BULLETIN DE LA S. M. F.

JEAN-PAUL BÉZIVIN

Factorisation de suites récurrentes linéaires et applications

Bulletin de la S. M. F., tome 112 (1984), p. 365-376

<http://www.numdam.org/item?id=BSMF_1984__112__365_0>

Bull. Soc. math. France,
112, 1984, p. 365-376

FACTORISATION DE SUITES RÉCURRENTES LINÉAIRES ET APPLICATIONS

PAR

JEAN-PAUL BÉZIVIN (*)

RÉSUMÉ. — On étudie un problème de factorisation pour des suites récurrentes linéaires, et on donne quelques applications.

ABSTRACT. — In this paper we study a factorisation problem for recurrent linear sequences, and give some applications.

I. Introduction et notations

Soient M un corps commutatif de caractéristique nulle, et L une clôture algébrique de M.

Si l'on considère une suite $u(n)$ d'éléments de M vérifiant une relation de récurrence linéaire du type :

$$a_s u(n+s)+\ldots+a_0 u(n)=0 \tag{1}$$

avec des coefficients a_i, $0\leqslant i\leqslant s$ dans M, a_s étant non nul, on sait que la suite $u(n)$ possède une unique expression sous la forme (*cf.* [10]) :

$$u(n)=\sum_1^t P_j(n)\, b_j^n. \tag{2}$$

Les b_j étant des éléments non nuls de L, et les P_j des polynômes de $L[X]$.

Dans ce travail, nous nous fixerons un corps K commutatif, de caractéristique nulle, nous noterons $R(K)$ l'ensemble des applications de $\mathbb{N}$ dans K de la forme (2), avec les b_j dans K^*, et les P_j éléments de $K[X]$.

(*) Texte reçu le 22 septembre 1983.

J.-P. BÉZIVIN, Université Pierre-et-Marie-Curie, Mathématiques, tour 45-46, 5e étage, 4, place Jussieu, 75230 Paris Cedex 05.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE — 0037-9434/1984/03 365 12/$ 3.20

L'ensemble $R(K)$ est muni d'une manière évidente d'une structure d'anneau commutatif unitaire.

Nous allons étudier la structure multiplicative de $R(K)$, et nous appliquerons les résultats trouvés à des problèmes de nature arithmétique.

On sait que l'anneau $R(K)$ n'est pas intègre; plus précisément, d'après un théorème de Mahler [7], les éléments de $R(K)$ qui sont réguliers pour la multiplication sont ceux qui n'ont qu'un nombre fini de zéros dans $\mathbb{N}$.

Nous noterons $R^*(K)$ l'ensemble des éléments de $R(K)$ réguliers pour la multiplication.

Soit P un élément de $R(K)$, $P(n)=\sum_1^t P_j(n)\, b_j^n$; les éléments b_j seront appelés les fréquences de P, et les polynômes P_j les coefficients de P.

On vérifie facilement que si la condition (3) suivante est réalisée, alors P est inversible dans $R(K)$:

Il existe un entier T non nul, et des éléments de K c_r et d_r non nuls, $0 \leqslant r \leqslant T-1$, tels que :

(3) $\qquad P(kT+r)=c_r d_r^{kT}$ pour tout k appartenant à $\mathbb{N}$.

Cette propriété caractérise en fait les éléments inversibles de $R(K)$:

THÉORÈME [B] (BENZAGHOU, [1]). — *Soit P appartenant à $R(K)$. Alors P est inversible dans $R(K)$, si et seulement si la condition* (3) *est satisfaite.*

On trouvera dans un article de REUTENAUER [9] une démonstration algébrique de ce résultat.

Nous dirons que l'élément P appartenant à $R(K)$, est irréductible si une égalité $P=QR$, avec Q et R dans $R(K)$, implique que Q ou R soit inversible dans $R(K)$.

Dans la partie II, nous étudions la factorisation des éléments de $R^*(K)$ quand K est de type fini sur $\mathbb{Q}$.

