JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

JEAN-PAUL ALLOUCHE

Note sur un article de Sharif et Woodcock

Journal de Théorie des Nombres de Bordeaux, tome 1, n° 1 (1989), p. 163-187

<http://www.numdam.org/item?id=JTNB_1989__1_1_163_0>

Séminaire de Théorie des Nombres,
Bordeaux, 1, *163–187 (1989)*

Note sur un article de Sharif et Woodcock

par JEAN-PAUL ALLOUCHE

Résumé—H. Sharif et C. Woodcock donnent dans [26] une caractérisation des séries formelles à coefficients dans un corps K de caractéristique non nulle et algébriques sur $K(X)$; ils en déduisent simplement l'algébricité du produit de Hadamard ou des diagonales de séries algébriques. (Ces résultats ont aussi été obtenus par T. Harase [14]). Nous donnons ici une démonstration légèrement différente de leur théorème et montrons comment on peut en déduire une généralisation intéressante de la notion de p^k-substitution sur un alphabet infini (inclus dans un corps de caractéristique p). Dans la dernière partie de cet article nous revenons sur l'indépendance algébrique de certaines séries formelles étudiées dans [2].

Abstract — H. Sharif and C. Woodcock give in [26] a characterization of formal power series with coefficients in a field K of positive characteristic, which are algebraic over $K(X)$. They deduce in a simple way from this theorem the algebraicity of Hadamard products and diagonals of algebraic power series. (These results have been also obtained by T. Harase [14]). We give here a slightly different proof of their theorem and we show how it can lead to an interesting generalization of the notion of p^k-substitution on an infinite alphabet (included in a field of characteristic p). In the last part of this paper we come back to the algebraic independence of certain formal power series which have been previously studied in [2].

1 - Introduction

Comment reconnaître si une série formelle est algébrique ? Plus précisément, étant donné un corps K (commutatif), une série formelle en les variables $X_1, \cdots, X_r$ (c'est-à-dire un élément de $K((X_1, \cdots, X_r))$) est dite *algébrique* si elle est algébrique sur le corps de fractions rationnelles $K(X_1, \cdots, X_r)$.

Par exemple :

$\sqrt{X}$ n'est pas une série formelle algébrique (il n'existe pas de série formelle F qui vérifie $F^2 = X$),

$\sum_{n=0}^{+\infty} \binom{2n}{n} X^n = (1-4X)^{-1/2}$ est algébrique quel que soit le corps K,

Manuscrit reçu le 10 avril 1989

$\sum_{n=0}^{+\infty} X^{q^n}$ est algébrique si q est une puissance de la caractéristique du corps K, et transcendante dans le cas contraire (voir [29]).

La question à laquelle nous nous intéressons ici est de reconnaître si une série formelle est algébrique et de déterminer quelles opérations conservent l'algébricité.

En 1967 Furstenberg propose ([13]) d'appeler un ensemble d'entiers A *algébrique* sur le corps K si la série formelle $\sum_{n\in A} X^n$ est algébrique sur $K(X)$, et il se demande si par exemple l'intersection de deux ensembles algébriques est algébrique. Comme la série formelle associée à l'intersection de A et de B n'est autre que le produit de Hadamard des séries $\sum_{n\in A} X^n$ et $\sum_{n\in B} X^n$ (rappelons que le produit de Hadamard des séries $\sum_{n=0}^{+\infty} a_n X^n$ et $\sum_{n=0}^{+\infty} b_n X^n$ est le produit "naïf" $\sum_{n=0}^{+\infty} a_n b_n X^n$), apparaît aussitôt une question (apparemment) plus générale : le produit de Hadamard de deux séries algébriques est-il algébrique ? Un autre problème abordé par Furstenberg dans cet article concerne les diagonales des séries formelles : si la série formelle

$$\sum_{n_1,\cdots,n_r} a(n_1,\cdots,n_r) X_1^{n_1}\cdots X_r^{n_r}$$

est rationnelle (c'est-à-dire appartient au corps $K(X_1\cdots,X_r)$), peut-on affirmer que la série "diagonale" $\sum_n a(n,\cdots,n)X^n$ est algébrique (sur le corps $K(X)$) ? Furstenberg répond à cette question dans le cas d'un corps de caractéristique non nulle et il formule et démontre une réciproque dans le cas d'un corps fini.

