BULLETIN DE LA S. M. F.

JEAN-PAUL BÉZIVIN

Suites récurrentes linéaires en caractéristique non nulle

Bulletin de la S. M. F., tome 115 (1987), p. 227-239

<http://www.numdam.org/item?id=BSMF_1987__115__227_0>

© Bulletin de la S. M. F., 1987, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (http://smf.emath.fr/Publications/Bulletin/Presentation.html) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Bull. Soc. math. France,
115, 1987, p. 227-239.

SUITES RÉCURRENTES LINÉAIRES EN CARACTÉRISTIQUE NON NULLE

PAR

JEAN-PAUL BEZIVIN (*)

RÉSUMÉ. – Nous étudions quelques problèmes sur les suites récurrentes linéaires en caractéristique p, comme l'analogue du théorème de SKOLEM-LECH-MAHLER sur les zéros des suites récurrentes linéaires, et aussi de certains théorèmes de G. POLYA.

ABSTRACT. – We study some problems for linear recurrent sequences in the case of characteristic p base field, such as the SKOLEM-LECH-MAHLER's theorem on zeros of linear recurrent sequences, and we generalize some theorems of G. POLYA.

I. Introduction

Soit K un corps commutatif, et $u=(u(n))\ n=0, 1, \ldots$ une suite d'éléments de K.

Nous dirons que u est une suite récurrente linéaire, s'il existe un entier naturel s non nul, et des éléments $a_j (j=0, 1, 2, \ldots s-1)$ de K, tels que l'on ait, pour tout n dans $\mathbf{N}$ la relation:

$$u(n+s)=a_{s-1}u(n+s-1)+\ldots+a_0 u(n), \tag{1}$$

avec a_0 non nul.

(*) Texte reçu le 15 avril 1986, revisé le 9 juin 1986

J. P. BEZIVIN, Université de Paris-VI, Mathématiques, tour 45/46, 5e étage, 4, place Jussieu, 75252 Paris Cedex 05

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE – 0037-9484/1987/02 227 13/$ 3.30
© Gauthier-Villars

Il est bien connu que dire que la suite $u=(u(n))$ vérifie une relation de récurrence linéaire du type (1) est équivalent à dire que la série formelle $F(x)=\sum_{n\geq 0} u(n)x^n$ représente le développement de Taylor à l'origine d'une fraction rationnelle $P(x)/Q(x)$, avec P et Q à coefficients dans K, $Q(0)$ non nul et $d^0 P$ plus petit que $d^0 Q$.

Notons par α_i $1\leq i\leq t$ les inverses des racines distinctes de Q dans une clôture algébrique L de K.

On sait alors qu'en caractéristique nulle, on peut représenter $u(n)$ à l'aide des éléments α_i, sous la forme:

$$u(n)=\sum_{i=1}^{t} P_i(n)\alpha_i^n, \tag{2}$$

où les P_i sont des polynômes à coefficients dans L.

En caractéristique non nulle, ce n'est plus le cas; on peut cependant se ramener au cas où les polynômes P_i sont des polynômes constants, *voir* [6], et le théorème 8 plus loin.

Les propriétés des suites $u(n)$ vérifiant une relation de récurrence linéaire ont été étudiées depuis longtemps, d'abord pour $K=\mathbb{Q}$, puis pour un corps K de caractéristique nulle quelconque. Il n'existe, à la connaissance de l'auteur, qu'un seul article étudiant les propriétés des suites récurrentes linéaires dans le cas d'un corps de caractéristique non nulle, à savoir un article de C. REUTENAUER [6], dont nous utiliserons d'ailleurs les résultats.

Le but du présent article est de généraliser deux résultats sur les suites récurrentes linéaires, connus en caractéristique nulle, au cas de la caractéristique non nulle.

Le premier de ces résultats est le théorème de SKOLEM-LECH-MAHLER ([3], [4]) qui décrit l'ensemble $A=\{n\,|\,u(n)=0\}$ quand $u=(u(n))$ est une suite récurrente linéaire: A est, à un nombre fini d'exceptions près, une réunion de progressions arithmétiques de même raison.

Plus précisément, on a le théorème suivant:

THÉORÈME 1. — *Soit K un corps de caractéristique nulle, et $u=(u(n))$ une suite récurrente linéaire d'éléments de K. Il existe un entier naturel d non nul tel que, en notant $A_r=\{k\,|\,u(kd+r)=0\}$ $0\leq r\leq d-1$, on ait l'alternative suivante:*

(a) A_r est un ensemble fini.