On a le résultat suivant :

THÉORÈME 1. — *Dans le monoïde multiplicatif $R^*(K)$, il y a factorisation unique en produit d'éléments irréductibles.*

La démonstration initiale très compliquée, (*voir* [3]), a été considérablement simplifiée par J. M. Fontaine. Je le remercie de m'avoir permis d'utiliser ici la méthode qu'il a suggérée. Notons que l'hypothèse « K de type fini sur $\mathbb{Q}$ » est peu restrictive, puisque, si l'on se donne un nombre fini de suites récurrentes, on peut trouver un corps L de type fini que $\mathbb{Q}$, tel que ces suites soient dans $R(L)$.

Dans la partie III, nous démontrerons le théorème 2, généralisant le résultat suivant de LEWIS et MORTON [5].

THÉORÈME [L-M]. — *Soient P et Q des polynômes non nuls de $\mathbb{Z}[X_1, \ldots, X_s]$, et $m_1, \ldots, m_s$ des éléments de $\mathbb{N}$ plus grand que deux, et premiers entre eux deux à deux.*

Si $P(m_1^n, \ldots, m_s^n)/Q(m_1^n, \ldots, m_s^n)$ appartient à $\mathbb{Z}$ pour tout entier n tel que $Q(m_1^n, \ldots, m_s^n)$ soit non nul, alors P/Q est un polynôme.

Leur méthode de démonstration leur permet de démontrer un résultat analogue, en remplaçant $\mathbb{Z}$ par l'anneau d'entier d'un corps de nombres inclus dans $\mathbb{R}$, mais ne leur permet pas, semble-t-il, de traiter le cas d'un corps de nombres quelconque.

Nous aurons besoin, pour la démonstration, d'un résultat lié à une conjecture de Pisot :

CONJECTURE DU QUOTIENT DE HADAMARD (notée P_1). — *Soient $u(n)$ et $v(n)$ deux suites récurrentes linéaires, dont les coefficients et les fréquences appartiennent à un corps de nombres K, et S un ensemble fini de places de K, contenant les places infinies. On suppose que, pour tout n assez grand, $v(n)$ est non nul, et $u(n)/v(n)$ est un S-entier de K. Dans ces conditions, $u(n)/v(n)$ est une suite récurrente linéaire.*

On a le résultat suivant, en direction de la conjecture (P_1) :

THÉORÈME [P-C] (PISOT-CANTOR, *voir* [1]). — *On suppose qu'il existe une valeur absolue de K, telle qu'une unique fréquence de v soit de plus grande valeur absolue. Alors, sous les hypothèses de (P_1), la suite $u(n)/v(n)$ est récurrente linéaire.*

Enfin, nous appliquons les résultats de la partie II à un problème de nature analogue à celui considéré par LEWIS et MORTON ; nous étudions (théorème 3) les conséquences d'une hypothèse du type $P(a_1^n, \ldots, a_s^n) = (b_n)^h$, où P est un polynôme à s variables, les a_i des éléments non nuls d'un corps de nombres K, et h un entier non nul fixé, b_n étant supposé S-entier de K pour tout n.

Rappelons à ce sujet une deuxième conjecture de Pisot :

CONJECTURE DE LA PUISSANCE h-ième (notée P_2). — *Soit $u(n)$ une suite récurrente linéaire, à valeurs dans un corps de nombres K. On suppose qu'il existe un entier $h \geqslant 1$, tel que, pour tout entier n on puisse écrire $u(n) = (b_n)^h$ où b_n est un S-entier de K. Alors on peut écrire $u(n) = [v(n)]^h$, où $v(n)$ est une suite récurrente linéaire.*

Nous utilisons le résultat suivant (*voir* [1]).

