Groupe de travail
d'analyse ultramétrique

Jean-Paul Bézivin

Factorisation de suites récurrentes linéaires

Groupe de travail d'analyse ultramétrique, tome 7-8 (1979-1981), exp. n° 33, p. 1-9
<http://www.numdam.org/item?id=GAU_1979-1981__7-8__A14_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
8e année, 1980/81, n° 33, 9 p.

11 mai 1981

FACTORISATION DE SUITES RÉCURRENTES LINÉAIRES

par Jean-Paul BÉZIVIN (*)

On démontre un résultat de factorisation pour les suites récurrentes linéaires, et on applique ce résultat à des problèmes de nature arithmétique sur ces suites.

1. Notations et introduction.

Soit K un corps commutatif de caractéristique nulle, on note $\mathcal{R}(K)$ l'ensemble des applications de $\underset{\sim}{N}$ dans K de la forme $P(n) = \sum_0^l P_i(n)\, \alpha_i^{n_i}$, où $P_i \in K[X]$ et $\alpha_i \in K$ sont non nuls. On dira que les α_i sont les fréquences de P, et les P_i les coefficients de P. On se limitera dans toute la suite au cas où le corps K est une extension de type fini de $\underset{\sim}{Q}$.

Il est clair que $\mathcal{R}(K)$ est un sous-anneau de l'ensemble des applications de $\underset{\sim}{N}$ dans K ; on notera $\mathcal{R}^*(K)$ le sous-ensemble de $\mathcal{R}(K)$ formé des éléments réguliers pour la multiplication, il résulte d'un théorème de MAHLER que $\mathcal{R}^*(K)$ est l'ensemble des P de $\mathcal{R}(K)$ qui n'ont qu'un nombre fini de zéro dans $\underset{\sim}{N}$.

Pour P dans $\mathcal{R}(K)$, on notera $\Gamma_0(P)$ le sous-groupe du groupe multiplicatif de K engendré par les fréquences de P, et $\Gamma(P)$ sera l'ensemble

$$\{z \in K \ ; \ \exists\ n \in \underset{\sim}{N}^* , \ z^n \in \Gamma_0(P)\}.$$

Les éléments inversibles de $\mathcal{R}(K)$ ont une forme simple.

THÉORÈME 1 (BENZAGHOU [1]). - *L'élément P de $\mathcal{R}(K)$ est inversible si, et seulement si, il existe un entier T non nul, et pour tout r entier inférieur ou égal à $T-1$, des éléments non nuls λ_r et μ_r de K tels que, $\forall\ r$ et $\forall\ k \in \underset{\sim}{N}$, on ait $P(kT + r) = \lambda_r \mu_r^{Tk}$.*

On dira que l'élément P de $\mathcal{R}^*(K)$ est irréductible, si une égalité $P = QR$, avec Q et R dans $\mathcal{R}^*(K)$ implique Q ou R inversible.

Le résultat de factorisation que nous avons en vue est le suivant.

PROPOSITION 1. - *Dans le monoïde multiplicatif $\mathcal{R}^*(K)$, il y a décomposition unique en produit d'éléments irréductibles.*

(*) Texte reçu le 18 mai 1981.

Jean-Paul BÉZIVIN, Mathématiques, Tour 46, Université P. et M. Curie, 4 place Jussieu, 75230 PARIS CEDEX 05.

La preuve de cette proposition utilise une idée due à RITT [4].

La partie 2 est consacrée à la démonstration de ce résultat ; la partie 3 à des applications à certaines conjectures de PISOT.

2. Factorisation.

LEMME 1. - *Soit Γ_0 un sous-groupe de type fini du groupe multiplicatif de K ; sous l'hypothèse que K est une extension de type fini de $\mathbb{Q}$, le sous-groupe Γ, défini par $\Gamma = \{z \in K ; \exists\, n \in \mathbb{N}^*, \ z^n \in \Gamma_0\}$, est aussi de type fini.*

Ce résultat est dû à LIARDET [2]. Notons que l'hypothèse faite sur K n'est pas très restrictive, puisque si l'on a un problème portant sur un nombre fini de suites récurrentes, on peut toujours trouver un corps L de type fini sur $\mathbb{Q}$ tel que ces suites récurrentes soient dans $\mathcal{R}(L)$.