(b) A_r est égal à $\mathbb{N}$.

On peut préciser que, dans le cas où l'ensemble $A=\{n \mid u(n)=0\}$ est infini, et différent de $\mathbb{N}$, la suite u est telle que, parmi les pôles de la fraction rationnelle $P(x)/Q(x)=\sum u(n)x^n$, il y en ait au moins deux distincts dont le quotient est une racine de l'unité.

La généralisation du théorème 1 que nous démontrons est le théorème 3 énoncé plus loin.

Un autre résultat important sur les suites récurrentes linéaires concerne la structure de l'ensemble des valeurs prises par une telle suite, et est dû, dans le cas $K=\mathbb{Q}$, à G. Polya. On se donne une suite récurrente linéaire $u=(u(n))$, à valeurs dans $\mathbb{Z}$, et un ensemble S fini de nombres premiers rationnels. On suppose que la propriété suivante est vérifiée:

(*) Pour tout n, l'ensemble des diviseurs premiers de $u(n)$ est inclus dans S.

Sous cette hypothèse, G. Polya démontre que la fraction rationnelle $F(x)=P(x)/Q(x)$ a une forme simple. Plus précisément, on a:

THÉORÈME 2. — (G. POLYA, [5]). — *Soit $u=(u(n))$ une suite récurrente linéaire d'éléments de $\mathbb{Z}$. On suppose que u vérifie la propriété (*). Alors il existe un entier d non nul, et des éléments a_r, b_r, $0\leqslant r\leqslant d-1$ dans $\mathbb{Z}$ tels que*

$$F(x)=\sum_{r=0}^{d-1}\frac{a_r x^r}{1-b_r x^d}.$$

Il est équivalent de dire que, pour tout k entier, on a

$$u(kd+r)=a_r(b_r)^k.$$

L'analogue pour un corps de nombres de ce théorème est dû à B. BENZAGHOU [1].

Nous démontrerons plus loin que ce théorème se généralise en caractéristique quelconque (théorème 5).

II. Énoncés des résultats

Nous aurons besoin de la définition suivante:

DÉFINITION 1 ([2], p. 72). — *Soit S une partie de $\mathbb{N}$. On appelle densité banachique supérieure de S, la quantité $d^*(S)$ suivante: $d^*(S)$ est la limite*

supérieure des nombres $Card(I \cap S)/Card(I)$, *où* I *décrit les intervalles de* $\mathbb{N}$ *et* $Card(I)$ *tend vers* $+\infty$.

On dira que S est de densité banachique nulle si $d^+(S)=0$. La généralisation que nous avons en vue du théorème 1 s'énonce alors de la façon suivante:

THÉORÈME 3. — *Soit* K *un corps commutatif de caractéristique* p *non nulle, et* $u(n)$ *une suite récurrente linéaire d'éléments de* K.

Il existe un entier d *supérieur ou égal à* 1, *tel que, en notant* $A_r=\{k \mid u(kd+r)=0\}$ $r=0, 1, \ldots, d-1$, *on ait l'alternative suivante:*

(*a*) A_r *est de densité banachique nulle;*

(*b*) A_r *est égal à* $\mathbb{N}$.

On notera que si A est une partie de $\mathbb{N}$ de densité banachique nulle, elle est de densité arithmétique nulle, mais que l'inverse n'est pas vrai, comme le montre l'exemple $A=\bigcup_{n\geq 1}[n^3, n^3+n]$, *voir* [2], p. 76.

Dans un certain sens, le théorème 3 est le meilleur possible. En effet, un exemple dû à LECH [3] montre que le cas (*a*) du théorème 3 peut se produire, sans que, comme dans le cas de la caractéristique nulle, l'ensemble A_r soit fini: on prend $K=\mathbb{F}_p(z)$, où z est un élément transcendant sur $\mathbb{F}_p$, et pour suite u la suite définie par $u(n)=(1+z)^n-1-z^n$.

On voit alors que l'ensemble $A=\{n \mid u(n)=0\}$ est formé des puissances de p, donc n'est pas fini, et est de densité banachique nulle.

Comme conséquence du théorème 3, on a le résultat suivant dû à C. REUTENAUER [6].