THÉORÈME [P] (PISOT). — *Soit $u(n)$ une suite récurrente linéaire d'éléments d'un corps de nombres K. On suppose que :*

(i) *Pour tout n appartenant à $\mathbb{N}$, $u(n)$ est la puissance h-ième d'un S-entier de K.*

(ii) *Il existe une valeur absolue de K, telle qu'une unique fréquence de u soit de plus grande valeur absolue.*

(iii) *Le polynôme coefficient de cette fréquence est une constante. Dans ces conditions, on peut écrire $u(n)=[v(n)]^h$ où $v(n)$ est une suite récurrente linéaire.*

Remarque. — La résolution des conjectures P_1 et P_2 permettrait de remplacer, dans la partie III, les hypothèses du type :

« Il existe une valeur absolue $|\ \ |$ de K, telle que $|a_1|, \ldots, |a_s|$ soient multiplicativement indépendants » par : « $a_1, \ldots, a_s$ sont multiplicativement indépendants. »

On notera que les deux hypothèses ne sont pas équivalentes, en prenant par exemple $s=3$, $K=\mathbb{Q}[i]$, et $a_1=1+2i$, $a_2=1-2i$, $a_3=1+4i$.

II. Étude de la factorisation des éléments de $R(K)$

Soit $K[K^*]$ l'algèbre du groupe multiplicatif, à coefficients dans K, (K étant un corps commutatif de type fini sur $\mathbb{Q}$). L'algèbre $K[K^*]$ est donc la K-algèbre engendrée par les $[a]$, a appartenant à K^*, avec la relation $[ab]=[a]\,[b]$ si a, b appartiennent à K^* (où le crochet a pour but de distinguer a vu comme élément de K^*, de a vu comme élément de K).

On note d'autre part, pour J sous-groupe de K^*, $K[J, X]$ l'anneau des polynômes en la variable X, à coefficients dans $K[J]$. On identifiera $K[X]$ et $K[[1], X]$.

Il est clair qu'il existe un unique homomorphisme de K-algèbres g de $K[K^*, X]$ dans $R(K)$ vérifiant :

a) $g(X)(n)=n$.

b) $g([a])(n)=a^n$, pour tout a dans K^*.

LEMME 1. — *L'homomorphisme g est un isomorphisme.*

En effet, g est surjectif par définition de $R(K)$. Il reste à montrer que g est injectif. Soit P appartenant à $K[K^*, X]$, $P=\sum_1^t P_j(X)[a_j]$, tel que

$g(P)=0$. On a donc : $\sum_1^t P_j(n)a_j^n=0$ pour toute valeur de n, et ceci implique $P_j=0$, $\forall j$ d'après l'unicité de l'écriture d'un élément de $R(K)$ sous la forme (2) ; d'où le résultat.

Preuve du théorème 1. — On peut, d'après le lemme 1, se placer dans $K[K^*, X]$, pour démontrer le théorème 1.

Soit tout d'abord J_1 un sous-groupe de type fini de K^*, et H le sous-groupe de torsion de J_1, M son ordre, et J_1' un sous-groupe libre de J_1 tel que $J_1=H\times J_1'$.

On a $K[J_1, X]$ isomorphe à $K[J_1', X]^M$, et, puisque J_1' est libre, $K[J_1', X]$ est isomorphe à $K[Y_1, \ldots, Y_n, Y_1^{-1}, \ldots, Y_n^{-1}, X]$ où n est le rang de J_1'.

On en déduit que $K[J_1, X]$ est à factorisation unique.

Soit maintenant P un élément de $K[K^*, X]$ et soit J le sous-groupe de type fini de K^* engendré par les fréquences de P.

Nous noterons $\tilde{J}$ le sous-groupe des éléments z de K^* tels que : il existe un entier n non nul vérifiant z^n appartient à J.

Puisque K est de type fini sur $\mathbb{Q}$, le groupe $\tilde{J}$ est un sous-groupe de type fini de K^* (*cf.* [6]), contenant le groupe des racines de l'unité de K. Nous notons G le groupe des racines de l'unité de K, et T son ordre.

Nous allons montrer qu'une décomposition quelconque $P=QR$ de P, a lieu essentiellement dans $K[\tilde{J}, X]$.

Plus précisément, il existe un élément S inversible de $K[K^*, X]$ tel que SQ et $S^{-1}R$ soient des éléments de $K[\tilde{J}, X]$.

Ceci démontrera le théorème 1.

Soit V un sous-groupe de type fini de K^* contenant $\tilde{J}$ et toutes les fréquences de Q et R.