Il résulte de ce lemme que si P appartient à $\mathcal{R}^*(K)$, le groupe $\Gamma(P)$ est de type fini. D'autre part, le groupe des racines de l'unité de K est fini, nous le noterons G , et M sera son ordre. Il est clair que si P est dans $\mathcal{R}^*(K)$, G est le sous-groupe de torsion de $\Gamma(P)$.

On déduit facilement du théorème 1 la propriété suivante.

LEMME 2. - *Un élément de $\mathcal{R}(K)$ est inversible si, et seulement si, la conclusion du theorème 1 est réalisée avec $T = M$.*

Soit P un élément fixé de $\mathcal{R}^*(K)$, le groupe $\Gamma(P)$ admet une décomposition du type $\Gamma(P) = L \oplus G$, où L est un groupe libre de type fini ; on fixe un tel groupe dans la suite de l'exposé.

PROPOSITION 2. - *Il existe $\tilde{P}$ dans $\mathcal{R}^*(K)$, associé à P , tel que :*

(a) Les fréquences de $\tilde{P}$ sont dans $\Gamma(P)$.

(b) Pour tout r entier inférieur ou égal à $M - 1$, $\tilde{P}(kM + r)$ possède la fréquence 1 , et le coefficient correspondant est un polynôme unitaire en la variable k .

(c) Il existe une base $e_1, \dots, e_t$ de L , telle que toutes les fréquences de $\tilde{P}$ aient leurs images dans L à coordonnées dans $\mathbb{N}$ dans cette base.

Preuve. - On commence par choisir une base quelconque $g_1, \dots, g_t$ de L , et on définit l'ordre lexicographique $\wp$ relatif à la base $g_1, \dots, g_t$ sur L .

Pour $r \in \{0, M - 1\}$, $P(kM + r)$ est un élément non nul de $\mathcal{R}(K)$, dont les fréquences sont parmi les puissances M-ième des fréquences de P , donc sont dans L . Pour chaque indice r , on choisit parmi les fréquences de $P(kM + r)$ la plus petite de celles-ci pour l'ordre $\wp$, que l'on note $\alpha_{i_r}^M$, et soit λ_{i_r} le coefficient du terme de plus haut degré dans le polynôme coefficient de cette fréquence ;

on définit l'élément U de $\mathcal{R}(K)$ par $U(kM + r) = \lambda_{i_r} \alpha_{i_r}^{Mk}$; il est clair que U est un élément inversible de $\mathcal{R}(K)$. On définit $\tilde{P}$ par l'égalité $P = U\tilde{P}$, et il est évident que $\tilde{P}$ vérifie les propriétés (a) et (b) de la proposition 2 .

Il reste à montrer que la propriété (c) est vérifiée ; on a besoin pour cela du lemme 3 suivant.

LEMME 3. - Soit $H = Z\,e_1 \oplus \dots \oplus Z\,e_t$ un groupe abélien libre de type fini, et $\mathcal{H}$ l'ordre lexicographique relatif à la base $e_1 , \dots , e_t$. Soient $u_1 , \dots , u_t$ des éléments de H , et M un entier non nul, on suppose que, pour tout i , Mu_i est positif pour l'ordre $\mathcal{H}$. Alors il existe une base de H , où tous les éléments u_i ont des coordonnées dans $\underset{\sim}{N}$ dans cette base.

Preuve. - On commence par construire une base de MH où tous les Mu_i ont des coordonnées dans $\underset{\sim}{N}$ dans cette base.

Soit T un entier quelconque, on définit les éléments $f_1 , \dots , f_t$ de MH par les relations

$$Me_1 = T^{t-1} f_1 + \dots + T^{t-k} f_k + \dots + f_t , \quad Me_2 = T^{t-2} f_1 + \dots + f_{t-1} , \dots , \quad Me_t = f_t$$

La matrice de passage de la base $\{Me_i\}$ à l'ensemble $\{f_1 , \dots , f_t\}$ est à coefficients dans $\underset{\sim}{Z}$, et de déterminant ± 1 , donc, pour toute valeur entière de T , $f_1 , \dots , f_t$ est une base de MH .

On écrit ensuite $Mq_i = \sum_1^t q_{i,j} Me_j$. D'après l'hypothèse faite, le premier $q_{i,j}$ non nul est un entier plus grand que 1 .