THÉORÈME 4. — *Soient* u *et* v *deux suites récurrentes linéaires, à valeurs dans un corps commutatif* K *de caractéristique quelconque. On suppose que l'on a* $u(n)v(n)=0$ *pour tout* n. *Il existe alors un entier* q *supérieur ou égal à* 1, *et une partition de* $\{0, 1, \ldots, q-1\}=I \cup J$ *telle que*

$$\{n \mid u(n)\neq 0\} \subset I+q\mathbb{N} \qquad et \qquad \{n \mid v(n)\neq 0\} \subset J+q\mathbb{N}.$$

Le théorème 2 dû à G. Polya se généralise de la façon suivante

THÉORÈME 5. — *Soit* K *un corps de caractéristique quelconque, et* G *un sous-groupe de type fini du groupe multiplicatif de* K. *Soit* $u=(u(n))$ *une suite récurrente linéaire d'éléments de* K. *On suppose que, pour tout* n *dans* $\mathbb{N}$, *on a la propriété suivante:*

$$u(n) \quad appartient\ à \quad G \cup \{0\}.$$

Alors il existe un entier d supérieur ou égal à 1, et pour tout r dans $\{0, 1, \ldots, d-1\}$ des éléments a_r dans K et b_r dans $K-\{0\}$, tels que l'on ait pour tout $r \leqslant d-1$ et tout k dans $\mathbb{N}$ la relation $u(kd+r) = a_r (b_r)^k$.

Le théorème 2 est le cas particulier du théorème 5 obtenu en prenant $K=\mathbb{Q}$ et G égal au groupe des S-unités de K. On remarquera que si $\sum u(n) x^n$ a plus de deux pôles distincts et si $u(n)$ vérifie l'hypothèse du théorème 5, ceci entraîne, pour que la conclusion du théorème soit réalisée, que le quotient de deux pôles distincts soit une racine de l'unité. Nous utiliserons plusieurs fois cette remarque dans la démonstration.

III. Rappels

Nous aurons besoin, pour les démonstrations des théorèmes 3, 4 et 5 des résultats suivants:

THÉORÈME 6 (SZEMEREDI, FURSTENBERG, [7], [2]). — *Soit A une partie de $\mathbb{N}$ de densité banachique supérieure strictement positive. Alors A contient des progressions arithmétiques arbitrairement longues.*

THÉORÈME 7 (VAN DER POORTEN, [8]). — *Soit K un corps de caractéristique nulle, et H un sous-groupe de type fini du groupe multiplicatif de K. Soit m un entier naturel non nul. Il existe seulement un nombre fini d'éléments $\underline{x} = (x_0, x_1, \ldots, x_m)$ dans $\mathbf{P}_m(K)$ tels que:*

(a) $x_0 + x_1 + \ldots + x_m = 0$;

(b) x_i *appartient à* H *pour tout* i;

(c) $x_{i_0} + \ldots + x_{i_t} \neq 0$ *pour toute partie non vide et propre* $\{i_0, \ldots, i_t\}$ *de* $\{0, 1, \ldots, m\}$.

THÉORÈME 8 (REUTENAUER [6]). — *Soit K un corps commutatif de caractéristique non nulle p, que l'on suppose algébriquement clos.*

Soit $u = (u(n))$ une suite récurrente linéaire d'éléments de K. Alors il existe un entier d, supérieur ou égal à 1, tel que, pour tout r appartenant à $\{0, 1, \ldots, d-1\}$, la suite $u(kd+r)$ soit ou nulle, ou une somme de séries géométriques, c'est-à-dire s'écrive

$$u(kd+r) = \sum_{i=1}^{t} a_i (b_i)^k \qquad \text{avec} \quad a_i \text{ et } b_i \text{ dans } K.$$

La différence avec le cas caractéristique nulle est que les coefficients polynômiaux P_i [voir la formule (2) de l'introduction] ont disparus.

Soient $f=\sum u(n)x^n$ et $g=\sum v(n)x^n$ deux séries formelles à coefficients dans un corps K de caractéristique quelconque. On appelle produit de Hadamard des séries f et g la série formelle $h=\sum u(n)v(n)x^n$.

Il est clair que la série formelle $\sum x^n=1/(1-x)$ est élément neutre pour le produit de Hadamard.