Cette question peut être étendue dans un sens : la diagonale d'une série formelle algébrique est-elle algébrique ? Cette question, comme on le verra plus loin, est très liée à l'algébricité du produit de Hadamard : des réponses sont données dans les articles de Fliess ([10]), de Deligne ([8]), de Denef et Lipshitz ([9]), de Salon ([23]), de Sharif et Woodcock ([26]) et de Harase ([14]) ; pour toutes les questions de diagonales il ne faut pas manquer de consulter les travaux de Christol, en particulier [6].

Nous vous proposons ici d'abord d'indiquer "l'état de l'art" sur ces questions, ensuite de montrer qu'une lecture "entre les lignes" des articles de Sharif et Woodcock ([26)] et de Harase ([14]) permet de généraliser la notion de suite engendrée par substitution de longueur constante au cas d'une suite

à plusieurs indices et à valeurs dans un corps de caractéristique non nulle (le corps n'étant pas nécessairement fini), de sorte que l'on ait le théorème : *Une suite $a(n_1, \cdots, n_r)$ à valeurs dans un corps K de caractéristique $p \neq 0$ est engendrée par une p-substitution si et seulement si la série formelle $\sum_{n_1,\cdots,n_r} a(n_1, \cdots, n_r) X_1^{n_1} \cdots X_r^{n_r}$ est algébrique sur $K(X_1, \cdots, X_r)$.*

Ce théorème est démontré dans le cas d'un corps fini par Christol, Kamae, Mendès France et Rauzy ([7]) pour les suites à un indice, et par Salon ([23]) pour les suites à plusieurs indices. On pourra aussi se reporter aux articles de Christol [4] et [5], de Denef et Lipshitz [9], et au récent survol de Lipshitz et van der Poorten [18].

Dans la dernière partie nous reviendrons sur le problème de l'indépendance algébrique des séries formelles $(1+X)^\lambda$ où λ est un entier p-adique, qui a été abordé dans [2] (voir aussi [19]).

2 - Deux résultats préliminaires

Le premier résultat que nous donnons ici est l'équivalence de deux questions posées plus haut :

PROPOSITION 1. *Soit K un corps (commutatif). Les deux propriétés suivantes sont équivalentes :*

a) le produit de Hadamard de tout couple de séries formelles (à un nombre fini de variables) algébriques est lui-même algébrique.

b) toute diagonale d'une série formelle (à un nombre fini de variables) algébrique est algébrique.

DÉMONSTRATION: La démonstration de l'implication $b \Rightarrow a$ est inspirée d'une démonstration donnée par Furstenberg, l'implication $a \Rightarrow b$ est donnée par Sharif et Woodcock dans [26], l'équivalence est évoquée dans le papier de Lipshitz et Van der Poorten [18].

Montrons d'abord que $a \Rightarrow b$:

soit $\sum a(n_1, \cdots, n_r) X_1^{n_1} \cdots X_r^{n_r}$ une série formelle algébrique, et montrons, quitte à renuméroter les variables, que la série

$$G(X, X_{k+1}, \cdots, X_r) = \sum_{n, n_{k+1}, \cdots, n_r} a(n, n, \cdots, n, n_{k+1}, \cdots, n_r) X^n X_{k+1}^{n_{k+1}} \cdots X_r^{n_r}$$

est algébrique sur le corps $K(X, X_{k+1}, \cdots, X_r)$. D'après l' hypothèse, le produit de Hadamard de la série initiale et de la série rationnelle (donc algébrique)

$$\frac{1}{1-X_1\cdots X_k}\prod_{j=k+1}^{r}\frac{1}{1-X_j}=\sum_{n,n_{k+1},\cdots,n_r}(X_1\cdots X_k)^n X_{k+1}^{n_{k+1}}\cdots X_r^{n_r}$$

est algébrique. Mais ce produit vaut :

$$\sum_{n,n_{k+1},\cdots,n_r} a(n,n,\cdots,n,n_{k+1},\cdots,n_r)(X_1\cdots X_k)^n X_{k+1}^{n_{k+1}}\cdots X_r^{n_r}$$
$$= G(X_1\cdots X_k, X_{k+1},\cdots,X_r),$$

