$$

Si $n = 2m + 1$ est impair, posons $y = 2^m$, alors

$$X^2 - 6y^2 = -39,$$

mais comme $\left(\dfrac{6}{13}\right) = -1$, l'équation n'a pas de solution. Donc n est pair, disons $n = 2m$. Posons encore $y = 2^m$, alors

$$X^2 - 3y^2 = -39.$$

Donc $X = 3z$ et

$$y^2 - 3z^2 = 13.$$

On peut montrer (cf. [42]) que les solutions $y \geqslant 0$ sont les valeurs de la suite (y_s) définie par

$$y_0 = 4, \quad y_1 = 11, \quad y_s = 4y_{s-1} - y_{s-2}, \quad s \in \mathbf{Z}.$$

Donc $\ldots y_{-2} = 16,\ y_{-1} = 5,\ y_0 = 4,\ y_1 = 11,\ y_2 = 40 \ldots$ et on constate que pour les petites valeurs de $|s|$ seuls y_0 et y_{-2} sont des puissances de 2 qui correspondent aux deux solutions de l'équation initiale

$$x = 1, \quad k = 1: \frac{1(1+1)}{2} = 3 \cdot 2 - 5,$$

et

$$x = 13\,, \quad k = 5 : \frac{13(13+1)}{2} = 3 \cdot 2^5 - 5\,.$$

Nous allons montrer que ce sont les seules. D'abord ce sont les seules pour $k \leqslant 6$. Supposons que l'équation ait une solution avec $k \geqslant 7$ (i.e. $m \geqslant 5$) alors $y = y_t = 2^m$. On vérifie sans peine que ceci impose $t \equiv 6 \bmod 16$ (regarder y_s modulo 32). On considère enfin (y_s) modulo 31, cette suite est de période 32 (on a $\left(\frac{3}{31}\right) = -1$) et

$$t \equiv 6 \bmod 16 \Rightarrow y_t \equiv \pm 7 \bmod 31\,.$$

Mais, modulo 31, les puissances de 2 sont 1, 2, 4, 8 et 16. Donc l'équation considérée n'a que les deux solutions notées précédemment.

La méthode appliquée ici est un cas particulier d'un algorithme général présenté en [42] et qui s'applique à toutes les équations diophantiennes de la forme $f(x) = c \cdot a^n$, où f est un polynôme du second degré; c'est ainsi que l'on peut obtenir une nouvelle démonstration du fait que l'équation de Ramanujan-Nagell $x^2 + 7 = 2^n$ sont obtenues pour $n = 3, 4, 5, 7, 15$ (on considère des congruences modulo 7681, voir [43]).

Exemple 3: Nous allons montrer que les seuls carrés de la suite de Lucas 2, 1, 3, 4, 7 ... sont 1 et 4 et que les seuls carrés de la suite de Fibonacci 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233 ... sont 0, 1 et 144. Ce résultat est dû à Cohn [20] (voir aussi le chapitre 8 du livre de Mordell [48]).

Si $\omega = \dfrac{1+\sqrt{5}}{2}$ et $\omega' = \dfrac{1-\sqrt{5}}{2}$, on sait déjà que

$$F_n = \frac{\omega^n - \omega'^n}{\sqrt{5}} \quad \text{et} \quad L_n = \omega^n + \omega'^n\,,$$

ce qui permet d'étendre la définition de ces suites à $n \leqslant 0$. Modulo 4, les deux suites sont de période 6

n	0	1	2	3	4	5	6	7	. .
F_n mod 4	0	1	1	2	3	1	0	1	. .
L_n mod 4	2	1	3	0	3	3	2	1	. .

comme on le voit sur cette table.

De la relation $L_n^2 - 5F_n^2 = 4(-1)^n$ et de la table on déduit que

$$(F_n, L_n) = 1 \quad \text{si} \quad n \not\equiv 0 \pmod 3,$$
$$(F_n, L_n) = 2 \quad \text{si} \quad n \equiv 0 \pmod 3.$$

Démontrons d'abord l'assertion sur L_n.

Si $n = 2m$ est pair la formule $L_{2m} = L_m^2 - 2$ montre que L_n ne peut être un carré.

Supposons donc n impair. Il suffit de considérer le cas $n > 0$, et même $n \geqslant 5$ ($L_1 = 1$ et $L_3 = 4$ sont des carrés). On peut écrire $n = c + 2 \cdot t\,k$ avec $t = 3^r$, $k > 0$, $k \equiv \pm 2 \pmod 6$ et $c = 1$ ou 3. Et les formules

$$\begin{aligned} 2L_{m+2k} &= 5F_m L_{2k} + L_m L_{2k} \\ &= 5F_m F_k L_k + L_m(L_k - 2) \\ &\equiv -2v_m \pmod{L_k} \end{aligned}$$

jointes au fait que L_k est impair montrent que

$$L_n = L_{c+2tk} \equiv -L_c \equiv -1, -4 \pmod{L_k}.$$

Si L_n est un carré $\left(\dfrac{-1}{L_k}\right) = +1$ mais comme $L_k \equiv 3 \pmod 4$ c'est impossible.

Passons maintenant aux nombres de Fibonacci F_n.