Il est facile de voir que l'ensemble des séries formelles à coefficients dans K, représentant le développement de Taylor à l'origine des fractions rationnelles à coefficients dans K est une algèbre pour l'addition ordinaire et le produit de Hadamard.

Il se posait alors le problème de caractériser les éléments inversibles de cette algèbre.

Ce problème a été résolu par B. BENZAGHOU dans le cas de la caractéristique nulle [1], et par C. REUTENAUER dans le cas de caractéristique non nulle [6].

On a en effet le résultat suivant:

THÉORÈME 9. — *Soit K un corps commutatif de caractéristique quelconque. Soit $u=(u(n))$ une suite récurrente linéaire d'éléments de K. Alors la série formelle $f=\sum u(n)x^n$ est inversible dans l'algèbre de Hadamard des séries formelles rationnelles, si et seulement si la condition suivante est réalisée. Il existe d plus grand ou égal à 1, et des éléments $a(r)$, $b(r)$ dans $K-\{0\}$, tels que l'on ait pour tout r $r=0, 1, \ldots, d-1$:*

$$u(k\,d+r)=a_r(b_r)^k \quad \textit{pour tout } k \textit{ dans } \mathbb{N}.$$

On notera que dire que u est Hadamard-inversible dans l'anneau des séries formelles rationnelles équivaut à dire que $u(n)$ est non nul pour tout n, et $v(n)=1/u(n)$ est une suite récurrente linéaire.

Remarquer enfin l'analogie entre le théorème 9 et le théorème 5. On peut d'ailleurs, dans le cas de caractéristique nulle, donner une démonstration du théorème 9 utilisant le théorème 5.

IV. Preuve des théorèmes 3 et 4

PREUVE DU THÉORÈME 3

Grâce au théorème 8, on peut supposer que $u(n)$ s'écrit comme somme de séries géométriques, avec les b_i et a_i appartenant à K (en faisant au besoin une extension de K). On peut de plus, en considérant des sous-suites de la forme $u(k\,d+r)$, se ramener au cas où $u(n)$ s'écrit $\sum_{i=1}^{t} a_i b_i^n$.

avec la propriété que pour i différent de j, le quotient de b_i par b_j n'est pas une racine de l'unité, et a_i non nul pour tout i. Ceci étant fait, il nous reste à démontrer que l'ensemble A des indices n dans $\mathbb{N}$ tels que $u(n)=0$ est de densité banachique nulle, si la suite $(u(n)$ n'est pas nulle.

On raisonne par l'absurde, et on suppose $d^+(A)>0$. D'après le théorème 6, il existe alors dans A t éléments en progression arithmétique; on les note $kd+r$, $0\leqslant k\leqslant t-1$. Le système d'équations linéaires en les inconnues X_i: $\sum_{i=1}^{t}(b_i^d)^k X_i=0$, $k=0,\ldots,t-1$, admet alors une solution non triviale, à savoir $X_i=a_i b_i^r$, $i=1,2,\ldots,t$.

Par conséquent, le déterminant du système, qui est un déterminant de Van der Monde construit sur les (b_i^d), est nul. Il existe alors i et j distincts, tels que $b_i^d=b_j^d$. Donc le quotient de b_i par b_j est une racine de l'unité, ce qui est contraire à l'hypothèse faite, et démontre le théorème 3.

Remarque. — On peut aussi démontrer de cette façon le théorème 3 dans le cas de caractéristique nulle, mais il semble difficile de donner une preuve du théorème 1 de cette manière.

Preuve du théorème 4

Nous notons tout d'abord que le théorème 3 est vrai en toute caractéristique compte tenu du théorème 1.

Il existe donc un entier d, supérieur ou égal à 1, tel que, pour tout r, $r=0,1,\ldots,d-1$, chacune des suites $u(kd+r)$, et $v(kd+r)$ vérifie l'une ou l'autre des deux propriétés (a) ou (b) de l'énoncé de ce théorème.

Soit $A_r=\{k\,|\,u(kd+r)=0\}$ et $B_r=\{k\,|\,v(kd+r)=0\}$. On note I l'ensemble des indices r tels que $d^+(A_r)=0$. Si I est vide, on a $u(kd+r)=0$ pour tout k et tout r, donc la suite u est la suite nulle, et il n'y a rien à démontrer.