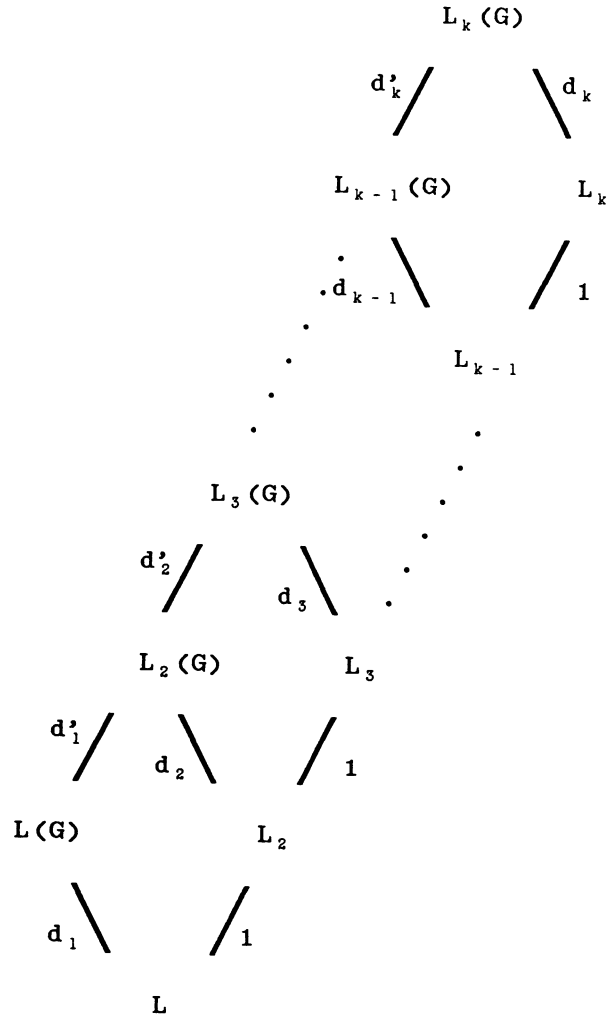
et le fait qu'il soit algébrique sur

$$K(X_1,X_2,\cdots,X_r)=K(X_1\cdots X_k,X_2,\cdots X_r)$$

signifie que $G(X,X_{k+1},\cdots,X_r)$ est algébrique sur $K(X,X_2,\cdots,X_r)$ (les variables $X_1\cdots X_k,X_2,\cdots,X_r$ sont algébriquement indépendantes sur K). Notons alors

$$L=K(X,X_{k+1},\cdots,X_r),$$
$$L_2=L(X_1),\ L_3=L_2(X_3),\cdots,L_k=L_{k-1}(X_k)$$

(d'où $L_k=K(X,X_2,X_3,\cdots,X_k)$) et regardons les degrés de transcendance des extensions suivantes :



Mais X_j est transcendant sur $L_{j-1}(G)$: si une expression polynomiale $\sum_{t=0}^{d} c_t\, X_j^t$, à coefficients dans $L_{j-1}(G)$, est nulle, comme c'est une série formelle en les variables $X, X_2, \cdots, X_{j-1}, X_j, X_{k+1}, \cdots X_r$, c'est que X_j "n'y apparaît pas", autrement dit que $c_t = 0$ pour $t \geq 1$. Ainsi $d'_j = 1$ quel que soit j, et comme on a $d_j + d'_j = d_{j+1} + 1$, on en déduit que $d_1 = d_2 = \cdots = d_k$. Mais d_k est nul car G est algébrique sur L_k, donc $d_1 = 0$, autrement dit G est algébrique sur $L = K(X, X_{k+1}, \cdots, X_r)$.