Comme $\tilde{J}$ contient le sous-groupe de torsion de K^*, il en est de même de V, et on peut écrire :

$$\tilde{J}=\tilde{J}_1\times G, \qquad V=\tilde{V}\times\tilde{J}_1\times G,$$

où $\tilde{V}$ et $\tilde{J}_1$ sont des groupes libres de type fini.

En raison des isomorphismes

$$K[\tilde{J}_1, X]\simeq K[\tilde{J}_1, X]^T \qquad \text{et} \qquad K[V, X]\simeq K[\tilde{V}\times\tilde{J}_1, X]^T,$$

il suffit de démontrer que si l'on a une égalité $\tilde{P}=\tilde{Q}\tilde{R}$ avec $\tilde{P}$ dans $K[\tilde{J}_1, X]$, et $\tilde{Q}$, $\tilde{R}$ dans $K[\tilde{V}\times\tilde{J}_1, X]$, alors il existe $\tilde{S}$ inversible dans

$K[K^*, X]$, tel que $\tilde{S}\tilde{Q}$ et $\tilde{S}^{-1}\tilde{R}$ appartiennent à $K[\tilde{J}_1, X]$; or ceci est clair, en raison de l'isomorphisme entre $K[W, X]$, où W est un groupe abélien libre de rang n, et l'anneau $K[Y_1, \ldots, Y_n, Y_1^{-1}, \ldots, Y_n^{-1}, X]$.

III. Applications

III. 1. Généralisation du théorème [L-M]

Comme annoncé dans l'introduction, nous nous proposons de généraliser le théorème de Lewis et Morton au cas d'un corps de nombres quelconque.

Soit donc K un corps de nombres, et $a_1, \ldots, a_s$ des éléments non nuls de K; soient par ailleurs P et Q deux éléments non nuls de $K[X_1, \ldots, X_s]$.

Nous notons S un ensemble fini de places de K, contenant les places infinies.

Lemme 2. — *On suppose qu'il existe une valeur absolue* $|\ |$ *de* K *telle que* $|a_1|, \ldots, |a_s|$ *soient multiplicativement indépendants, et que*

$$w(n) = P(a_1^n, \ldots, a_s^n)/Q(a_1^n, \ldots, a_s^n)$$

soit un S*-entier de* K*, pour tout* n *dans* $\mathbb{N}$ *tel que* $Q(a_1^n, \ldots, a_s^n)$ *soit non nul. Alors :*

1) $w(n)$ *est une suite récurrente linéaire.*

2) *La fraction rationnelle* P/Q *est un élément de :*

$$K[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}].$$

Preuve. — 1) Il suffit de remarquer, que pour la valeur absolue $|\ |$, il existe une unique fréquence de $v(n) = Q(a_1^n, \ldots, a_s^n)$ de plus grande valeur absolue, et d'appliquer le théorème [P-C].

2) D'après 1), il existe des éléments $b_0, b_1, \ldots, b_h$ de K, avec $b_0 b_h$ non nul, tels que :

$$\sum_0^h b_j w(n+j) = 0 \quad \text{pour tout } n \text{ dans } \mathbb{N}.$$

Soit F la fraction rationnelle définie par :

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

On a alors $F(a_1^n, \ldots, a_s^n)=0$, pour toutes les valeurs n dans $\mathbb{N}$ telles que $v(n+j)\neq 0$, pour $j=0, 1, 2, \ldots, h$.

Il en résulte, puisque les a_j sont multiplicativement indépendants, que $F=0$.

On peut supposer P et Q premiers entre eux dans $K[X_1, \ldots, X_s]$. Si $G=P/Q$ n'est pas un monôme, il existe alors des éléments x_i, $i=1, 2, \ldots, s$, dans une clôture algébrique de K, tous non nuls, et tels que $Q(x_1, \ldots, x_s)=0$, $P(x_1, \ldots, x_s)\neq 0$.

La relation $F=0$ montre alors qu'il existe une suite d'entiers n_k, strictement croissante, telle que G soit non régulière au point $(a_1^{n_k}x_1, \ldots, a_s^{n_k}x_s)$, pour tout k dans $\mathbb{N}$.