Si I est non vide, soit r_0 un élément de I. Comme on a $u(kd+r_0)$ $v(kd+r_0)=0$ pour tout k, il en résulte que $v(kd+r_0)$ est nul, sauf peut être pour un ensemble de densité nulle, mais alors $v(kd+r_0)=0$ pour tout k. Ceci démontre que $\{n\,|\,v(n)\neq 0\}\subset {}^cI+d\mathbb{N}$, et on a bien sûr $\{n\,|\,u(n)\neq 0\}\subset I+d\mathbb{N}$, d'où le résultat.

V. Preuve du théorème 5

(A) Le cas de la caractéristique nulle

On se donne un corps K de caractéristique nulle, et on se place dans les hypothèses du théorème 5.

On peut supposer, après avoir au besoin considéré des suites $u(kd+r)$, d entier supérieur ou égal à 1, r appartenant à $\{0, 1, \ldots, d-1\}$, que dans l'expression de $u(n)$ sous la forme $\sum_{i=1}^{t} P_i(n) b_i^n$, aucun des quotients de b_i par b_j quand i est différent de j n'est une racine de l'unité, et que, pour tout n assez grand on ait $u(n) \neq 0$ (grâce au théorème 1).

Sous ces hypothèses, nous allons démontrer que $t=1$, et que le polynôme P_1 est constant.

On écrit la relation de récurrence vérifiée par la suite u sous la forme $d_s u(n+s)+d_{s-1} u(n+s-1)+\ldots+d_0 u(n)=0$, les d_i étant des éléments non tous nuls de K.

Il est clair qu'il existe alors une partie D de $\{0, 1, \ldots, s\}$, de cardinal supérieur ou égal à deux, telle que l'on ait, pour une infinité de valeurs de n les deux propriétés suivantes:

1. $\sum_{j \in D} d_j u(n+j)=0$

2. Pour toute partie D', incluse dans D, non vide et propre, on a $\sum_{j \in D'} d_j u(n+j)$ non nul.

On remarque que si j est dans D, alors d_j est non nul, à cause de la propriété 2.

Soit H le sous-groupe de type fini de $K-\{0\}$ engendré par G et tous les d_j non nuls, et notons $l+1$ le cardinal de D.

D'après le théorème 7, on peut alors trouver un élément $w=(w_j)_{j \in D}$ de $\mathbb{P}_l(K)$, tel que l'on ait, pour une infinité de valeurs de n, l'égalité $(d_j u(n+j))_{j \in D}=w$ dans $\mathbb{P}_l(K)$. Soient i_0 et j_0 deux éléments distincts de D. D'après ce qui précède, on peut trouver e dans $K-\{0\}$, et une infinité de valeurs de n, tels que l'on ait $u(n+j_0)=eu(n+i_0)$.

En supposant $j_0 \geq i_0+1$, et en posant $m=j_0-i_0$, on en déduit l'existence d'une infinité de valeurs de n telles que

$$v(n)=u(n+m)-eu(n)=0.$$

La suite v est récurrente linéaire et possède une infinité de termes nuls. D'après la remarque suivant le théorème 1, si la suite v n'est pas

identiquement nulle, il existe deux pôles distincts de la fraction rationnelle $\sum v(n)x^n$ dont le quotient est une racine de l'unité. Mais on voit facilement que les pôles de la série $\sum v(n)x^n$ sont des pôles de $\sum u(n)x^n$; vu l'hypothèse faite sur la suite u, ceci implique $v(n)=0$ pour tout entier n.

Si l'on pose $F(x)=\sum u(n)x^n$, on a la relation $S(x)=(1-ex^m)F(x)$ où S est un polynôme. Si $F(x)=P(x)/Q(x)$, on voit donc, en faisant l'hypothèse que P et Q sont premiers entre eux, que Q divise le polynôme $1-ex^m$. Donc, Q a toutes ses racines simples, puisqu'il en est ainsi de $1-ex^m$. De plus, si le degré de Q est plus grand que deux, le rapport de deux de ses racines est une racine de l'unité. Donc, $d^0Q=1$, et P_1 est un polynôme constant; et ceci démontre le théorème dans le cas de caractéristique nulle.

