Groupe de travail
d'analyse ultramétrique

Jean-Paul Bezivin

Suites récurrentes et polynômes à plusieurs variables

Groupe de travail d'analyse ultramétrique, tome 10, n° 1 (1982-1983), exp. n° 2, p. 1-6
<http://www.numdam.org/item?id=GAU_1982-1983__10_1_A1_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
10e année, 1982/83, n° 2, 6 p.

18 octobre 1982

SUITES RÉCURRENTES ET POLYNÔMES À PLUSIEURS VARIABLES

par Jean-Paul BÉZIVIN (*)

1. Introduction.

Le but de cet exposé est de généraliser un résultat de LEWIS et MORTON dans [4], ces auteurs prouvent le résultat suivant : Soient P et Q deux polynômes de $\mathbb{Z}[X_1, \ldots, X_s]$, et $m_1, \ldots, m_s$ des entiers naturels premiers entre eux deux à deux ; l'hypothèse $P(m_1^n, \ldots, m_s^n)/Q(m_1^n, \ldots, m_s^n)$ appartient à $\mathbb{Z}$ pour tout n assez grand entraîne que Q divise P dans $\mathbb{Q}[X_1, \ldots, X_s]$. Leur méthode de démonstration leur permet de démontrer un résultat analogue pour un corps de nombres inclus dans $\mathbb{R}$.

2. Notations et rappels.

Soit L un corps de type fini sur $\mathbb{Q}$, on note $\mathcal{R}(L)$ l'ensemble des applications de $\mathbb{N}$ dans K de la forme $A(n) = \sum_{i=1}^{i=t} P_i(n)\, a_i^n$, où les a_i sont des éléments non nuls de L, et les P_i des éléments de $L[X]$. Si A est dans $\mathcal{R}(L)$, on dira que les P_i sont les coefficients de A, et les a_i les fréquences de A. L'ensemble $\mathcal{R}(L)$ est muni d'une manière évidente d'une structure d'anneau non intègre, nous noterons $\mathcal{R}^*(L)$ les éléments réguliers de $\mathcal{R}(L)$ pour la multiplication.

On sait que les éléments inversibles de $\mathcal{R}(L)$ sont caractérisés par la propriété suivante : Il existe un entier M non nul, et des éléments de L^* b_r et c_r pour $0 \leqslant r < M - 1$ tels que $I(kM + r) = b_r\, c_r^k$, $\forall\, k, r$. Pour A dans $\mathcal{R}(L)$ non nul, nous noterons $\Gamma_0(A)$ le sous-groupe multiplicatif de L engendré par les fréquences de A, et nous poserons $\Gamma(A) = \{z \in L ;\ \exists\, h \geqslant 1,\ z^h \in \Gamma_0(A)\}$.

On dira qu'un élément A de $\mathcal{R}(L)$ est associé à B, s'il existe I inversible dans $\mathcal{R}(L)$ tel que $A = IB$.

Avec ces notations, on a le résultat suivant [2].

PROPOSITION 1. - *Soit* A *dans* $\mathcal{R}^*(L)$. *Il existe* I *inversible dans* $\mathcal{R}(L)$, *à fréquences dans* $\Gamma(A)$, *tel que* $\widetilde{A} = IA$ *possède la propriété suivante : Soient* B *et* C *dans* $\mathcal{R}(L)$, *tels que* $A = BC$, *alors il existe* $\widetilde{B}$ *et* $\widetilde{C}$, *associés à* B *et* C, *et à fréquences dans* $\Gamma(A)$ *tels que* $\widetilde{A} = \widetilde{B}\widetilde{C}$.

(*) Jean-Paul BÉZIVIN, Mathématiques, Université Pierre et Marie Curie, 4 place Jussieu, 75230 PARIS CEDEX 05

Nous rappelons d'autre part la conjecture du quotient de Hadamard pour les suites récurrentes : Soient $u(n)$ et $v(n)$ deux suites récurrentes linéaires, dont les coefficients et les fréquences sont dans un corps de nombres K, et S un ensemble fini de places de K, contenant les places infinies. On suppose que, pour tout entier n assez grand, on a $v(n)$ non nul et $u(n)/v(n)$ S-entier de K ; dans ces conditions la suite $u(n)/v(n)$ est une suite récurrente linéaire.