Si $n \equiv 1 \pmod 4$, supposons $n \neq 1$ (sinon $F_n = 1$ est un carré). Comme plus haut écrivons $n = 1 + 2\,t\,k$ avec $t = 3^r$, $k \equiv \pm 2$ modulo 6. Les formules

$$\begin{aligned} 2F_{m+2k} &= F_n L_{2k} + F_{2k} L_n \\ &= F_n(L_k^2 - 2) + F_k L_k L_n \\ &\equiv -2F_n \pmod{L_k} \end{aligned}$$

et le fait que L_k est impair, impliquent

$$L_n \equiv -1 \pmod{L_k},$$

et comme nous l'avons déjà vu cette congruence est impossible. Donc $n = 1$ et $F_n = 1$.

Si $n \equiv 3 \pmod 4$, le changement de n en $-n$ nous ramène au cas précédent.

Si $n = 2n$ est pair alors $F_{2m} = F_m L_m = x^2$ et on peut supposer $m > 0$.

— Si $m \not\equiv 0 \pmod 3$ on a $(F_m, L_m) = 1$ donc $F_m = y^2$ et $L_m = z^2$. Par conséquent $m = 1$ ou 3, $F_n = 1$ ou 8; le seul carré est encore 1.

— Si $m \equiv 0 \pmod 3$ alors $(F_m, L_m) = 2$ et donc $F_m = 2y^2$ et $L_m = 2z^2$. Si m est impair on a $z^4 - 5y^4 = -1$, ce qui est impossible modulo 8. Si $m = 2m'$ alors $F_{m'} L_{m'} = 2y^2$. Si m' est impair on a $F_{m'} = 2t^2$ et $L_{m'} = w^2$ donc $m' = 1$ ou 3 et $F_n = 1$ ou 144. Si m' est pair alors $F_{m'} = t^2$; dans ce cas, tout ce qui précède montre que $n = 3 \cdot 2^s s \geqslant 3$ et que les nombres de Fibonacci d'indices $n/4$, $n/16$... sont tous des carrés mais, comme $F_6 = 8$ et F_{48} ne sont pas des carrés, ce dernier cas est impossible. [Il n'est pas nécessaire de calculer F_{48}: si $F_{48} = x^2$ alors $F_{24} = 2y^2$ puis $L_{12} = 2z^2$, mais $L_{12} = 322$.]

II. Méthodes p-adiques

Pour une introduction aux nombres p-adiques, le lecteur pourra consulter Borevitch et Schafarevitch [10] ou J. P. Serre [54], et pour une étude plus détaillée de l'analyse p-adique Y. Amice [2] ou K. Mahler [36].

1. *Le théorème de Skolem-Mahler*

Théorème. *Soit (ξ_n) une suite récurrente linéaire à valeurs entières. Alors l'ensemble des indices n tels que ξ_n soit nul est égal à une union finie de progressions arithmétiques (certaines de ces progressions peuvent être de raison nulle et l'union peut même être vide!).*

Comme en A.I.3, écrivons ξ_n sous la forme

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n \quad \text{pour} \quad n \geqslant 0\,,$$

les P_j étant des polynômes à coefficients dans le corps de nombres $L = \mathbf{Q}(\omega_1, \ldots, \omega_k)$, et soit $\mathfrak{P}$ un idéal premier de L tel que les ω_j soient tous des $\mathfrak{P}$-unités. Il est facile de voir que, pour tout $\varepsilon > 0$, il existe un entier T tel que

$$|\,\omega_j^T - 1\,|_{\mathfrak{P}} < \varepsilon\,, \quad j = 1, \ldots, k\,.$$

En particulier, il existe un entier T tel que chacune des T fonctions (à valeurs dans le complété $L_{\mathfrak{P}}$ de L)

$$f_m : x \to P_j(xT+m)\omega_j^m \exp\big((\operatorname{Log} \omega_j^T)x\big)\,, \quad m = 0, 1, \ldots, T-1\,,$$

où exp et Log sont l'exponentielle et le logarithme $\mathfrak{P}$-adiques, soient définies et analytiques pour x parcourant l'anneau $\mathbf{Z}_p$ des entiers p-adiques (p étant le nombre premier au-dessous de $\mathfrak{P}$).

Bien sûr, pour n entier, on a $f_m(n) = \xi_{nT+m}$. Donc, si la suite (ξ_n) possède une infinité de zéros, il en est de même pour certaines des fonctions f_m. Or, chaque f_m est une fonction analytique sur l'ensemble compact $\mathbf{Z}_p$ et, à moins d'être identiquement nulle, elle ne possède qu'un nombre fini de zéros. D'où la conclusion. □

COROLLAIRE. *Si* (ξ_n) *admet une infinité de zéros, alors, si* ξ_n *s'écrit comme plus haut*

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n,$$

où les P_j *sont des polynômes non nuls et les* ω_j *des nombres algébriques non nuls; pour tout* i *il existe un indice* $j \neq i$ *tel que* ω_i/ω_j *soit une racine de l'unité.*

Soit en effet m tel que l'on ait $\xi_{nT+m} = 0$ pour tout n. La conclusion résulte de la formule

$$P_1(nT+m)\,\omega_1^m \cdot \omega_1^{Tn} + \ldots + P_k(nT+m)\,\omega_k^m \cdot \omega_k^T = 0, \qquad n \geqslant 0,$$

et du fait qu'un polynôme exponentiel $\Sigma\, R_h(n)\,\rho_h^n$, relatifs à des ρ_h deux à deux distincts, ne peut s'annuler que si les polynômes R_h sont tous nuls (ce qu'on a déjà vu en A.III.3.c)). □