(B) Le cas de caractéristique non nulle

Dans le cas particulier où le corps K est fini, le résultat du théorème est tout à fait évident. En effet, la suite récurrente linéaire u prenant un nombre fini de valeurs est alors périodique. Dans le cas général, on peut sans nuire à la généralité supposer que $u(n)$ s'écrit sous la forme d'une somme de séries géométriques: $u(n)=\sum_{i=1}^{t} a_i(b_i)^n$, grâce au théorème 8. D'autre part, on peut supposer que le corps K contient tous les a_i et b_i $1\leqslant i\leqslant t$, et est de type fini sur $\mathbb{F}_p$.

Nous appelons alors s le degré de transcendance de K sur $\mathbb{F}_p$, et nous allons démontrer le théorème 5 par récurrence sur s. Pour $s=0$, c'est le cas d'un corps fini, et le théorème est vrai dans ce cas.

Nous supposons donc, à partir de ce moment, le théorème vrai pour un corps K de degré de transcendance inférieur ou égal à $s-1$ (s entier $s\geqslant 1$), et nous nous plaçons dans le cas où le degré de transcendance du corps K est s.

Lemme 1. — *On peut supposer que le corps K est une extension galoisienne de $\mathbb{F}_p(T_1,\ldots,T_s)$, où $T_1,\ldots,T_s$ sont des éléments de K algébriquement indépendants sur $\mathbb{F}_p$.*

Preuve. — On choisit une base de transcendance $T_1,\ldots,T_s$ de K sur $\mathbb{F}_p$, de sorte que K est une extension algébrique finie de $\mathbb{F}_p(T_1,\ldots,T_s)$. On peut toujours supposer que K est extension normale de $\mathbb{F}_p(T_1,\ldots,T_s)$.

Il existe alors une extension galoisienne L de $\mathbb{F}_p(T_1,\ldots,T_s)$ telle que K soit extension purement inséparable de L.

Il existe donc un entier naturel e, tel que, pour tout x élément de K, x^{p^e} appartienne à L. On peut d'autre part supposer, en considérant des progressions arithmétiques, que la suite $u(n)$ s'écrit sous la forme $\sum_1^t a_i(b_i)^n$, avec, pour i différent de j, la propriété que le quotient de b_i par b_j ne soit pas une racine de l'unité.

On applique alors l'homomorphisme $x \to x^{p^e}$, qui est injectif. On a alors que $v(n) = u(n)^{p^e} = \sum_1^t a_i^{p^e}(b_i^{p^e})^n$ est une suite récurrente qui possède les propriétés énoncées dans le théorème, et $a_i^{p^e}$, $b_i^{p^e}$ appartiennent à L; comme le quotient de $b_i^{p^e}$ par $b_j^{p^e}$, pour i différent de j, n'est pas une racine de l'unité, on en déduit, en appliquant le théorème 5 supposé vrai pour L, que $t = 1$, ce qui démontre le lemme 1.

LEMME 2. — *On peut supposer que*

(*a*) *K est Galoisien sur $\mathbb{F}_p(T_1, \ldots, T_s)$;*

(*b*) *la suite $u(n)$ est à valeurs dans $\mathbb{F}_p[T_1, \ldots, T_s]$.*

Preuve. — Le fait que l'on puisse supposer K galoisien sur $\mathbb{F}_p(T_1, \ldots, T_s)$ est le lemme 1. On se place donc dans ce cas. Il existe H non nul dans $\mathbb{F}_p[T_1, \ldots, T_s]$ tel que $H^{n+1}u(n)$ soit, pour tout n, entier sur $\mathbb{F}_p[T_1, \ldots, T_s]$. Comme la suite $H^{n+1}u(n)$ vérifie encore les hypothèses du théorème, on peut donc supposer dès le départ que $u(n)$ est entier sur $\mathbb{F}_p[T_1, \ldots, T_s]$ pour tout n.

Soit alors N la norme de K sur $\mathbb{F}_p(T_1, \ldots, T_s)$, et v la suite définie par $v(n) = N(u(n))$.

Pour tout n, on a $v(n) \in \mathbb{F}_p[T_1, \ldots, T_s]$, et $v(n)$ appartient à un sous-groupe de type fini du groupe multiplicatif du corps $\mathbb{F}_p(T_1, \ldots, T_s)$.

Par conséquent, si le théorème est vrai dans ce cas, il existe d, entier supérieur ou égal à r, tel que, pour tout r, ou la suite $v(kd+r)$ est nulle, ou elle est Hadamard-inversible. Mais alors, la suite $u(kd+r)$ est, ou nulle, ou Hadamard inversible; dans ce dernier cas, elle est de la forme indiquée dans le théorème 5 (pour un d' convenable), grâce au théorème 9, et ceci démontre le lemme 2.