La coordonnée de Mu_i sur f_k est donnée par l'expression suivante :

$$C_{i,k}(T) = q_{i,1} T^{t-k} + q_{i,2} T^{t-k-1} + \dots + q_{i,t-k+1}$$

Il y a alors deux possibilités : ou le polynôme $C_{i,k}$ est nul, ou bien le coefficient de son terme de plus haut degré est un entier positif. On peut donc, puisque l'on a un nombre fini de polynômes à considérer, trouver un entier T assez grand, tel que tous les $C_{i,k}(T)$ soient des entiers positifs ou nuls. La base $f_1 , \dots , f_t$ correspondante est telle que tous les Mu_i soient à coordonnées dans $\underset{\sim}{N}$ dans cette base.

Pour terminer la démonstration, il suffit de remarquer que des éléments de H vérifiant les relations $M\theta_i = f_i$, pour tout i , forment une base de H qui possède la propriété indiquée dans le lemme 3 .

On termine alors la démonstration de la proposition 2 en appliquant le lemme 3 à $H = L$, et aux $\varphi(\tilde{\beta})$, où les $\tilde{\beta}$ sont les fréquences de $\tilde{P}$, et φ la projection de $\Gamma(P)$ sur L .

Remarque 1. - Au lieu de $\Gamma(P)$, on peut prendre un sous-groupe de type fini du groupe multiplicatif de K contenant $\Gamma(P)$.

Soient maintenant Q et R dans $R^*(K)$ tels que $P = QR$. Il est facile de voir que l'on peut écrire $\tilde{P} = \tilde{Q}\tilde{R}$, où $\tilde{Q}$ et $\tilde{R}$ vérifient la première propriété du (b) de la proposition 2 . Dans ces conditions, on a le résultat suivant.

LEMME 4

(a) Les fréquences de $\tilde{Q}$ et $\tilde{R}$ sont dans $\Gamma(P)$.

(b) Les images des fréquences de $\tilde{Q}$ et $\tilde{R}$ dans L sont à coordonnées entières positives ou nulles dans la base $e_1 , \ldots , e_t$ de la proposition 2.

Preuve.

(a) Soit T_0 le sous-groupe du groupe multiplicatif de K engendré par les fréquences de $\tilde{P}$, $\tilde{Q}$ et $\tilde{R}$, et $T = \{z ; \exists\, n \geq 1 , \ z^n \in T_0\}$.

On a $\Gamma(P) < T$, et le groupe $T/\Gamma(P)$ est un groupe libre de type fini. Pour démontrer (a), il faut démontrer que ce groupe est réduit à l'élément neutre.

On raisonne par l'absurde ; soit ψ l'application canonique de T sur $T/\Gamma(P)$; il existe par exemple une fréquence $\tilde{\beta}_1$ de $\tilde{Q}$ dont l'image dans $T/\Gamma(P)$ est non nulle ; soit $r_1 , \ldots , r_m$ une base de $S = T/\Gamma(P)$, on peut supposer que la coordonnée de $\psi(\tilde{\beta}_1)$ sur r_1 est un entier plus grand que 1 . La fréquence $\tilde{\beta}_1^M$ intervient au moins dans un des éléments $\tilde{Q}(kM + r)$, car sinon, en notant $\tilde{Q}(n) = \sum Q_j(n)\, \tilde{\beta}_j^n$, on trouverait que la somme des $\tilde{Q}_j(n)\, \tilde{\beta}_j^n$, pour les indices j tels que $\tilde{\beta}_j^M = \tilde{\beta}_1^M$, est nulle pour toute valeur de n , ce qui est absurde.