On peut se poser le problème de savoir décider si (ξ_n) comporte ou non une infinité de zéros. Pour cela, remarquons d'abord que l'idéal $\mathfrak{P}$ et le nombre T qui apparaissent dans la démonstration ci-dessus peuvent être déterminés effectivement; il suffit, par exemple, de choisir $\mathfrak{P}$ au-dessus d'un nombre premier qui ne divise pas le produit $\omega_1 \ldots \omega_k$. Discr $(\omega_1, \ldots, \omega_k)$, on peut alors prendre $T = p^f - 1$ avec $f = [L:\mathbf{Q}]$ (donc $f \leqslant k!$). On considère alors les T suites $(\xi_{nT+m})_{n\geqslant 0}$, $m = 0, 1, \ldots, T-1$ et on a vu que (ξ_n) a une infinité de zéros si, et seulement si, une de ces suites est (identiquement) nulle. Enfin comme chacune de ces T suites est une s.r.l. d'ordre k, elle est identiquement nulle si, et seulement si, ses k premières valeurs sont nulles. Pour répondre à la question il suffit donc de calculer les Tk premières valeurs ξ_n. (A ce sujet, voir aussi Berstel-Mignotte [6].)

Par contre la preuve du théorème de Skolem-Mahler ne permet pas de déterminer effectivement tous les zéros de (ξ_n), mais seulement — comme nous venons de voir — tous les zéros sauf peut-être un nombre fini d'entre eux. Cependant, le théorème suivant — dû à Strassman — permet de majorer le nombre de zéros de (ξ_n), lorsque ce nombre est fini.

THÉORÈME. *Soit* $f(x) = \sum_{k \geqslant 0} a_k x^k$, *les* a_k *appartenant à un corps* $\mathfrak{P}$*-adique* $K_{\mathfrak{P}}$, *une série qui converge sur l'anneau* $O_{\mathfrak{P}}$, *et qui n'est pas identiquement nulle. Alors le nombre de zéros de* f *dans l'ensemble* $O_{\mathfrak{P}}$ *est majoré par la quantité* $\max \{k \geqslant 0 ; | a_k |_{\mathfrak{P}}$ *est maximal*$\}$.

On trouvera une démonstration dans l'article de Lewis [32]. □

2. *Un exemple*

Avec de la chance, on peut quelquefois déterminer l'ensemble des zéros d'une suite récurrente linéaire en n'utilisant que l'analyse p-adique.

Considérons l'exemple suivant, dû à J. Berstel, de la suite définie par

$$\xi_0 = \xi_1 = 0, \quad \xi_2 = 1, \quad \xi_{n+3} = 2\xi_{n+3} - 4\xi_{n+1} + 4\xi_n \quad \text{pour} \quad n \geqslant 0.$$

On constate que l'on a

$$\xi_0 = \xi_1 = \xi_4 = \xi_6 = \xi_{13} = \xi_{52} = 0.$$

Nous allons montrer que les zéros trouvés ci-dessus sont les seuls. Choisissons $p = 53$. Modulo p, le polynôme $G = X^3 - 2X^2 + 4X - 4$ se décompose en facteurs linéaires distincts. Soient ω_1, ω_2 et ω_3 les racines de G dans le corps $\mathbf{Q}_p$, ce sont des p-unités. Comme p divise les $\omega_j^{p-1} - 1$, les 52 fonctions

$$n \mapsto \xi_{52n+m}, \quad m = 0, 1, ..., 51,$$

se prolongent en des fonctions analytiques f_m de $\mathbf{Z}_p$ dans lui-même. Posons

$$f_m(x) = \sum_{k \geqslant 0} a_{k,m} x^k ;$$

on vérifie facilement que l'on a

$$(*) \qquad p^i \mid a_{k,m} \quad \text{si} \quad k \geqslant i, \quad \text{pour} \quad i = 1, 2, 3$$

(où le symbole | signifie divise).
On constate que

$$p \nmid f_m(0) = \xi_m \quad \text{si} \quad m \notin \{0, 1, 4, 6, 13\} \quad \text{et} \quad 0 \leqslant m \leqslant 51,$$

et dans ce cas une égalité

$$f_m(x) = a_{0,m} + (\sum_{k \geqslant 1} a_{k,m} x^k) = 0$$

est impossible pour x dans $\mathbf{Z}_p$ [puisque p divise la somme entre parenthèses mais pas $a_{0,m} = \xi_m$].

Pour $m = 1, 4, 6, 13$, on a

$$f_m(0) = 0\,, \quad 53 \mid f_m(1) \quad \text{mais} \quad f_m(1) \not\equiv 0 \pmod{53^2}$$

et, en utilisant la propriété (*) pour $i = 2$, on voit que

$$f_m(x) = x(a_{1,m} + \sum_{k \geqslant 2} a_{k,m}\, x^{k-1}) \neq 0 \quad \text{si} \quad x \in \mathbf{Z}_p^*\,.$$

Enfin, pour $m = 0$, on a (en oubliant l'indice zéro)

$$f(0) = f(1) = 0\,, \quad f(2) \equiv 0 \pmod{p^2} \quad \text{et} \quad f(2) \not\equiv 0 \pmod{p^3}\,,$$

$$f(x) = x(a_1 + \sum_{k \geqslant 2} a_k\, x^{k-1}) \quad \text{avec} \quad p^2 \mid a_1 \quad \text{mais} \quad a_1 \not\equiv 0 \pmod{p^3};$$

mais ici la méthode précédente ne s'applique plus, nous avons besoin d'un outil plus puissant.