Nous nous plaçons donc dans les hypothèses du lemme 2, et nous terminons la démonstration du théorème 5. On peut écrire pour tout n,

$$u(n) = c_n H_1^{l_1(n)} \ldots H_m^{l_m(n)},$$

où les H_j sont des polynômes irréductibles distincts et fixés de $\mathbb{F}_p[T_1, \ldots, T_s]$, et c_n une suite d'éléments de $\mathbb{F}_p$, grâce à l'hypothèse sur l'image de u.

On suppose de plus que la suite u n'est pas identiquement nulle, et s'écrit $u(n)=\sum_1^t a_i(b_i)^n$, le rapport de deux des b_i d'indices distincts n'étant pas une racine de l'unité, et aussi que les a_i et b_i sont entiers sur $\mathbb{F}_p[T_1, \ldots, T_s]$.

Nous allons démontrer qu'il existe une progression arithmétique kd_0+r_0, d_0 entier supérieur ou égal à un, r_0 appartenant à $\mathbb{N}$, telle que toutes les fonctions $l_j(kd_0+r_0)$ soient des fonctions affines de k.

Nous notons pour cela H l'un quelconque des polynômes H_j, et nous le démontrons pour H, ce qui suffira clairement. Nous introduisons sur le corps $\mathbb{F}_p(T_1, \ldots, T_s)$ la valuation H-adique v_H, en posant, pour $F=P/G=H^q(P_1/Q_1)$ où $q\in\mathbb{Z}$, et H ne divise ni P_1 ni Q_1, $v_H(F)=q$, en nous inspirant de la démonstration du théorème 9 faites dans [1] dans le cas d'un corps de nombres.

Soit w_H une extension de v_H au corps K, et π une uniformisante pour le corps valué (K, w_H).

On écrit $b_i=\pi^{\theta_i}\beta_i$, avec $\theta_i\in\mathbb{N}$, β_i unité w_H-adique, et on note $I=\{i \mid \theta_i$ est minimal$\}$, et θ la valeur commune des θ_i pour i appartenant à I.

Soit $a(n)=\sum_{i\in I} a_i\beta_i^n$. La suite $a(n)$ est une suite récurrente linéaire, et vérifie une relation de récurrence linéaire du type

$$a(n+h)=\varphi_{h-1}a(n+h-1)+\ldots+\varphi_0 a(n),$$

les φ_j étant dans l'anneau de valuation de w_H pour tout j, et φ_0 étant une unité w_H-adique, puisque tous les β_j sont des unités w_H-adique. Soit l un entier naturel tel que, pour k variant entre 0 et $h-1$, $\pi^{-l}a(k)$ soit dans l'anneau de valuation, et qu'il existe k_0, $0\leqslant k_0\leqslant h-1$, tel que $\pi^{-l}a(k_0)$ soit une unité w_H-adique. Soit $b(n)=\pi^{-l}a(n)$, la suite $b(n)$ est à valeurs dans l'anneau de valuation de w_H pour tout n, et son image dans le corps résiduel de (K, w_H) n'est pas identiquement nulle, puisque l'un au moins des $b(k)$, $k=0, 1, \ldots, h-1$ est une unité w_H-adique. La suite $b(n)$ vérifie la même relation de récurrence que la suite $a(n)$; donc l'image $\bar{b}(n)$ de $b(n)$ dans le corps résiduel de (K, w_H) vérifie

$$\bar{b}(n+h)=\bar{\varphi}_{h-1}\bar{b}(n+h-1)+\ldots+\bar{\varphi}_0\bar{b}(n).$$

Il en résulte, puisque $\bar{\varphi}_0$ n'est pas nul et que la suite $\bar{b}(n)$ est non identiquement nulle, qu'il existe une infinité de valeurs de n telles que $\bar{b}(n)$ soit non nul.

Soit maintenant $r(n)$ la suite $\pi^{l-\theta n}u(n)=b(n)+d(n)$.

Cette suite est, pour n assez grand, dans l'anneau de valuation de (K, w_H), et son image dans le corps résiduel $\bar{r}(n)$ est égale à $\bar{b}(n)$. Elle est donc non nulle pour une infinité de valeurs de n.