Pour montrer à rebours que b implique a, on se donne deux séries for-

melles algébriques

$$\sum a(n_1,\cdots,n_r)X_1^{n_1}\cdots X_r^{n_r} \text{ et } \sum b(m_1,\cdots,m_r)\, X_1^{m_1}\cdots X_r^{m_r}.$$

Soient $Y_1,\cdots,Y_r$ d'autres variables (c'est-à-dire que l'on suppose que $X_1,\cdots,X_r,Y_1,\cdots,Y_r$ sont algébriquement indépendantes sur K). La série

$$\sum b(m_1,\cdots,m_r)Y_1^{m_1}\cdots Y_r^{m_r}$$

étant algébrique sur $K(Y_1,\cdots,Y_r)$, on voit que la série

$$\sum_{\substack{n_1,\cdots,n_r\\ m_1,\cdots,m_r}} a(n_1,\cdots,n_r)b(m_1,\cdots,m_r)\, X_1^{n_1}\cdots X_r^{n_r}Y_1^{m_1}\cdots Y_r^{m_r}$$

est algébrique sur $K(X_1,\cdots,X_r,Y_1,\cdots,Y_r)$, puisque c'est le produit de deux séries algébriques sur ce corps. En prenant plusieurs fois des "diagonales partielles" de cette dernière série, on obtient que la série formelle $\sum a(n_1,\cdots,n_r)b(n_1,\cdots,n_r)X_1^{n_1}\cdots X_r^{n_r}$, c'est-à-dire précisément le produit de Hadamard des deux séries initiales, est algébrique sur le corps $K(X_1,\cdots,X_r)$.

Remarque : Comme nous l'a indiqué le referee toute diagonale s'obtient par une succession de diagonalisations portant sur deux termes, il suffit donc de démontrer l'implication $a \Rightarrow b$ dans ce cas-là, le seul avantage de la rédaction ci-dessus est de donner directement toute diagonale comme un (seul) produit de Hadamard.

Le second résultat que nous donnons ici permet de jouer avec des surcorps L du corps K, il est donné dans [26], (mais aussi dans [14] avec l'hypothèse -inutile- de l'algébricité de L sur K) :

PROPOSITION 2. *Soient K et L deux corps commutatifs avec $K \subset L$. Soit $F(X_1,\cdots,X_r)$ une série formelle dans $K((X_1,\cdots,X_r))$. F est algébrique sur $L(X_1,\cdots,X_r)$ si et seulement si elle est algébrique sur $K(X_1,\cdots,X_r)$.*

Nous modifions légèrement la démonstration donnée dans [26] :

il est clair que l'algébricité de F sur $K(X_1,\cdots,X_r)$ implique l'algébricité de F sur $L(X_1,\cdots,X_r)$.

Supposons à rebours que F est algébrique sur $L(X_1,\cdots,X_r)$, il existe donc des polynômes $a_j(X_1,\cdots,X_r)$ à coefficients dans L, non tous nuls, tels que

$$(*) \qquad \sum_{j=0}^{d} a_j(X_1,\cdots,X_r)F^j(X_1,\cdots,X_r) = 0.$$

Notons $a_j(X_1,\cdots,X_r) = \sum_{n_1,\cdots,n_r} b_j(n_1,\cdots,n_r)X_1^{n_1}\cdots X_r^{n_r}$, où les b_j sont dans L et la somme finie. Il existe un $(n+1)$-uple $(k,m_1,\cdots,m_r)$ tel que $\gamma = b_k(m_1,\cdots,m_r)$ soit non nul. On construit alors une base $\mathcal{B}$ de L sur K de la façon suivante : si γ est dans K, on complète γ en une K-base $\mathcal{B}$ de L ; si γ n'est pas dans K, on complète $\{1,\gamma\}$ en une K-base $\mathcal{B}$ de L. On peut alors définir une application K-linéaire φ de L dans K en imposant comme valeurs sur $\mathcal{B}$:

$$\varphi(x) = x \text{ si } x \in \{\gamma\} \cup (\mathcal{B} \cap K)$$
$$\varphi(x) = 0 \text{ sinon.}$$