On a donc, pour toute valeur de k, $Q(a_1^{n_k}x_1, \ldots, a_s^{n_k}x_s)=0$. D'après un théorème de MAHLER [7], ceci implique l'existence d'un entier non nul d, et de m dans $\mathbb{N}$, tels que, pour toute valeur q dans $\mathbb{N}$ on ait :

$$Q(a_1^{qd+m}x_1, \ldots, a_s^{qd+m}x_s)=0.$$

Si l'on pose : $Q(X_1, \ldots, X_s)=Q(\mathfrak{X})=\sum_k b_k \mathfrak{X}^k$, les b_k étant presque tous nuls, on a, avec des notations évidentes : $\sum b_k x^k \mathfrak{a}^{mk}(\mathfrak{a}^{kd})^q=0$ pour toute valeur de q.

Les $\mathfrak{a}^{kd}$ sont tous distincts, puisque les a_i sont multiplicativement indépendants. Il résulte alors de l'unicité de l'écriture d'une suite récurrente linéaire sous la forme (2) que $b_k x^k \mathfrak{a}^{mk}=0$ pour tout k; d'où $Q=0$, ce qui est absurde.

Remarque. — On peut aussi, pour démontrer le point 2) du lemme précédent, utiliser le théorème 1.

THÉORÈME 2. — *Soit K un corps de nombres, et $a_1, a_2, \ldots, a_s$ des éléments non nuls de K. On suppose qu'il existe une valeur absolue $|\ |$ de K telle que $|a_1|, \ldots, |a_s|$ soient multiplicativement indépendants, et que, de plus, pour tout i, $1\leqslant i\leqslant s$, il existe une valeur absolue $|\ |_i$ de K, telle que :*

Pour tout j différent de i, $|a_j|_i=1$, et $|a_i|_i<1$.

Soient P et Q deux éléments non nuls de $K[X_1, \ldots, X_s]$.

L'hypothèse (i) : *$P(a_1^n, \ldots, a_s^n)/Q(a_1^n, \ldots, a_s^n)$ est entier pour tout n tel que $Q(a_1^n, \ldots, a_s^n)$ soit non nul, implique*

(ii) P/Q est un polynôme.

Preuve. — Les hypothèses du lemme 2 étant vérifiées, on sait que P/Q est dans $K[X_1, \ldots, X_s, X_1^{-1}, \ldots, X_s^{-1}]$.

Écrivons $P/Q = \sum_{k \in J} b_k \mathfrak{X}^k$, où J est une partie finie de $\mathbb{Z}^s$, b_k est un élément non nul de K^* pour k dans J, et $\mathfrak{X}^k = X_1^{k_1} \ldots X_s^{k_s}$.

La suite $w(n) = P(a_1^n, \ldots, a_s^n)/Q(a_1^n, \ldots, a_s^n)$ est dans l'anneau d'entiers de K pour toute valeur de n assez grande. Il résulte alors du lemme de Fatou ([1], p. 223) que les fréquences de w sont des entiers algébriques.

Par conséquent, pour tout k dans J, $a_1^{k_1} \ldots a_s^{k_s}$ est entier algébrique. En prenant la valeur absolue $|\ \ |_i$ de cet élément, on en déduit $|a_i|_i^{k_i} \leqslant 1$, et donc, puisque $|a_i|_i < 1$, on a $k_i \in \mathbb{N}$ et $J \subset \mathbb{N}^s$, donc P/Q est un polynôme.

III. 2. Affaiblissement des hypothèses du théorème 2

On peut affaiblir les hypothèses du lemme 2 et donc aussi du théorème 2, de la manière suivante.

Soit p un nombre premier; on note $\mathbb{Z}_p$ l'anneau des entiers p-adiques, $\mathbb{Q}_p$ le corps des nombres p-adiques, et $\mathbb{C}_p$ le complété d'une clôture algébrique de $\mathbb{Q}_p$.