Soit donc r_0 un indice tel que $\tilde{\beta}_1^M$ soit une fréquence de $\tilde{Q}(kM + r_0)$, et soit $\mathcal{S}$ l'ordre lexicographique sur S relatif à la base $r_1 , \ldots , r_m$. Soit E l'ensemble des indices j tels que $\tilde{\beta}_j^M$ soit une fréquence de $\tilde{Q}(kM + r_0)$ et que $\psi(\tilde{\beta}_j^M)$ soit maximal pour l'ordre $\mathcal{S}$. De même, en écrivant $\tilde{R}(n) = \sum \tilde{R}_i(n)\, \gamma_i^n$, soit F l'ensemble des indices h tels que $\tilde{\gamma}_h^M$ soit une fréquence de $\tilde{R}(kM + r_0)$, et $\psi(\tilde{\gamma}_h^M)$ maximal pour l'ordre $\mathcal{S}$. On remarque que si j est dans E , $\psi(\tilde{\beta}_j^M)$ est strictement positif pour l'ordre $\mathcal{S}$; et si h est dans F , $\psi(\tilde{\gamma}_h^M)$ est positif ou nul pour l'ordre $\mathcal{S}$, parce que $\tilde{R}(kM + r_0)$ possède la fréquence 1 .

On note alors A(k) la somme des $\tilde{Q}_j(kM + r_0)\, \tilde{\beta}_j^{r_0 + kM}$ pour j dans E , et B(k) la somme des $\tilde{R}_h(kM + r_0)\, \tilde{\gamma}_h^{r_0 + kM}$ pour h dans F . Le produit A(k) B(k) n'est pas nul ; en effet, si c'était le cas, l'une des deux expressions, par exemple A(k) , aurait une infinité de zéros, et d'après un théorème de MAHLER, il existerait deux indices distincts i et j de E tels que le quotient de $\tilde{\beta}_i^M$ et de $\tilde{\beta}_j^M$ soit une racine de l'unité différente de 1 ; mais ceci est impossible car M est l'ordre du groupe des racines de l'unité de K .

On en déduit alors qu'une fréquence quelconque de A(k) B(k) est une fréquence

de $\tilde{Q}(kM + r_0)\,\tilde{R}(kM + r_0)$, donc de $\tilde{P}(kM + r_0)$, et ceci est contradictoire, puisqu'une fréquence de $A(k)\,B(k)$ a une image non nulle dans S , et toutes les fréquences de $\tilde{P}(kM + r_0)$ sont dans $\Gamma(P)$.

(b) D'après (a), on sait que toutes les fréquences de $\tilde{Q}$ et $\tilde{R}$ sont dans $\Gamma(P)$. On raisonne alors par l'absurde, en supposant que l'une des fréquences de $\tilde{Q}$, par exemple, a une image dans L ayant une coordonnée négative sur e_1 ; ceci équivaut à dire qu'il existe un indice r_0 et une fréquence de $\tilde{Q}(kM + r_0)$ ayant une coordonnée strictement négative sur e_1 . On définit alors l'ordre lexicographique sur la base e_1 , ... , e_t de L , et on prend la fréquence de $\tilde{Q}(kM + r_0)$ minimale pour cet ordre. On procède de même pour $\tilde{R}(kM + r_0)$. On voit facilement que le produit de ces deux fréquences est une fréquence de $\tilde{P}(kM + r_0)$, ayant une coordonnée strictement négative sur e_1 , ce qui est la contradiction cherchée.

On peut maintenant démontrer la proposition 1. En notant θ_i la puissance M-ième de e_i , il résulte du lemme 4 et de la proposition 2 que l'on peut écrire, pour tout r ,

$$\tilde{P}(kM + r) = U_r(k\,,\ \theta_1^k\,,\ \dots\,,\ \theta_t^k)\,,\quad \tilde{Q}(kM + r) = V_r(k\,,\ \theta_1^k\,,\ \dots\ \theta_t^k)\,,$$

et

$$\tilde{R}(kM + r) = W_r(k\,,\ \theta_1^k\,,\ \dots\,,\ \theta_t^k)\,,$$

où U_r , V_r et W_r sont des éléments de $K[X\,,\ X_1\,,\ \dots\,,\ X_t]$. Il est clair que les θ_i sont des éléments multiplicativement indépendants de K , donc les égalités $\tilde{P}(kM + r) = \tilde{Q}(kM + r)\,\tilde{R}(kM + r)$ sont équivalentes aux égalités $U_r = V_r\,W_r$ entre polynômes.

On peut remarquer que, dans tout ce qui a précédé, les suites inversibles que nous avons utilisées étaient définies explicitement, donc nous n'avons pas utilisé véritablement le théorème 1 ; en appliquant le résultat que nous venons de démontrer à $P(n) = 1$ pour tout n , on retrouve donc le théorème 1 .