Pour k entier positif, posons

$$(X)_k = X(X-1)\ldots(X-k+1)\,, \quad \text{et en particulier} \quad (X)_0 = 1\,.$$

Du fait que X^n est une combinaison linéaire à coefficients entiers des $(X)_i$ pour $0 \leqslant i \leqslant n$, on voit qu'une série $\Sigma\, a_n\, X^n$ peut se mettre sous forme $\Sigma\, b_n \,.\, (X)_n$ avec $p^j \mid b_n$ si $p^j \mid a_m$ pour tout $m \geqslant n$. Si on applique ceci à l'exemple de f_0, on trouve

$$f(x) = f_0(x) = b_2 \,.\, (x)_2 + \sum_{k \geqslant 3} b_k \,.\, (x)_k\,,$$

où $p^2 \mid b_2$, $b_2 \not\equiv 0 \pmod{p^3}$ et $p^3 \mid b_k$ si $k \geqslant 3$ (utiliser (*) avec $i=3$). Donc f s'écrit

$$f(x) = b_2\, x(x-1)\,(1+g(x)) \quad \text{avec} \quad p \mid g(x) \quad \text{si} \quad x \in \mathbf{Z}_p\,.$$

Ceci montre que, pour z parcourant $\mathbf{Z}_p$, les seuls zéros de f_0 sont 0 et 1. D'où le résultat annoncé.

Pour d'autres détails sur cet exemple voir [37] et [44].

3. *Multiplicités de suites récurrentes linéaires*

Ce sujet a été traité très en détail par R. Tijdeman dans son exposé [60], ce qui nous permet d'être relativement brefs.

Nous ne considérerons ici que des suites à valeurs dans un anneau $\mathscr{A}$ contenu dans le corps des complexes. Pour un élément a de cet anneau, la *a-multiplicité* de la suite (ξ_n) est le nombre d'indices n pour lesquels

$\xi_n = a$; la *multiplicité* est la borne supérieure de ses a-multiplicités lorsque a parcourt $\mathscr{A}$. Lorsque (ξ_n) est une s.r.l. de rang m, sa multiplicité est égale à la 0-multiplicité d'une s.r.l. de rang au plus $m + 1$ [ceci résulte de l'exemple de A.II]. Inversement, si $\mathscr{A}$ est un corps et si le polynôme caractéristique d'une s.r.l. (ξ_n) a une racine simple ω_k alors la 0-multiplicité de (ξ) est majorée par la multiplicité d'une s.r.l. (η_n) de rang $m - 1$, m étant le rang de (ξ_n); en effet on a alors

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_{k-1}(n)\,\omega_{k-1}^n + P_k\,\omega_k^n,\ P_k \text{ constant},$$

et il suffit de poser

$$\eta_m = P_1(n)\,(\omega_1/\omega_k)^n + \ldots + P_{k-1}(n)\,(\omega_1/\omega_{k-1})^n,$$

et la 0-multiplicité de (ξ_n) est égale à la — P_m — multiplicité de (η_n).

On dira que (ξ_n) est *dégénérée* lorsqu'il existe α tel que son α-multiplicité soit infinie. Cette définition diffère de celle de [60] où la suite est dite dégénérée ssi sa 0-multiplicité est infinie. D'après le paragraphe précédent, on sait tester si une s.r.l. est dégénérée ou non.

Le problème de la multiplicité a surtout été étudié pour le premier cas non trivial, celui des s.r.l. binaires non dégénérées et à valeurs entières. M. Ward, qui a écrit plusieurs dizaines d'articles sur les suites récurrentes linéaires, avait conjecturé dans les années trente que la multiplicité d'une telle suite ne dépasse pas 5.

Après des travaux de Skolem, Chowla, Dunton, Lewis, Laxton... Kubota a prouvé cette conjecture, et même montré que la multiplicité d'une telle suite n'excède jamais 4, voir [31]. Nous avons placé l'étude de la multiplicité d'une s.r.l. dans le chapitre relatif aux méthodes p-adiques, en effet la preuve de Kubota utilise de manière essentielle la méthode de Skolem, mais elle est trop compliquée pour que nous puissions en donner une idée ici. Les résultats de Kubota ont ensuite été améliorés par Beukers [8] qui a montré que la somme de la a-multiplicité et de la $(-a)$-multiplicité d'une suite récurrente binaire entière non dégénérée est au plus 3 sauf dans le cas de la suite

$$\xi_{n+2} = \xi_{n+1} - 2\,\xi_n, \qquad \xi_0 = \xi_1 = 1$$

où cette somme vaut 5 ($\xi_0 = \xi_1 = 1$ et $\xi_2 = \xi_4 = \xi_{12} = -1$)

et dans quatre autres cas (explicites) où cette somme vaut 4. L'exemple de la suite (ξ_n) définie par

$$\xi_0 = \xi_1 = 1, \qquad \xi_{n+2} = -\xi_{n+1} + N\,\xi_n \quad (\text{donc } \xi_3 = 1),$$

avec N entier quelconque montre qu'il existe une infinité de suites récurrentes linéaires entières et non dégénérées dont la multiplicité est égale à trois.

Notons une conjecture énoncée en [60] par R. Tijdeman.

CONJECTURE. Si (ξ_n) est une s.r.l. binaire entière non dégénérée et si $\xi_s = \xi_t$ avec $r < s < t$ alors la différence $t - r$ est bornée par une constante absolue.

Récemment Beukers et Tijdeman ont démontré des résultats généraux sur la multiplicité des s.r.l. binaires à valeurs complexes, voir [9], leur article contient en particulier le très joli résultat suivant.