La définition de φ montre que $\varphi|_K$ est l' identité sur K (ce qui n'est pas nécessairement le cas dans la démonstration donnée dans [26]). On prolonge alors φ à $L[X]$, puis à $L((X))$ par $\varphi(X^n) = X^n$, et la relation $(*)$ implique :

$$\sum_{j=0}^{d} (\varphi a_j)(X_1,\cdots,X_r)F^j(X_1,\cdots,X_r) = 0.$$

Les polynômes $(\varphi a_j)(X_1,\cdots,X_r)$ sont à coefficients dans K, et ne sont pas tous nuls (par choix de φ on a $(\varphi a_k) \neq 0$), donc F est algébrique sur $K(X_1,\cdots,X_r)$.

3 - Le théorème fondamental en caractéristique non nulle.

Nous allons donner un théorème de caractérisation des séries formelles algébriques dans le cas où le corps de base est de caractéristique non nulle. Ce théorème se trouve en majeure partie (l'équivalence entre a et b ou b') dans l'article de Sharif et Woodcock [26], ainsi que dans celui d'Harase [14] dans le cas où le corps de base est parfait ; on pourra aussi consulter l'article de Christol [5] qui étend les résultats au cas où le corps de base est non archimédien d'inégales caractéristiques, et celui de Denef et Lipshitz [9]. La perfection du corps de base étant sans importance d'après la proposition 2, nous avons préféré formuler le théorème dans le cas d'un corps quelconque, plutôt que d'indiquer pour chaque application, comme dans [26] et [14], comment supprimer la condition de perfection (par exemple ici les espaces vectoriels utilisés ne sont pas sur le corps de base mais sur un surcorps parfait de ce corps). La preuve que nous donnons est élémentaire, elle est très inspirée de [26] et [14] (voir aussi [4], [7], et [23] pour l'inspiration à partir du cas d'un corps fini). On pourra aussi consulter [8] qui n'est pas élémentaire. Nous indiquerons plus loin comment la nouvelle condition (c) permet de généraliser la notion de substitution.

THÉORÈME FONDAMENTAL. *Soit K un corps commutatif de caractéristique non nulle p, et soit $\overline{K}$ un corps parfait qui contient K (par exemple $\overline{K} = \Omega$ ou $\overline{K} = K^{p^{-\infty}}$, une clôture algébrique ou radicielle de K). Soit $(a(n_1, ..., n_r))$ une suite à valeurs dans K, soit enfin $s \geq 1$ un entier. Les quatre propriétés suivantes sont équivalentes :*

a) la série formelle $\sum_{n_i \geq 0} a(n_1, \cdots, n_r) X_1^{n_1} \cdots X_r^{n_r}$ est algébrique sur le corps $K(X_1, \cdots, X_r)$,

b) il existe un $\overline{K}$-espace vectoriel $\mathcal{W}$ de suites, de dimension finie sur $\overline{K}$, qui contient la suite a et stable par les applications

$$(b(n_1, \cdots, n_r)) \to (b^{1/q}(qn_1 + j_1, \cdots, qn_r + j_r)),$$

pour $0 \leq j_1, \cdots, j_r \leq q - 1$,

b') L'espace vectoriel engendré sur $\overline{K}$ par l'ensemble de suites

$$\{(a^{1/q^k}(q^k n_1 + j_1, \cdots, q^k n_r + j_r));\ k \geq 0\ ;\ 0 \leq j_1, \cdots, j_r \leq q^k - 1\}$$