D'autre part, si P est supposé irréductible, et si $\tilde{P}$ est tel qu'il existe au moins deux indices r_1 et r_2 tels que U_{r_1} et U_{r_2} soient différents du polynôme constant égal à 1 , on trouve immédiatement une contradiction ; il existe donc un unique indice r_0 tel que U_{r_0} soit différent de 1 , et le polynôme U_{r_0} doit être irréductible.

Réciproquement, on voit qu'un élément de $\mathcal{R}^*(K)$ possédant ces propriétés est irréductible.

Enfin, on trouve que tout élément de $\mathcal{R}^*(K)$ s'écrit comme produit d'éléments irréductibles, et l'unicité de cette décomposition provient du fait que $K[X\,,\ X_1\,,\ \dots\,,\ X_t]$ est factoriel.

PROPOSITION 3. - Soient P, Q dans $\mathcal{R}^*(K)$, et R dans $\mathcal{R}^*(L)$, où L est un corps contenant K. Si on a $P = QR$, alors R appartient à $\mathcal{R}^*(K)$. De plus, si l'on suppose qu'il existe $e_1, \dots, e_t$, éléments multiplicativement indépendants du corps K (1), et des polynômes U_r et V_r de $K[X, X_1, \dots, X_t]$ tels que $U_r(X, 0, \dots, 0)$ et $V_r(X, 0, \dots, 0)$ soient non nuls et unitaires, vérifiant

$$P(kM + r) = U_r(k, e_1^{Mk}, \dots, e_t^{Mk}) \quad \text{et} \quad Q(kM + r) = V_r(k, e_1^{Mk}, \dots, e_t^{Mk}),$$

alors il existe des polynômes W_r possédant les mêmes propriétés tels que

$$R(kM + r) = W_r(k, e_1^{Mk}, \dots, e_t^{Mk}).$$

Preuve. - On pose

$$P(n) = \sum_0^s P_j(n)\, \alpha_F^n, \quad Q(n) = \sum_0^h Q_j(n)\, \beta_j^n \quad \text{et} \quad R(n) = \sum_0^m R_j(n)\, \gamma_j^n.$$

On définit sur l'ensemble $\{\gamma_0, \gamma_1, \dots \gamma_m\}$ une relation d'équivalence par $\gamma_i \equiv \gamma_j \iff \gamma_i/\gamma_j \in K$. Soient $E_1, \dots, E_\ell$ les différentes classes d'équivalence, et pour tout i, θ_i un représentant de la classe E_i. La somme des $R_j(n)\, \gamma_j^n$ pour γ_j dans E_i peut s'écrire $\theta_i^n S_i(n)$ avec S_i dans $\mathcal{R}(K)$. On a donc l'égalité

$$\sum_1^\ell \theta_i^n S_i(n)\, Q(n) = P(n).$$

Il est impossible que $S_i(n)\, Q(n) = 0$, puisque S_i n'est pas nulle, et Q est régulière ; toute fréquence de $\theta_i^n S_i(n)\, Q(n)$ est donc une fréquence de P, donc dans K. Il en résulte qu'il ne peut y avoir qu'une seule classe d'équivalence, formée d'eléments de K, donc toutes les fréquences de R sont dans K. On voit ensuite facilement que les polynômes R_j ont des coefficients qui sont des fractions rationelles à coefficients dans K en les fréquences de R, donc sont aussi dans K.

Un raisonnement analogue à celui fait dans le lemme 4 termine alors la démonstration.

3. Applications.

Nous allons appliquer ce qui précède à deux conjectures de PISOT.

(P_1) Soit K un corps de nombre, S un ensemble fini de places de K contenant toutes les places infinies, et $P(n)$, $Q(n)$ deux éléments de $\mathcal{R}^*(K)$. On suppose qu'il existe une suite $c(n)$ de S-entiers de K telle que $P(n) = Q(n)\, c(n)$

---

(1) tels que si $\Gamma = \{e_1, \dots, e_t\} \times G$, et si $z \in K$ et tel que $\exists\, n \geqslant 1$, $z^n \in \Gamma$, on ait $z \in \Gamma$.

pour tout n . Alors il existe un élément de $R(\underset{\sim}{C})$, R tel que $P(n) = Q(n)\,R(n)$ pour tout n .