THÉORÈME. *Soit* α *un nombre complexe de module* $\geqslant 2$ *et soit* L *une droite du plan complexe qui ne passe pas par l'origine. Alors, au plus sept puissances entières de* α *sont sur* L.

Ce travail n'utilise pas l'analyse p-adique mais les polynômes hypergéométriques, méthode qui remonte à Thue et Siegel.

4. *Critères de rationalité*

La partie A conduit au critère de rationalité suivant: Une série formelle

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

à coefficients dans un corps $\mathscr{K}$ représente une fraction rationnelle si, et seulement si, il existe k tel que, pour N assez grand, le déterminant de Hankel d'ordre N associé à la suite $(\xi_{n+k})_{n \geqslant 0}$ est nul.

Grâce à cette caractérisation, Dwork a considérablement généralisé un résultat de Borel et obtenu un théorème qui, dans le cas rationnel, s'énonce ainsi.

THÉORÈME. *Soit une série formelle à coefficients rationnels*

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

S'il existe un ensemble fini S *de nombres premiers tels que*

(i) *pour* $p \notin S$, *chaque* ξ_n *admet un dénominateur non divisible par* p,

(ii) Ξ *définit une fonction méromorphe dans un disque de* $\mathbf{C}$ *de rayon* R_0,

(iii) *pour* $p \in S$, f *définit dans* $\mathbf{C}_p$ *une fonction méromorphe dans un disque ouvert du centre* 0 *et de rayon* R_p,

(iv) *on a* $R_0 \cdot \prod_{p \in S} R_p \geqslant 1$,

alors f est une fonction rationnelle. (Le corps $\mathbf{C}_p$ est le complété de la clôture algébrique de $\mathbf{Q}_p$).

Le théorème de Borel correspond au cas où S est vide. Le principe de la démonstration du théorème ci-dessous est le suivant. On considère, pour k assez grand, le déterminant du Hankel H_N d'ordre N de la suite (ξ_{n+k}) et on majore $|H_N|_v$ pour toutes les places v du corps $\mathbf{Q}$:

— Si v est ultramétrique et n'appartient pas à S, alors trivialement

$$|H_N|_v \leqslant 1 .$$

— Si $v \in S$ on utilise les inégalités de Cauchy dans $\mathbf{C}_p$.

— Si v est la valeur absolue ordinaire, on utilise les inégalités de Cauchy dans $\mathbf{C}$.

Pour k et N assez grands, on aboutit à l'estimation

$$\prod_v |H_N|_v < 1 ,$$

qui implique $H_N = 0$. D'où la conclusion.

Une démonstration détaillée figure en [2], ainsi que celle du théorème de Polya-Bertrandias, qui généralise le théorème précédent.

III. Méthodes transcendantes

1. *Minoration de* $|\xi_n|$

Grâce au théorème de Roth-Ridout, K. Mahler [35] avait obtenu une minoration non effective de $|\xi_n|$ pour une s.r.l. binaire. Les méthodes transcendantes conduisent à des résultats effectifs.

Soit (ξ_n) une s.r.l. donnée par

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n \quad \text{pour} \quad n \geqslant 0 , \quad \omega_1, \ldots, \omega_k \in \mathbf{C} \text{ distincts} .$$

On peut supposer $|\omega_1| \geqslant |\omega_2| \geqslant \ldots \geqslant |\omega_k|$. Lorsque $|\omega_1| > |\omega_2|$ on a trivialement

$$|\xi_n| \sim |P_1(n)|\,|\omega_1|^n$$

donc $|\xi_n| \geqslant \frac{1}{2} P_1(n)\,|\omega_1|^n$ pour $n \geqslant n_0$ (effectif).

Minorer $|\xi_n|$ n'est plus aussi facile lorsque ω_1 et ω_2 sont de même module. Considérons en effet le cas le plus simple où (ξ_n) est réelle et donnée par $\xi_n = \omega_1^n + \omega_2^n$.

Si ω_1 et ω_2 sont réels alors $\omega_2 = -\omega_1$, et on a $\xi_n = 2\,\omega_1^n$ si n est pair et $\xi_n = 0$ sinon. Par contre si ω_1 n'est pas réel, $\omega_2 = \bar{\omega}_1$ et on peut écrire $\omega_1 = \rho\, e^{i\theta}$, $\omega_2 = \rho\, e^{-i\theta}$ avec ρ réel > 0; alors

$$\xi_n = 2\,\rho^n \cos(n\,\theta), \quad \text{avec} \quad 0 < \theta < \pi .$$

Pour minorer ξ_n dans ce cas il faut minorer la quantité

$$\operatorname*{Min}_{k \in \mathbf{Z}} \left| n\theta - \left(k + \frac{1}{2}\right)\pi \right| .$$

Le cas $\theta = \dfrac{\pi}{2}$ correspond à une suite dégénérée, nous l'excluons. Ainsi, dans le cas non dégénéré, on aboutit à un problème d'approximation diophantienne.

Si f est une fonction de $\mathbf{N}$ dans lui-même qui croît arbitrairement vite, on peut trouver θ tel que, pour une infinité de valeurs de n, il existe k entier avec $\left| n\theta - \left(k + \dfrac{1}{2}\right)\pi \right| < 1/f(n)$. Pour obtenir une minoration non triviale de $|\,\xi_n\,|$ il est donc nécessaire de faire des hypothèses sur l'approximation du quotient θ/π par des rationnels.

