Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 33 (1987)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUITES RÉCURRENTES LINÉAIRES Propriétés algébriques et

arithmétiques

Autor: Cerlienco, L. / Mignotte, M. / Piras, F.

Kapitel: IV.

DOI: https://doi.org/10.5169/seals-87887

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 25.11.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Théorème (Peterson-Taft, 1980). La bialgèbre $\mathcal G$ 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 $\mathcal{K}[X]$. 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. $\eta = (\eta_m)_{m \ge 0}$ donné par

$$\eta_m = \sum_{m_0, \dots, m_n} Z_{m_0 \dots m_n}^{(m)} \xi_{m_0}^{(0)} \xi_{m_1}^{(1)} \dots \xi_{m_n}^{(n)}$$

où on a posé

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

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

$$Z(\omega_i; \omega_{1, i_1}, ..., \omega_{n, i_n}) = 0$$

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

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

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 $\mathcal{K}[X]$ 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): $P = G \cdot q(P) + r(P)$, 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,...)

$$R_{G} = \begin{pmatrix} 1 & 0 & \dots & 0 & , & \zeta_{m}^{(0)} & , & \zeta_{m+1}^{(0)} & , & \dots \\ 0 & 1 & \dots & 0 & , & \zeta_{m}^{(1)} & , & \zeta_{m+1}^{(1)} & , & \dots \\ & & & & & & & & & & \\ 0 & 0 & \dots & 1 & , & \zeta_{m}^{(m-1)} & , & \zeta_{m+1}^{(m-1)} & , & \dots \end{pmatrix}$$

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:

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

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

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 $P(X) = b_n X^n + ... + b_0$ fait usage de (12) relativement aux fonctions $\Phi(u, v)$ et $\Psi(u, v)$ telles que

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

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 $\hat{R} \cdot P$, reste de P modulo G^2 (où on a posé $\hat{R} = R_{G^2}$):

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

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

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

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

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 $x_i = b_0 \sigma_i + b_1 \sigma_{i+1} + ... + b_n \sigma_{i+n}$, (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 $|\rho_1| \ge ... \ge |\rho_m|$, 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

$$H_{j,n} = \begin{bmatrix} \xi_n & \xi_{n+1} & \dots & \xi_{n+j-1} \\ \dots & \vdots & \vdots & \vdots \\ \xi_{n+j-1} & \xi_{n+j} & \dots & \xi_{n+2j-2} \end{bmatrix} , n \geqslant 0.$$

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

Cas (I_j) : La suite $(\theta_{j,n})_{n\geq 0}$ 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 ρ_1 , $\rho_1\rho_2$, ..., $\rho_1\rho_2$... ρ_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

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

(Un cas particulier apparaît en [39]).

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

- a) la suite $(H_{j,n})_{n\geq 0}$ 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

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

Notons enfin que:

- i) Si au lieu de G(X) on utilise $\widetilde{G}(X)$, 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 \widetilde{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, $n \ge 0$, construites en utilisant les relations de récurrence

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

Notre algorithme donne la formule explicite suivante:

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

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 $\mathscr A$)

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

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 $(\xi_n, \xi_{n+1}, ..., \xi_{n+k-1})_{n \ge 0}$ 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 $n_0 \ge 0$ et t > 0 tels que

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

Grâce à la relation de récurrence cette égalité reste vraie pour tout $n \ge n_0$ et on a donc $\xi_{n+t} = \xi_n$ pour $n \ge n_0$. 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 $n_0 \ge 1$ alors la relation de récurrence montre que