(P_2) Soit K un corps de nombres, P un élément de $R^*(K)$, et s un entier supérieur ou égal à 1 . S'il existe une suite $c(n)$ de S-entiers de K telle que $P(n) = c(n)^s$ pour tout n , alors il existe un élément Q de $R(\underset{\sim}{C})$ tel que $P = Q^s$.

La conjecture (P_1) a été démontrée par POURCHET [3]. La méthode utilisée ici ne permet pas de redémontrer cette conjecture, on aura simplement un résultat partiel ; cependant nous pourrons affaiblir les hypothèses de (P_1) . De même, on aura un résultat partiel pour la conjecture (P_2) .

On trouve dans [1] de plus amples informations sur ces deux conjectures. On va utiliser dans les deux cas la proposition suivante.

PROPOSITION 4. - Soit K un corps de nombres, P et Q deux polynômes de $K[X , X_1 , \ldots , X_t]$, P étant supposé irréductible et premier avec Q . On suppose de plus que P est de degré non nul en la variable X .

Si p est un nombre premier, on se donne un prolongement de la valeur absolue p-adique de $\underset{\sim}{Q}$ à K . Soient $\theta_1 , \ldots , \theta_t \in K^*$ multiplicativement indépendants. Il existe alors une infinité de nombres premiers p tels que : il existe T entier, et r entier, $0 \leqslant r \leqslant T - 1$, tels que les applications de $\underset{\sim}{N}$ dans K , définies par

$$k \longrightarrow P(kT + r , \theta_1^{kT+1} , \ldots , \theta_t^{kT+1}) \quad \text{et} \quad k \longrightarrow Q(kT + r , \theta_1^{kT+1} , \ldots , \theta_t^{kT+1})$$

se prolongent en des fonctions analytiques de $\underset{\sim}{Z}_p$ dans K_p (K_p est le complété de K pour la valeur absolue p-adique), que nous noterons f et g , et un élément x_0 de Z_p tel que $f(x_0) = 0$ et $|f'(x_0)|_p = |g(x_0)|_p = 1$.

Preuve. - On note R le résultant des deux polynômes P et Q considérés comme polynômes en la variable X , R est non nul, vu les hypothèses faites sur P et Q . On note A le produit des coefficients non nuls de P considéré comme polynôme en X , et H son résultant. Il existe U et V dans $K[X , X_1 , \ldots , X_t]$ tels que $UP + VQ = R$; enfin on note B le produit RAH . Le polynôme B est non nul ; il existe donc un entier m tel que l'on ait $B(\theta_1^m , \ldots , \theta_t^m) \neq 0$.

Soit alors S un ensemble fini de nombres premiers tel que

(a) S contient les nombres premiers qui se ramifient dans K ,

(b) si p n'appartient pas à S , tous les coefficients de tous les polynômes P , Q , H , R , U et V sont des entiers p-adiques,

(c) si p n'appartient pas à S , tous les θ_i et $B(\theta_1^m , \ldots , \theta_t^m)$ sont des

unités p-adiques.

On considère alors le polynôme en la variable k, $W(k) = P(k, \theta_1^m, \dots, \theta_t^m)$.

D'après les hypothèses faites, W est un polynôme non constant de $K[X]$.

D'après un théorème de RENZAGHOU [1], il existe une infinité de nombres premiers p tels qu'il existe k dans $\underset{\sim}{N}$ vérifiant $|W(k)|_p < 1$.

Soit E l'ensemble de ces nombres premiers n'appartenant pas à S, et p appartenant à E. Il existe un entier h tel que $|\theta_i^{p^h-1} - 1|_p \leqslant 1/p$, $\forall\, i$.

Soit k un entier tel que $|W(k)|_p < 1$, et q un entier tel que l'on ait $q \equiv k\ [p]$ et $q \equiv m\ [p^h - 1]$. On a alors $|P(q, \theta_1^q, \dots, \theta_t^q)|_p \leqslant 1/p$ et $|B(\theta_1^q, \dots, \theta_t^q)|_p = 1$. On pose $T = p^h - 1$, et soit $r_0 \in \{0, \dots, T-1\}$ tel que $q \equiv r_0\ [T]$. On note f la fonction analytique sur Z_p prolongeant $P(kT + r_0, \theta_1^{kT+r_0}, \dots, \theta_t^{kT+r_0})$, h la fonction analytique prolongeant $B(\theta_1^{kT+r_0}, \dots, \theta_t^{kT+r_0})$, et g celle prolongeant $Q(kT + r_0, \theta_1^{kT+r_0}, \dots, \theta_t^{kT+r_0})$.