Depuis les travaux de Gel'fond, on sait que de telles hypothèses sont vérifiées lorsque $\cos\theta$ est un nombre algébrique, donc en particulier lorsque ω_1 et ω_2 sont algébriques. Nous nous limiterons donc à l'étude des s.r.l. à valeurs algébriques.

Définissons s par

$$|\,\omega_1\,| = \ldots = |\,\omega_s\,| > |\,\omega_{s+1}\,|,$$

et posons $r_j = 1 + \deg(P_j)$ pour $j = 1, \ldots, k$.

La première minoration effective a été obtenue — pour les s.r.l. binaires — par A. Schinzel [55]. Un théorème plus général a été ensuite publié en [38], où on montre que sous les hypothèses $s \leqslant 3$ et $r_1 = \ldots = r_s = 1$, il existe des constantes effectives c et n_0 telles que, pour $n \geqslant n_0$,

$$|\,\xi_n\,| \geqslant |\,\omega_1\,|^n\, n^{-c}, \quad \text{pourvu que} \quad \sum_{j=1}^{s} P_j\,.\,\omega_j^n \neq 0 .$$

La démonstration est une application directe des estimations de A. Baker sur les formes linéaires de logarithmes de nombres algébriques [4].

Depuis ces résultats ont été étendus en [45], où le résultat suivant est démontré.

THÉORÈME. *Supposons* $s \leqslant 3$ *et qu'au moins un des nombres* ω_i/ω_j, $1 \leqslant i < j \leqslant s$ *ne soit pas une racine de l'unité. Alors il existe des constantes effectivement calculables* $C_1 > 0$ *et* $C_2 > 0$ *qui ne dépendent que de* (ξ_n) *telles que l'on ait*

$$|\xi_n| \geqslant |\omega_1|^n \exp(-C_1(\operatorname{Log} n)^2),$$

pour $n \geqslant C_2$.

La preuve repose aussi sur les minorations de Baker. Pour $s \leqslant 3$, on peut donc déterminer effectivement toutes les solutions de l'équation $\xi_n = \alpha$ pour α fixé.

Si on se limite à l'équation $\xi_n = 0$, on montre dans le même article que les indices n peuvent être déterminés effectivement sous les hypothèses: $s = 4$, $|\omega_1| > 1$ et aucun des ω_i/ω_j, $1 \leqslant i < j \leqslant 4$, n'est une racine de l'unité.

Dans le cas général, la question suivante est ouverte.

PROBLÈME. Etant donné une s.r.l. entière (ξ_n), existe-t-il un algorithme permettant de trouver tous les indices n tels que $\xi_n = 0$?

Nous énonçons la conjecture suivante.

CONJECTURE. Il existe un entier positif k tel que, si $\xi^{(1)}, \ldots, \xi^{(k)}$ sont k suites récurrentes linéaires entières quelconques, la propriété

$$\exists (n_1, n_2, \ldots, n_k), \quad \xi^{(1)}_{n_1} + \ldots + \xi^{(k)}_{n_k} = 0$$

soit indécidable.

Sous certaines hypothèses (voir [45] th. 3), on peut aussi minorer $|\xi_m - \xi_n|$ de manière effective et donc alors — en principe — déterminer les répétitions de la suite (voir [44] pour un exemple).

2. *L'équation* $\xi_m = \eta_n$

En utilisant encore une estimation sur les formes linéaires de logarithmes, on peut montrer (cf. [41]) le résultat suivant.

THÉORÈME. *Soient* (ξ_m) *et* (η_n) *deux suites récurrentes linéaires à valeurs algébriques données par*

$$\xi_m = P_1(m)\,\omega_1^m + \ldots + P_h(m)\,\omega_h^m, \quad P_1 \neq 0,$$

et

$$\eta_n = Q_1(n)\,\rho_1^n + \ldots + Q_k(n)\,\rho_k^n, \quad Q_1 \neq 0.$$

On suppose

$$|\omega_1| > |\omega_2| \geqslant \ldots, \quad |\rho_1| > |\rho_2| \geqslant \ldots, \quad |\omega_1| > 1, \quad |\rho_1| > 1.$$

Alors,

(i) *il existe un entier* N_1, *effectivement calculable, tel que pour* $m+n \geqslant N_1$ *la relation* $\xi_m = \eta_n$ *implique*

$$(*) \qquad P_1(m)\,\omega_1^m = Q_1(n)\,\rho_1^n;$$

(ii) *il existe un entier* N_2, *effectivement calculable, tel que si l'équation* (*) *admet une solution vérifiant* $m+n \geqslant N_1$, *alors* ω_1 *et* ρ_1 *sont multiplicativement dépendants;*

(iii) *soit* Z *l'ensemble des couples* (m, n) *tels que* $\xi_m = \eta_n$, *alors:*

(a) *si* P_1 *et* Q_1 *sont de même degré,* Z *est égal à l'union d'un ensemble fini et d'une union finie de progressions arithmétiques,*

(b) *si les degrés de* P_1 *et* Q_1 *sont distincts et si* Z *est infini, cet ensemble n'est pas du type précédent et on a même*

$$\lim \mathrm{Log}(m_{k+1}/m_k) > 0, \quad \textit{si} \quad (m_k, n_k)$$

désigne la suite des points de Z, *ordonnée par valeurs croissantes de* m.

On peut noter que la preuve de (ii) est élémentaire et que le cas (b) peut se produire: exemple, $\xi_m = 2^m$ et $\eta_n = n\,2^n$. De plus, on sait décider si deux nombres algébriques sont multiplicativement indépendants ou non, donc — sous les hypothèses du théorème — on sait décider si Z est fini ou non. En supposant en outre que les $|\omega_i|$ d'une part, et les $|\rho_j|$ d'autre part, sont distincts on peut même déterminer effectivement Z.