Definition. — *On dit qu'une partie A de $\mathbb{N}$ est arithmétiquement dense* (noté a.d.) *si A rencontre toute progression arithmétique.*

On a les propriétés suivantes (*voir* [2] et [8]) :

a) Si A est a.d., alors A est dense dans $\mathbb{Z}_p$ pour tout p premier;

b) Si A est a.d. et si a et b sont deux entiers, avec a non nul, alors $B = \{k \in \mathbb{N} \mid ak + b \in A\}$ est aussi a.d.

Lemme 3. — *Soit K un corps de nombres, $a_1, \ldots, a_s$ des éléments non nuls de K. On suppose qu'il existe une valeur absolue de K, notée $|\ \ |$, telle que $|a_1|, \ldots, |a_s|$ soient multiplicativement indépendants.*

Soient P et Q deux polynômes non nuls de $K[X_1, \ldots, X_s]$, et S un ensemble fini de places de K contenant les places infinies.

On suppose que, pour tout n dans une partie a.d. de $\mathbb{N}$,

$$w(n) = P(a_1^n, \ldots, a_s^n)/Q(a_1^n, \ldots, a_s^n)$$

est un S-entier.

Alors P/Q appartient à $K[X_1, \ldots, X_s, X_1^{-1}, \ldots, X_s^{-1}]$.

Preuve. — Nous allons montrer que les hypothèses du lemme 2 sont satisfaites avec un ensemble S' de places de K contenant S.

Soit S' la réunion des places de S, et des places de K, où l'un des éléments a_i n'est pas une unité du corps valué correspondant.

Soit v une place de K n'appartenant pas à S'. Elle induit sur $\mathbb{Q}$ une valeur absolue ultramétrique, que nous noterons $|\ \ |_p$, p étant le nombre premier correspondant, et nous considérerons que K est plongé dans $\mathbb{C}_p$.

Il existe, puisque chaque a_i est un élément de valeur absolue p-adique 1, un entier M non nul, tel que $|a_i^M - 1|_p < 1$, pour $i = 1, 2, \ldots, s$.

Ceci entraîne que les applications $k \in \mathbb{N} \to a_i^{kM+n}$ (n est un entier fixé) se prolongent en des applications continues de $\mathbb{Z}_p$ dans $\mathbb{C}_p$.

L'application $k \to w(kM+n)$ est donc la restriction à $\mathbb{N}$ du quotient de deux applications continues de $\mathbb{Z}_p$ dans $\mathbb{C}_p$; elle est donc continue, en particulier, en tout point n_0 appartenant à $\mathbb{N}$ tel que $Q(a_1^{n_0}, \ldots, a_s^{n_0})$ soit non nul.

Soit $B = \{k \mid kM + n_0 \subset A\}$. D'après les propriétés rappelées plus haut, B est dense dans $\mathbb{Z}_p$. Il existe donc une suite k_q d'éléments de $\mathbb{N}$, telle que $k_q M + n_0$ appartienne à A et que k_q ait pour limite zéro dans $\mathbb{Z}_p$.

Il en résulte que $w(k_q M + n_0)$ est p-entier pour tout q, et donc que sa limite $w(n_0)$ est p-entier.

On a donc montré que $w(n)$ est S'-entier pour tout n tel que $Q(a_1^n, \ldots, a_s^n)$ soit non nul, ce qui permet d'appliquer le lemme 2.

On a alors le résultat suivant :

PROPOSITION 4. — *Si, dans les hypothèses du théorème* 2 *on remplace* (i) *par : $P(a_1^n, \ldots, a_s^n)/Q(a_1^n, \ldots, a_s^n)$ est entier pour tout n appartenant à une partie a.d. de* $\mathbb{N}$, *alors la conclusion* (ii) *subsiste.*

Preuve. — Le lemme 3 précédent montre que P/Q appartient à $K[X_1, \ldots, X_s, X_1^{-1}, \ldots, X_s^{-1}]$; d'autre part, le lemme de FATOU a été généralisé par RAUZY [8], de sorte que si l'on a une suite récurrente linéaire $a(n)$ d'éléments d'un corps de nombres K, le fait que $a(n)$ soit entier pour n appartenant à une partie a.d. de $\mathbb{N}$ implique que les fréquences de $a(n)$ sont des entiers algébriques. La fin de la démonstration de la proposition 4 est analogue à celle du théorème 2.