On pose $q = Ty + r_0$, et on a

$$|f(y)|_p \leqslant 1/p\ , \quad |h(y)|_p = |f'(y)|_p = 1\ .$$

On en déduit alors qu'il existe x_0 dans Z_p, tel que $f(x_0) = 0$ et $x_0 \equiv y\ [p]$, d'où $|f'(x_0)|_p = |h(x_0)|_p = 1$. Enfin en utilisant l'égalité $UP + VQ = R$, on en déduit $|g(x_0)|_p = 1$.

Application à la conjecture (P_1). - On peut se ramener au cas où, pour tout t,

$$P(kM + t) = U_t(k, \theta_1^k, \dots, \theta_s^k) \quad \text{et} \quad Q(kM + t) = V_t(k, \theta_1^k, \dots, \theta_s^k),$$

U_t et V_t étant des polynômes de $K[X, X_1, \dots, X_s]$. On regarde alors sur chacune des progressions arithmétiques $kM + t$, et il est clair que l'on peut supposer que U_t et V_t sont premiers entre eux ; soit A un facteur irréductible de V_t de degré non nul en X ; la proposition 4 nous permet alors de trouver une contradiction, en considérant $A = P$, $U_t = Q$, et des entiers de la forme $k = uT + r$ avec u tendant vers x_0 dans Z_p, pour p convenablement choisi. Par conséquent, on a démontré P_1 dans le cas où, dans tous les facteurs irréductibles de Q, la variable X intervient. On peut remplacer l'hypothèse c(n) S-entiers par : pour tout p n'appartenant pas à S, la suite c(n) est p-adiquement bornée.

Application à la conjecture (P_2). - On écrit

$$P(kM + r) = \lambda_r \alpha_r^h P_r(k, \theta_1^k, \dots, \theta_t^k)\ .$$

On fixe r, et on écrit la décomposition de P_r en facteurs irréductibles dans $K[X, X_1, \dots, X_t]$ sous la forme $P_r = A_1^{\alpha_1}, \dots, A_m^{\alpha_m}$.

Supposons que le facteur irréductible A_1 soit de degré non nul en X. On applique alors la proposition 4, en prenant $P = A_1$, et pour Q le produit des autres A_i. On prend p tel que λ_r et α_r soient des unités p-adiques ; on appelle f la fonction analytique prolongeant la fonction $A_1(kT + t_0)$, et g celle prolongeant $A_2^{\alpha_2}(kT + t_0)$, ..., $A_m^{\alpha_m}(kT + t_0)$.

Au point x_0, la fonction f a un zéro, et $f'(x_0)$ et $g(x_0)$ sont des unités p-adiques ; par conséquent, pour x entier assez proche de x_0, on aura $\alpha_1 v_p(x - x_0)$ qui sera un multiple entier de s. Il en résulte facilement que α_1 est un multiple de s.

En faisant l'hypothèse que dans tous les facteurs irréductibles de P, la variable X intervient, il en résulte que la conjecture est démontrée dans ce cas, puisque une unité de $R(X)$ est une puissance s-ième d'un élément de $R(\underset{\sim}{C})$.

Enfin, il est clair qu'une proposition analogue à la proposition 4 sans hypothèse restrictive sur le polynôme P, conduirait à une démonstration de la conjecture (P_2).

BIBLIOGRAPHIE

[1] BENZAGHOU (Benali). - Algèbres de Hadamard, Bull. Soc. math. France, t. 98, 1970, p. 209-252 (Thèse Sc. math., Paris, 1969).

[2] LIARDET (Pierre). - Sur une conjecture de Serge Lang, "Journées arithmétiques [1974. Bordeaux]," Astérisque n° 24-25, 1975, p. 187-209.

[3] POURCHET (Yves). - Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles, C. R. Acad. Sc. Paris, t. 288, 1979 série A, p. 1055-1057.

[4] RITT (J. F.). - A factorization theory for functions, Trans. Amer. math. Soc., t. 29, 1927, p. 584-596.