Le cas de l'équation $\xi_m = \xi_n$, pour une s.r.l. binaire, a été traité grâce à une méthode analogue par J. C. Parmani et T. N. Shorey [49].

3. *Sur le plus grand diviseur premier de* ξ_n

Cette question fait l'objet du long article de C. L. Stewart [58], le lecteur désirant plus de détails pourra consulter ce travail. Bien entendu, nous supposons que (ξ_n) est une s.r.l. à valeurs entières. Dans l'écriture

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n,$$

nous supposons de plus qu'aucun des quotients ω_i/ω_j, $i \neq j$, n'est une racine de l'unité. Enfin le plus grand diviseur d'un entier a sera noté $P(a)$ (avec la convention $P(0) = P(\pm 1) = 1$).

En 1921, Polya a montré que lim sup $P(\xi_n) = \infty$. Grâce à une généralisation p-adique du théorème de Thue-Siegel-Roth-Schmidt (généralisation due à Schlickewei), récemment R. van der Poorten et Schlickewei ont montré [53] qu'en fait $P(\xi_n)$ tend vers l'infini, une preuve indépendante mais voisine a été donné par Evertse [24]. A ce jour, ces preuves sont ineffectives.

Grâce à la théorie des formes linéaires de logarithmes, Stewart a démontré le résultat suivant (cf. [57]).

THÉORÈME. *Si on a* $|\omega_1| > |\omega_2| \geqslant \ldots |\omega_k|$ *alors, pour tout* $\varepsilon > 0$, *il existe une constante effective* $N = N(\varepsilon, \omega_1, \ldots, \omega_k, P_1, \ldots, P_k)$ *telle que, pour* $n \geqslant N$, *on ait*

$$P(\xi_n) > (1-\varepsilon) \operatorname{Log} n$$

lorsque $\xi_n \neq P_1(n)\, \omega_1^n$.

Des résultats plus forts ont été démontrés pour les s.r.l. binaires, en particulier par C. L. Stewart et T. Shorey; voir [58] pour plus d'information.

BIBLIOGRAPHIE

[1] ABE, E. *Hopf algebras.* Cambridge Univ. Press, 1980.

[2] AMICE, Y. *Les nombres p-adiques.* Paris, P.U.F., 1975.

[3] BACHMANN, P. *Niedere Zahlentheorie.* Zweiter teil, Leipzig, Teubner, 1910.

[4] BAKER, A. A sharpening of the bounds for linear forms in logarithms, II. *Acta Arithm. 24* (1973), 33-36.

[5] BERSTEL, J. *Transductions and context-free languages.* Stuttgart, Teubner, 1979.

[6] BERSTEL, J. et M. MIGNOTTE. Deux propriétés décidables des suites récurrentes linéaires. *Bull. Soc. Math. France 104* (1976), 175-184.

[7] BERSTEL, J. et REUTENAUER. *Les séries rationnelles et leurs langages.* Paris, Masson, 1984.

[8] BEUKERS, F. The multiplicity of binary recurrences. *Compositio Math. 40* (1980), 251-267.

[9] BEUKERS, F. and R. TIJDEMAN. On the multiplicity of binary complex recurrences. *Compositio Math. 51* (1984), 193-213.

[10] BOREVITCH, S. I. et I. R. SCHAFAREVITCH. *Théorie des nombres.* Paris, Gauthier-Villars, 1967.

[11] BOURBAKI, N. *Eléments de mathématiques. Algèbre, chap. 5.* Paris, Herman, 1959.

[12] CERLIENCO, L. e F. PIRAS. Risultante, m.c.m. e M.C.D. di due polinomi col metodo delle s.r.l. *Rend. Sem. Fac. Sci., Univ. Cagliari 50* (1980), 711-717.