Remarque. — En particulier, ce dernier résultat montre qu'un ensemble du type $W = \{(a_1^n, \ldots, a_s^n) \mid n \in A\}$ où A est une partie a.d. de $\mathbb{N}$ et $a_1, \ldots, a_s$ des entiers naturels plus grands que deux, premiers entre eux deux à deux, vérifie la propriété (D) de [5].

On notera qu'il existe des parties a.d. de $\mathbb{N}$ de densité arithmétique nulle, (*cf.* [2]).

III. 3. Étude d'un problème de même nature

Nous allons maintenant étudier un problème analogue à celui considéré par Lewis et Morton.

Soit K un corps de nombres, et h un entier naturel 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. (S est un ensemble fini de places contenant les places infinies.)

Théorème 3. — *Soient $a_1, \ldots, a_s$ des éléments non nuls de K^* tels qu'il existe une valeur absolue de K vérifiant : $|a_1|, \ldots, |a_s|$ sont multiplicativement indépendants.*

Soit P appartenant à $K[X_1, \ldots, X_s]$, 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 $P(\mathfrak{X}) = \mathfrak{X}^k Q(\mathfrak{X})^h$ où $\mathfrak{X} = (X_1, \ldots, X_s)$, $k = (k_1, \ldots, k_s) \in \mathbb{N}^s$, et Q appartient à $K[X_1, \ldots, X_s]$.

Preuve. — D'après le théorème [P], on peut écrire :

$$u(n) = P(a_1^n, \ldots, a_s^n) = (v(n))^h,$$

où $v(n)$ est une suite récurrente linéaire. En effet, on a déjà vu que l'hypothèse $|a_1|, \ldots, |a_s|$ multiplicativement indépendants entraînait l'existence d'une unique fréquence de $u(n)$ de plus grande valeur absolue, et les coefficients de u sont des polynômes constants.

Soit L un corps contenant K et toutes les fréquences et coefficients de la suite v. On peut supposer L de type fini sur $\mathbb{Q}$.

On note J le sous-groupe multiplicatif de L^* engendré par les éléments $a_1, \ldots, a_s$.

La suite $v(n)$ est un facteur de $u(n)$ dans $R(L)$. D'après la démonstration du théorème 1, il existe un élément inversible de $R(L)$, $I(n)$, tel que $I^{-1} v = T$ soit à fréquences dans $\tilde{J} = \{ z \in L \mid \exists k \geqslant 1, z^k \in J \}$.

D'après la forme des éléments inversibles de $R(L)$ (théorème B), et la définition de $\tilde{J}$, il existe un entier M tel que l'on ait :

1) $I(nM) = c d^n$ avec c, d dans L^* ;

2) $T(nM)$ à fréquences dans J.

De l'égalité $u(n) = v(n)^h$ on déduit que $u(nM) = [v(nM)]^h$ pour tout n, d'où

$$P(a_1^{nM}, \ldots, a_s^{nM}) = I(nM)^h [T(nM)]^h,$$

ou encore

$$P(a_1^{nM}, \ldots, a_s^{nM}) = c^h d^{hn} [T(nM)]^h.$$

On en déduit que d^h appartient à J.

Donc on a :

$$P(X_1^M, \ldots, X_s^M) = m X_1^{k_1} \ldots X_s^{k_s} [H(X_1, \ldots, X_s)]^h,$$

où m est un élément non nul de L, et H un polynôme à coefficients dans L. On peut supposer qu'aucun des monômes X_i ne divise le polynôme H.

Soit $\tilde{L}$ une clôture algébrique de L, et A un facteur irréductible de $P(X_1, \ldots, X_s)$ dans $\tilde{L}[X_1, \ldots, X_s]$, différent des monômes X_i. On peut écrire $P = A^q B$ avec A et B premiers entre eux.

Le polynôme $[A(X_1^M, \ldots, X_s^M)]^q$ est donc la puissance h-ième d'un polynôme. Si le polynôme $A(X_1^M, \ldots, X_s^M)$ est encore réductible, il en résulte que h divise q.