D'autre part, puisque $u(n)$ est soit nul, soit appartient à un sous-groupe de type fini de K^*, il en est de même de $r(n)$, et donc aussi de son image $\bar{r}(n)$ dans le corps résiduel.

Or, d'après N. Bourbaki, algèbre commutative, chapitre 6, § 10, n° 3, p. 167, corollaire 4, le corps résiduel de (K, w_H) a un degré de transcendance strictement plus petit que celui de K, qui est s.

On peut donc appliquer l'hypothèse de récurrence à la suite $\bar{r}(n)$: il existe un entier d_0 non nul, et des éléments a_r^* et b_r^* du corps résiduel de (K, w_H), tels que, pour tout k assez grand, on ait: $\bar{r}(kd_0+r)=a_r^*(b_r^*)^k$, pour $r=0, 1, \ldots, d_0-1$.

Comme la suite $\bar{r}(n)$ a une infinité de termes non nuls, il existe au moins un indice r_0 tel que l'on ait $a_{r_0}^*$ et $b_{r_0}^*$ non nuls.

Il en résulte facilement que la valuation v_H-adique de $u(kd_0+r_0)$ est une fonction affine de k.

La suite $c(kd_0+r_0)$ [*voir* l'expression de départ pour $u(n)$] est alors une suite récurrente, toujours non nulle, et à valeurs dans $\mathbb{F}_p$; elle est donc périodique, et on peut la supposer constante, égale à c.

On a donc, pour tout k assez grand

$$\sum_{i=1}^{t} a_i (b_i)^{r_0} (b_i^{d_0})^k - c H_1^{\alpha_1} \ldots H_1^{\alpha_m} \ldots H_m^{\alpha_m} (H_1^{\beta_1} \ldots H_m^{\beta_m})^k = 0.$$

Cette relation implique qu'il existe i_0 tel que l'on ait $b_{i_0}^{d_0} = H_1^{\beta_1} \ldots H_m^{\beta_m}$, d'où la relation

$$\sum_{i \neq i_0} a_i (b_i)^{r_0} (b_i^{d_0})^k + (a_{i_0} b_{i_0}^{r_0} - c H_1^{\alpha_1} \ldots H_m^{\alpha_m}) (b_i^{d_0})^k = 0.$$

Comme tous les $b_i^{d_0}$ sont distincts, une telle relation n'est possible que s'il n'y a pas d'indice différent de i_0, donc $t=1$, ce qui termine la démonstration du théorème 5.

Remarque. – Il serait intéressant, dans le cas de caractéristique non nulle, de décrire plus explicitement ce qui se passe quand l'ensemble $A = \{ n \mid u(n) = 0 \}$ des zéros d'une suite récurrente linéaire est infini, et de densité nulle.

En particulier, peut-on décrire cet ensemble à l'aide de progressions géométriques, comme dans l'exemple de LECH ?

BIBLIOGRAPHIE

[1] BENZAGHOU (B.). – Algèbres de Hadamard, *Bull. Soc. Math. France*, vol. 98, 1970, p. 209-252.

[2] FURSTENBERG (H.). – *Recurrence in ergodic theory and combinatorial number theory*, Princeton University Press, 1981.

[3] LECH (C.). – A note on recurring series, *Ark Mat.*, vol. 2, 1952, p. 417-421.

[4] MAHLER (K.). – On the Taylor coefficients of rational functions, *Proc. Cambridge Phil. soc.*, vol. 52, 1956, p. 39-48.

[5] POLYA (G.). – Arithmetische Eigenschaften der Reiherentwicklungen rationaler Funktionen, *Journal für die reine ungewandk Math.*, vol. 151, 1921, p. 1-21.

[6] REUTENAUER (C.). – Sur les éléments inversibles de l'algèbre de Hadamard des séries rationnelles, *Bull. soc. Math. France.*, vol. 110, 1982, p. 225-232.

[7] SZEMEREDI (E.). – On sets of integers containing no k elements in arithmetic progression, *Acta Math.*, vol. 27, 1975, p. 199-245.

[8] VAN DER POORTEN (A. J.). – Additive relations in number fields, *Séminaire de théorie des nombres de Paris*, 1982-1983, p. 259-266. *Progress in Math.*, 1984, Birkhaüser-Boston.