[13] CERLIENCO, L. e F. PIRAS. Successioni ricorenti lineari e algebra del polinomi. *Rend. Math. Roma 7*, n° 1 (1981), 305-318.
[14] CERLIENCO, L. e F. PIRAS. Powers of a matrix. *Boll. Un. Mat. Italiana 6* (1983), 681-690.
[15] CERLIENCO, L. e F. PIRAS. Coefficienti binomiali generalizzati. *Rend. Sem. Fac. Sci. Univ. Cagliari 52* (1982), 47-56.
[16] CERLIENCO, L. e F. PIRAS. Aspetti coalgebrici del calcolo umbrale. *Rend. Sem. Mat. Brescia* (1984), 205-217 (Atti del Convegno « Geomitrica combinatoria e di incidenza: fondamenti e applicazioni », La Mendola, luglio 1982).
[17] CERLIENCO, L., G. DELOGU e F. PIRAS. Prodotti esterni di s.r.l. e metodi per la ricerca approssimata delle radici di un polinomio. *Rend. Sem. Fac. Sci. Cagliari, suppl. t. 50* (1980), 177-191.
[18] CERLIENCO, L., G. DELOGU e F. PIRAS. La ricerca di divisori quadratici di un polinomio col metodo delle s.r.l. *Rend. Math. Roma, t. 7, n° 1* (1981), 623-631.
[19] CERLIENCO, L., G. NICOLETTI e F. PIRAS. Representative functions on the monoid algebra $\mathscr{K}[M]$. (Preprint.)
[20] COHN, J. H. E. On square Fibonacci numbers. *J. London Math. Soc. 39* (1964), 537-540.
[21] COMTET, L. *Analyse combinatoire.* Paris, P.U.F., 1970.
[22] DICKSON, L. E. *History of the theory of numbers*, 3 v. New York, 1952.
[23] DURAND, F. *Solutions numériques des équations algébriques.* Paris, Masson, 1960.
[24] EVERTSE, J. H. On sums of S-units and linear recurrences. A paraître.
[25] FIBONACCI, L. *Liber Abaci.* 1202.
[26] GEL'FOND, A. O. *Calcul des différences finies.* Paris, Dunod, 1963.
[27] GOLOMB, S. W. *Shift register sequences.* San Francisco, Holden-Day, 1967.
[28] GYÖRY. On some arithmetical properties of Lucas and Lehmer numbers. *Acta Arith. 40* (1982), 369-373.
[29] HENRICI, P. *Elements of numerical analysis.* New York, Wiley, 1964.
[30] —— *Applied and computational complex analysis.* New York, Wiley, 1974.
[31] KUBOTA, K. On a conjecture of M. Ward, I, II, III. *Acta Arith. 33* (1977), 11-28, 29-48 et 99-109.
[32] LEWIS, D. J. Diophantine equations: p-adic methods. *Studies in Number Theory 6*, ed. W. J. Leveque, Englewood Cliffs, New Jersey, 1969.
[33] LUCAS, E. *Théorie des nombres.* Paris, Gauthier-Villars, 1891.
[34] MAC WILLIAMS, F. J. and N. J. A. SLOANE. *The theory of error correcting codes.* Amsterdam, North-Holland, 1978.
[35] MAHLER, K. A remark on recursive sequences. *J. Math. Sci. 1* (1966), 12-17.
[36] —— *Introduction to p-adic numbers and their functions.* Cambridge, Camb. Univ. Pr., 1973.
[37] MIGNOTTE, M. Suites récurrentes linéaires. *Sém. Delange-Pisot-Poitou, t. 15*, 1973/74, G. E n° 14, 9 pages.
[38] —— A note on linear recursive sequences. *J. Austral. Math. Soc., Ser. A, 20* (1975), 242-244.
[39] —— Note sur la méthode de Bernoulli. *Num. Math. 26* (1976), 325-326.
[40] —— Un algorithme sur la décomposition des polynômes dans un corps fini. *C. R. Acad. Sc. Paris 280* (1975), 137-139.
[41] —— Une extension du théorème de Skolem-Mahler. *C. R. Acad. Sc. Paris 288* (1979), 233-235.
[42] —— On the automatic resolution of certain diophantine equations. EUROSAM 84, *Lecture Notes in Computer Science n° 174*, 378-385, Springer Verlag, 1984.

[43] —— Une nouvelle résolution de l'équation $x^2 + 7 = 2^n$. *Rend. Sem. Fac. Sci. Univ. Cagliari* (à paraître).
[44] —— Sur les répétitions dans certaines suites récurrentes linéaires. Manuscrit Cagliari, oct. 84.
[45] MIGNOTTE, M., T. N. SHOREY and R. TIJDEMAN. The distance between terms of an algebraic recurrence sequence. *J. Reine ang. Math. 349* (1984), 63-76.
[46] MILNE-THOMSON, L. M. *The Calculus of finite differences*, London, Mac Millan, 1960.
[47] MONTEL, P. *Leçons sur les récurrences et leurs applications*. Paris, Gauthier-Villars, 1957.
[48] MORDELL, L. J. *Diophantine equations*. London, Acad. Press, 1969.
[49] PARMANI, J. C. and T. N. SHOREY. Subsequences of binary recursive sequences. *Acta Arith. 40* (1982), 193-196.
[50] PATHIAUX, G. Algèbre de Hadamard de fractions rationnelles. *C. R. Acad. Sci. Paris 267* (1968), 977-979.
[51] PETERSON, B. and E. J. TAFT. The Hopf algebra of linearly recursive sequences. *Aequationes Math. 20* (1980), 1-17.
[52] PISOT, C. Quelques aspects de la théorie des entiers algébriques. *Sém. Univ. Montréal*, 1963.
[53] VAN DER POORTEN, A. J. and H. P. SCHILCKEWEI. The growth conditions for recurrence sequences. Report 82-0041, Macquarie University, N.S.W., Australia, 1982.
[54] SERRE, J. P. *Cours d'arithmétique*. Paris, P.U.F., 1970.
[55] SCHINZEL, A. On two theorems of Gelf'ond and some of their applications. *Acta Arith. 13* (1967), 177-236.
[56] SIERPINSKI, W. *Elementary theory of numbers*. Warszawa, P. W. N., 1964.
[57] STEWART, C. L. On divisors of terms of linear recurrence sequences. *J. reine angew. Math. 333* (1982), 12-31.
[58] —— On the greatest prime factor of terms of a linear recurrence sequence. A paraître.
[59] SWEEDLER, M. F. *Hopf algebras*. New York, Benjamin, 1969.
[60] TIJDEMAN, R. Multiplicities of binary recurrences. *Sém. Théorie des Nombres*, Bordeaux, 1980/81, n° 29, 11 pages.

(Reçu le 21 février 1985)

M. Mignotte

Université Louis Pasteur
Centre de calcul de l'Esplanade
7, rue René-Descartes
F-67084 Strasbourg (France)

L. Cerlienco et F. Piras

Università di Cagliari
Dipartimento di Matematica
Via Ospedale, 72
Cagliari (Italie)