Si le polynôme $A(X_1^M, \ldots, X_s^M)$ est réductible, ses facteurs irréductibles sont alors simples (*cf.* [4]). Donc h divise aussi q dans ce cas. Finalement on peut écrire : $P(X_1, \ldots, X_s) = X_1^{k_1} \ldots X_s^{k_s} [W(X_1, \ldots, X_s)]^h$, avec W appartenant à $\tilde{L}[X_1, \ldots, X_s]$.

On voit facilement qu'il en résulte :

$$P(X_1, \ldots, X_s) = b X_1^{k_1} \ldots X_s^{k_s} [Q(X_1, \ldots, X_s)]^h \qquad \text{avec} \quad b \in K^*$$

et Q élément de $K[X_1, \ldots, X_s]$. En utilisant un n multiple de h tel que $Q(a_1^n, \ldots, a_s^n) \neq 0$, on voit que b est une puissance h-ième d'un élément de K, d'où le résultat.

COROLLAIRE 1. — *On conserve les hypothèses du théorème* 3, *et on suppose de plus que P n'est divisible par aucun des monômes* X_i. *Alors P est la puissance h-ième d'un élément de* $K[X_1, \ldots, X_s]$.

On peut aussi donner un résultat plus précis que le théorème 3, en faisant des hypothèses sur les a_i :

Donnons un énoncé pour $K = \mathbb{Q}$:

COROLLAIRE 2. — *On conserve les hypothèses du théorème* 3 ; *de surcroît, on suppose que, pour tout i compris entre* 1 *et s, il existe un entier premier* p_i *tel que la valuation* p_i*-adique de* a_i *soit* 1, *et la valuation* p_i*-adique de* a_j *soit nulle pour j différent de i. Dans ces conditions, P est la puissance h-ième d'un polynôme.*

Preuve. — D'après le théorème 3, on a :

$$P(X_1, \ldots, X_s) = X_1^{k_1} \ldots X_s^{k_s} Q(X_1, \ldots, X_s)^h.$$

Soit i fixé, $1 \leqslant i \leqslant s$. On pose :

$$|P(a_1^n, \ldots, a_s^n)|_{p_i} = p_i^{hd_n} |Q(a_1^n, \ldots, a_s^n)| = p_i^{e_n},$$

d'où

$$p_i^{hd_n} = p_i^{-k_i + he_n} \qquad \text{et} \qquad k_i = h(e_n - d_n),$$

donc k_i est multiple de h; d'où le résultat.

REFERENCES

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

[2] J. BERSTEL. — Factorisation de fractions rationnelles et suites récurrentes, Acta arithmetica, t. XXX, (1976), p. 5-17.

[3] J. P. BEZIVIN. — Factorisation de suites récurrentes linéaires, Groupe d'étude d'analyse ultramétrique 1979-1981, exposé n° 33.

[4] E. GOURIN. — On irreducible polynomials in several variables which becomes reductible when the variables are replaced by power of them selves, Trans. Amer. math. soc., 32, (1930), p. 485-501.

[5] D. J. LEWIS, P. MORTON. — Quotients of polynomials and a theorem of PISOT, Journal of the faculty of Sciences, Tokyo university, vol. 28, no. 3, (1981), p. 813-823.

[6] P. LIARDET. — Sur une conjecture de Serge LANG, Journées arithmétiques, 1974, Bordeaux, Astérisque n° 24-25, p. 187-208.

[7] K. MAHLER. — On the Taylor coefficients of rational functions Proc. Cambridge Phil. soc., t. 52, (1956), p. 39-48.

[8] G. RAUZY. — Ensembles arithmétiquement denses, CR. Acad. Sci. Paris, t. 265, (1967), p. 37-38.

[9] C. REUTENAUER. — Sur les éléments inversibles de l'algèbre de Hadamard des séries rationnelles, Bull. soc. math. France, t. 110, (1982), p. 225-233.

[10] H. SHAPIRO. — On a theorem concerning exponential polynomials, comm. on pure and applied Maths, vol. XII, (1959), p. 487-500.