est de dimension finie sur $\overline{K}$,

c) il existe un entier $c \geq 1$, une famille de matrices carrées à c lignes et c colonnes $\{A_{j_1, \cdots, j_r}\ ;\ 0 \leq j_1, \cdots, j_r \leq q - 1\}$, et une suite $(U(n_1, \cdots n_r))$ à valeurs dans $\overline{K}^c$ tels que

i) si φ est la première projection canonique de $\overline{K}^c$ sur $\overline{K}$, on a $\varphi(U) = a$,

ii) $\forall (j_1, ..., j_r) \in [0, q-1]^r$, $\forall (n_1, \cdots, n_r) \in \mathbb{N}^r$, on a :

$$U^{1/q}(qn_1 + j_1, \cdots, qn_r + j_r) = A_{j_1, \cdots, j_r}\ U(n_1, \cdots n_r)$$

où $U^{1/q}$ est le vecteur dont les composantes dans la base canonique sont les racines $q^{\text{èmes}}$ de celles de U.

Remarques :

. L'entier s du théorème ($q = p^s$, $s \geq 1$) est quelconque, ce qui implique en particulier que si une suite vérifie ces propriétés pour un s, elle les vérifie quel que soit s entier strictement positif.

. Les propriétés b et b' sont clairement équivalentes.

. La condition c est liée à la *reconnaissabilité* d'une certaine série en plusieurs variables non comutatives (voir l'article de Schützenberger [25]).

DÉMONSTRATION DU THÉORÈME :

Notons $E_{j_1,\cdots,j_r}$ l'opérateur défini sur $\overline{K}[[X_1,\cdots,X_r]]$ par

$$E_{j_1,\cdots,j_r}\Big(\sum_{n_i\geq 0} a(n_1,\cdots,n_r)X_1^{n_1}\cdots X_r^{n_r}\Big)$$
$$= \sum_{n_i\geq 0} a^{1/q}(qn_1+j_1,\cdots,qn_r+j_r)X_1^{n_1}\cdots X_r^{n_r}.$$

Pour deux séries formelles quelconques A et B, et pour λ dans $\overline{K}$ on a :

$$A(X_1,\cdots,X_r) = \sum_{0\leq j_1,\cdots,j_r\leq q-1} X_1^{j_1}\cdots X_r^{j_r}(E_{j_1,\cdots,j_r}(A))^q$$
$$E_{j_1,\cdots,j_r}(A+\lambda B) = E_{j_1,\cdots,j_r}(A) + \lambda^{1/q}E_{j_1,\cdots,j_r}(B)$$
$$E_{j_1,\cdots,j_r}(A^qB) = AE_{j_1,\cdots,j_r}(B).$$

Remarquons que $E_{j_1,\cdots,j_r}$ est bien défini car le corps $\overline{K}$ est parfait, donc l'application $\alpha \to \alpha^q$, itérée de l'application de Frobenius est surjective ; la première et la deuxième propriété de l'opérateur E sont immédiates, si l'on n'oublie pas (pour la première) que l'application de Frobenius, et donc ses itérées, sont des homomorphismes de corps.

La dernière de ces relations se montre en choisissant successivement $A = X_j$, puis $A = X_j^\ell$, puis A égal à un monôme en $X_1,\cdots,X_r$, puis à un polynôme, puis à une série formelle.

- Montrons alors que a implique b :

Comme la série

$$F(X_1,\cdots,X_r) = \sum_{n_i\geq 0} a(n_1,\cdots,n_r)X_1^{n_1}\cdots X_r^{n_r}$$

est algébrique sur $K(X_1,\cdots,X_r)$, donc sur $\overline{K}(X_1,\cdots,X_r)$, il existe des a_j dans $\overline{K}[X_1,\cdots,X_r]$, non tous nuls, tels que

$$\sum_{j=0}^{d} a_j(X_1,\cdots,X_r)F^{q^j}(X_1,\cdots,X_r) = 0.$$

Si cette relation est choisie de longueur minimale, alors on a $a_0 \neq 0$, en effet si l'on avait :