On a le résultat suivant (voir [1]).

THÉORÈME 1 [PISOT-CANTOR]. - On suppose qu'il existe une valeur absolue de K, telle qu'il existe une unique fréquence de v de plus grande valeur absolue. Alors la conjecture du quotient de Hadamard est vraie.

3. Généralisation du résultat de LEWIS et MORTON.

Soit K un corps de nombres, et $a_1, \dots, a_s$ s éléments non nuls de K. On suppose qu'il existe une valeur absolue de K, que nous noterons $|\ |$, telle que $|a_1|, \dots, |a_s|$ soient multiplicativement indépendants. Soient d'autre part P et Q deux polynômes de $K[X_1, \dots, X_s]$, et S un ensemble fini de place de K, contenant les places à l'infini. On suppose que, pour tout n assez grand, $W(n) = P(a_1^n, \dots, a_s^n)/Q(a_1^n, \dots, a_s^n)$ est un S-entier.

LEMME 1. - Dans ces conditions, $W(n)$ est une suite récurrente linéaire.

Preuve. - Il suffit de remarquer que, pour la valeur absolue $|\ |$, il existe parmi les fréquences de $v(n) = Q(a_1^n, \dots, a_s^n)$ une seule de plus grande valeur absolue, et d'appliquer le théorème 1.

LEMME 2. - Dans les mêmes conditions, il existe un monôme $\underset{\sim}{X}^{\underset{\sim}{v}} = X_1^{v_1}, \dots, X_s^{v_s}$ tel que $\underset{\sim}{X}^{\underset{\sim}{v}} P(\underset{\sim}{X})/Q(\underset{\sim}{X})$ soit un polynôme.

Preuve. - D'après le lemme 1, la suite $W(n)$ est une suite récurrente linéaire ; il existe donc des constantes b_j, $0 \leqslant j \leqslant h$, avec $b_0\, b_h$ non nul, telles que $\sum_0^h b_j W(n+j) = 0$ pour tout n assez grand.

Soit F la fraction rationnelle

$$F(X_1, \dots, X_s) = \sum_{j=0}^{j=h} b_j P(a_1^j X_1, \dots, a_s^j X_s)/Q(a_1^j X_1, \dots, a_s^j X_s) .$$

On a alors $F(a_1^n, \dots, a_s^n) = 0$ pour tout n assez grand ; les a_i étant multiplicativement indépendants, on en déduit que $F = 0$. Il est clair que l'on peut supposer P et Q premiers entre eux dans $K[\underset{\sim}{X}]$.

Si Q n'est pas alors un monôme, il existe $x_1, \dots, x_s$ dans une clôture algébrique de K, tels que $x_i \neq 0$ pour tout i et $Q(x_1, \dots, x_s) = 0$, $P(x_1, \dots, x_s) \neq 0$.

Soit $G = P/Q$, en utilisant la relation $F = 0$, on montre qu'il existe une suite d'entiers n_k strictement croissante telle que $G(a_1^{n_k} X_1, \dots, a_s^{n_k} X_s)$

soit non régulière au point $(x_1 , \dots , x_s)$; on en déduit donc que $Q(a_1^{n_k} x_1 , \dots , a_s^{n_k} x_s) = 0$ pour tout k , ce qui entraîne que Q est le polynôme nul puisque aucun des x_i n'est nul, et les a_i multiplicativement indépendants, et cette contradiction prouve le lemme.

PROPOSITION 2. - Soit K un corps de nombres, et $a_1 , \dots , a_s$ des éléments non nuls de K , on suppose qu'il existe une valeur absolue $| \ |$ de K telle que les $|a_i|$ soient multiplicativement indépendants, et de plus que, pour tout i , il existe un nombre premier p_i vérifiant $|a_i|_{p_i} < 1$ et $|a_j|_{p_i} = 1$ pour j différent de i . Soient P et Q deux éléments de $K[X_1 , \dots , X_s]$, alors l'hypothèse $P(a_1^n , \dots , a_s^n)/Q(a_1^n , \dots , a_s^n)$ entier pour tout n assez grand entraîne P/Q est un polynôme.

Preuve. - D'après le lemme 2, il suffit de regarder le cas où Q est un monôme. On suppose que l'exposant de X_i dans Q est non nul, et que l'on peut écrire $P(X_1 , \dots , X_s) = H(X_2 , \dots , X_s) + X_1 R(X_1 , \dots , X_s)$ avec H non nul. Il est facile de voir qu'il existe alors une constante C telle que l'on ait, pour tout n assez grand,

$$(*) \qquad |H(a_2^n , \dots , a_s^n)|_{p_1} \leqslant C_1 \, |a_1|_{p_1}^n ,$$

où p_1 est le nombre premier donné dans les hypothèses de la proposition 2.

On sait qu'il existe un entier $T \geqslant 1$ tel que les applications $k \longrightarrow a_i^{kT}$, $2 \leqslant i \leqslant s$, se prolongent en des applications continues de $\underset{\sim}{Z}_{p_1}$ dans $\underset{\sim}{C}_{p_1}$; Soit y un élément de $\underset{\sim}{Z}_{p_1}$ et k une suite d'entiers tendant p_1-adiquement vers y et tendant vers $+\infty$ dans $\underset{\sim}{R}$. Puisque $|a_1|_{p_1} < 1$, il résulte de la continuité des applications $x \longrightarrow a_i^{xT}$ et de l'inégalité $(*)$, que l'on a

$$H(a_2^{yT} , \dots , a_s^{yT}) = 0$$

pour tout y dans $\underset{\sim}{Z}_{p_1}$, et donc pour tout n dans $\underset{\sim}{N}$, ce qui montre, puisque les a_i sont multiplicativement indépendants, que $H = 0$.

Il en résulte donc que P/Q est un polynôme, ce qui démontre la proposition 2.

Remarque. - Dans le cas où $K = \underset{\sim}{Q}$, on améliore faiblement le résultat de [4] ; en effet, on peut appliquer la proposition 2, par exemple pour $a = 6$ et $a = 10$ dans le cas $s = 2$, et 6 et 10 ne sont pas premiers entre eux.

On peut aussi affaiblir les hypothèses du lemme 2 et de la proposition 2, de la manière suivante :

Définition. - Soit A une partie de $\underset{\sim}{N}$, on dit que A est arithmétiquement dense (noté a.r) si A rencontre toute progression arithmétique.

Propriétés.

(a) Si A est a.r , alors A est dense dans $\underset{\sim}{Z}_p$ pour tout p premier.

(b) Si A est a.r , et si a et b sont des éléments de $\underset{\sim}{N}$ avec a non nul, alors $B = \{k \ ; \ ak + b \in A\}$ est aussi a.r .

PROPOSITION 3. - On se place dans le cas où les hypothèses du début du § 3 sont réalisées, à l'exeption de $W(n)$ S-entier pour tout n , que l'on remplace par : $W(n)$ est S-entier pour tout n appartenant à une partie a.r de $\underset{\sim}{N}$. Alors la conclusion du lemme 2 est encore valable.

Preuve. - Il suffit de montrer que $W(n)$ est S'-entier, S' étant un ensemble fini de places contenant les places archimédiennes de K . On prend pour S' les places de S et aussi les places non archimédiennes où l'un des a_i n'est pas une unité du corps valué correspondant.

Soit v une place n'appartenant pas à S , elle induit sur $\underset{\sim}{Q}$ une valeur absolue ultramétrique que nous noterons $|\ |_p$, p étant le nombre premier correspondant. Il existe un entier M non nul, tel que chacune des applications $k \longrightarrow a_i^{k_M+1}$ de $\underset{\sim}{N}$ dans K se prolonge en une application continue de $\underset{\sim}{Z}_p$ dans $\underset{\sim}{C}_p$; il en est donc de même pour $W(kM + r)$, qui sera donc continue en tout point où elle sera définie. Comme par hypothèse, $W(n)$ est dans la boule unité de $\underset{\sim}{C}_p$ pour tout n dans une partie a.r de $\underset{\sim}{N}$, on en conclut facilement que $W(n)$ est v-entier chaque fois que $W(n)$ est défini, ce qui montre que $W(n)$ est S'-entier, et démontre la proposition 3.

On peut aussi donner une version affaiblie de la proposition 2, en supposant $W(n)$ entier pour tout n dans une partie a.r de $\underset{\sim}{N}$.

4. Étude d'un problème de nature analogue.

Soit K un corps de nombre, et h un entier non nul. On se propose d'étudier les conséquences, pour un polynôme P de $K[X_1 , \ldots , X_s]$ d'une hypothèse de la forme $P(a_1^n , \ldots , a_s^n) = (b_n)^h$, où b_n est un S-entier de K pour tout n dans N , et les a_i des éléments non nuls de K .

On rappelle le résultat suivant (Voir [1]).

THÉORÈME 2 [PISOT]. - Soit $u(n)$ une suite récurrente d'éléments de K . On suppose que, pour tout n , $u(n)$ est la puissance h-ième d'un S-entier de K , et qu'il existe une valeur absolue de K , telle qu'il existe une unique fréquence de u de plus grande valeur absolue, celle-ci étant pôle simple de la fraction rationnelle associée à la suite récurrente $u(n)$. Dans ces conditions, on peut écrire $u(n) = (v(n))^h$ où $v(n)$ est une suite récurrente.

PROPOSITION 4. - Soient $a_1 , \ldots , a_s$ des éléments de K^* , tels qu'il existe une valeur absolue de K vérifiant $|a_1| , \ldots , |a_s|$ sont multiplicativement indépendants. Soit P un élément de $K[X_1 , \ldots , X_s]$ tel que, pour tout n entier naturel, on ait $P(a_1^n , \ldots , a_s^n) = (b_n)^h$, où b_n est un S-entier de K . Dans

ces conditions, on a $P = \underset{\sim}{X}^{\nu} Q^h$, où $\underset{\sim}{X} = X_1^{\nu_1}, \ldots, X_s^{\nu_1}$ est un monôme, et Q un élément de $K[X_1, \ldots, X_s]$.

Preuve. - D'après le théorème 2, on peut écrire $u(n) = P(a_1^n, \ldots, a_s^n) = v(n)$, où $v(n)$ est une suite récurrente.

On utilise ensuite la proposition 1, en notant L un corps contenant K et toutes les fréquences et coefficients de $v(n)$.

Il existe donc $I(n)$, inversible dans $\mathcal{R}(L)$, à fréquences dans $\Gamma(u)$, et $J(n)$ inversible dans $\mathcal{R}(L)$, tels que $J(n)\, v(n)$ et $I(n)\, j^{-1}(n)\, v(n)^{h-1}$ soient toutes deux à fréquences dans $\Gamma(u)$.

D'après la propriété caractéristique des éléments inversibles de $\mathcal{R}(L)$ et la définition de $\Gamma(u)$, on peut trouver un entier non nul M tel que $J(nM) = \lambda\, \mu^n$ et $(Jv)(nM) = T(n)$ soit à fréquences dans $\Gamma_0(u)$. On peut alors écrire $P(a_1^{nM}, \ldots, a_s^{nM}) = \lambda^{-h}\, \mu^{-hn}\, T(n)^h$, d'où on déduit facilement que μ^{-h} appartient à $\Gamma_0(u)$. Il en résulte, puisque les a_i sont multiplicativement indépendants, que l'on peut écrire $P(X_1^M, \ldots, X_s^M) = X_1^{r_1}, \ldots, X_s^{r_s}\, G(X_1, \ldots, X_s)^h$, où l'on peut supposer que, pour tout i , X_i ne divise pas le polynôme G .

Le facteur $X_i^{r_i}$ est alors la plus grande puissance de X_i qui divise $P(X_1^M, \ldots, X_s^M)$. On écrit $P(X_1, \ldots, X_s) = X_1^{\alpha_1}, \ldots, X_s^{\alpha_s}\, Q(X_1, \ldots, X_s)$ avec X_i ne divisant pas Q , et on est ramené à étudier l'égalité $Q(X_1^M, \ldots, X_s^M) = [G(X_1, \ldots, X_s)]^h$.

On trouve dans [3] le lemme suivant.

LEMME 3. - Soit H un polynôme irréductible de $L[X_1, \ldots, X_s]$, où L est un corps algébriquement clos de caractéristique zéro, que l'on suppose non divisible par les variables X_i . Soient d'autre part $t_1, \ldots, t_s$ des entiers non nuls. Si le polynôme $H(X_1^{t_1}, \ldots, X_s^{t_s})$ est réductible, soit A un de ses facteurs irréductibles, alors on obtient tous les autres facteurs irréductibles de $H(X_1^{t_1}, \ldots, X_s^{t_s})$ en remplaçant dans A les X_i par $\xi_i X_i$, où les ξ_i sont des racines t_i-ièmes de l'unité, et en prenant une, et une seule, fois chaque polynôme à équivalence près (deux polynômes sont équivalents si l'un est multiple scalaire de l'autre). En particulier, $H(X_1^{t_1}, \ldots, X_s^{t_s})$ n'a pas de facteurs multiples.

On utilise le lemme 3 de la manière suivante : tout d'abord, si B et C sont des facteurs irréductibles distincts de $Q(X_1, \ldots, X_s)$, alors $B(X_1^M, \ldots, X_s^M)$ et $C(X_1^M, \ldots, X_s^M)$ sont premiers entre eux. On regarde alors la décomposition de $B(X_1^M, \ldots, X_s^M)$ par exemple, qui d'après le lemme n'a que des facteurs simples. Soit D l'un d'entre eux, la multiplicité de D dans $Q(X_1^M, \ldots, X_s^M)$ est donc égale à la multiplicité de B dans $Q(X_1, \ldots, X_s)$. Comme $Q(X_1^M, \ldots, X_s^M)$ est une puissance h-ième, la multiplicité de D est un multiple de h ; donc la multiplicité de tout facteur irréductible de $Q(X_1, \ldots, X_s)$ est un multiple de

h , et Q est la puissance h-ième d'un polynôme, a priori à coefficients dans une extension algébrique de K . On montre facilement, en utilisant la relation de départ $P(a_1^n , \dots , a_s^n) = (b_n)^h$ avec b_n dans K , que Q est en fait la puissance h-ième d'un polynôme de $K[X_1 , \dots , X_s]$.

Remarque. - L'exemple $s = 1$, $P(X) = X$, $a = 4$, $h = 2$, montre que l'on n'obtient pas que P est une puissance h-ième en général.

COROLLAIRE 1. - Sous les hypothèses de la proposition 4, si l'on suppose de plus que P n'est divisible par aucun des X_i , alors P est la puissance h-ième d'un élément de $K[X_1 , \dots , X_s]$.

On peut enfin donner un résultat plus précis que celui de la proposition 4 en faisant des hypothèses sur les a_i , nous donnons un énoncé pour le cas $K = \mathbb{Q}$:

COROLLAIRE 2. - Soit h un entier naturel non nul, P un polynôme à s variables à coefficients dans $\mathbb{Q}$, et a_i des éléments non nuls de $\mathbb{Q}$. On suppose que $P(a_1^n , \dots , a_s^n)$ est la puissance h-ième d'un rationel pour tout n entier naturel, et que de plus, pour tout i , il existe un nombre premier p tel que la valuation p_i-adique de a_i soit 1 , et celle des a_j avec $j \neq i$ soit nulle, alors P est la puissance h-ième d'un polynôme de $\mathbb{Q}[X_1 , \dots , X_s]$.

Preuve. - Il est facile de voir que l'on est dans les conditions d'application de la proposition 4. On peut donc écrire $P = X^{r_1} , \dots , X^{r_s} Q^h$. On regarde alors la valuation p_i-adique des deux membres de l'égalité

$$P(a_1^n , \dots , a_s^n) = a_1^{r_1 n} , \dots , a_s^{r_s n} Q(a_1^n , \dots , a_s^n)^h ,$$

n appartenant à $\mathbb{N}$, on a alors r_i multiple de h , d'où le résultat.

RÉFÉRENCES

[1] BENZAGHOU (Benali). - Algèbres de Hadamard, Bull. Soc. math. France, t. 98, 1970, p. 209-252.

[2] BÉZIVIN (Jean-Paul). - Factorisation de suites récurrentes, Groupe d'étude d'analyse ultramétrique, 7e-8e années, 1979-1981, n° 33, 9 p.

[3] GOURIN (Eli). - Irreductibles polynomials in several variables which become reductible when the variables are replaced by powers of themselves, Trans. Amer. math. Soc., t. 32, 1930, p. 485-501.

[4] LEWIS (D. J.) and MORTON (Patrick). - Quotients of polynomials and a theorem of Pisot and Cantor, J. Fac. Sc. Univ. Tokyo, Section 1, t. 28, 1981, p. 813-823.