$$\sum_{j=e}^{d} a_j(X_1,\cdots,X_r)F^{q^j}(X_1,\cdots,X_r) = 0 \text{ avec } e\geq 1 \text{ et } a_e\neq 0,$$

alors quels que soient $k_1, \cdots, k_r$ dans $[0, q-1]$:

$$\sum_{j=e}^{d} E_{k_1,\cdots,k_r}(a_j(X_1,\cdots,X_r)F^{q^j}(X_1,\cdots,X_r)) = 0,$$

c'est-à-dire

$$(**) \qquad \sum_{j=e}^{d}(E_{k_1,\cdots,k_r}(a_j(X_1,\cdots,X_r))F^{q^{j-1}}(X_1,\cdots,X_r) = 0.$$

Comme $a_e = \sum_{0\leq k_1,\cdots,k_r\leq q-1} X_1^{k_1}\cdots X_r^{k_r}\ E_{k_1,\cdots,k_r}(a_e)$ est non nul, c'est donc que l'un des $E_{k_1,\cdots,k_r}(a_e)$ est non nul, et donc que $(**)$ est une relation plus courte que la relation initiale.

Posons alors $G(X_1,\cdots,X_r) = \frac{F(X_1,\cdots,X_r)}{a_0(X_1,\cdots,X_r)}$, la relation initiale s'écrit :

$$G = -\sum_{j=1}^{d} a_j(X_1,\cdots,X_r)a_0^{q^j-2}(X_1,\cdots,X_r)G^{q^j}(X_1,\cdots,X_r).$$

Soit alors $\mathcal{V}$ l'ensemble de séries formelles défini par :

$$\mathcal{V} = \{H \in \overline{K}[[X_1,\cdots,X_r]]\ ;\ H = \sum_{j=0}^{d} b_j G^{q^j}\ ; b_j \in \overline{K}[X_1,\cdots,X_r]\ ;\ d^\circ b_j \leq D\}$$

où $d^\circ b_j$ représente le degré maximal de b_j, et où

$$D = max\{d^\circ a_0, d^\circ(a_1 a_0^{q-2}), d(a_2 a_0^{q^2-2}), \cdots, d^\circ(a_d a_0^{q^d-2})\}.$$

$\mathcal{V}$ est un $\overline{K}$-espace vectoriel de dimension finie, qui contient $F = a_0 G$ et qui est invariant par les $E_{k_1,\cdots,k_r}$ puisque, si $0 \leq k_1,\cdots,k_r \leq q-1$, on a

pour H dans $\mathcal{V}$:

$$\begin{aligned} E_{k_1,\cdots,k_r}(H) &= E_{k_1,\cdots,k_r}(\sum_{j=0}^{d} b_j G^{q^j}) \\ &= E_{k_1,\cdots,k_r}(-b_0(\sum_{j=1}^{d} a_j a_0^{q^j-2} G^{q^j}) + \sum_{j=1}^{d} b_j G^{q^j}) \\ &= E_{k_1,\cdots,k_r}(\sum_{j=1}^{d}(b_j - b_0 a_j a_0^{q^j-2}) G^{q^j}) \\ &= \sum_{j=1}^{d} E_{k_1,\cdots,k_r}(b_j - b_0 a_j a_0^{q^j-2}) G^{q^{j-1}} \end{aligned}$$

et ce dernier élément est bien dans $\mathcal{V}$, car

$$d^\circ E_{k_1,\cdots,k_r}(b_j - b_0 a_j a_0^{q^j-2}) \leq \frac{2D}{q} \leq D.$$

Il suffit alors d'appeler $\mathcal{W}$ l'ensemble de suites défini par :

$$\mathcal{W} = \{(\alpha(m_1,\cdots,m_r)) \; ; \; \sum_{m_i \geq 0} \alpha(m_1,\cdots,m_r) X_1^{m_1} \cdots X_r^{m_r} \in \mathcal{V}\} \; ,$$

et de se convaincre que $\mathcal{W}$ vérifie les conditions énoncées dans la propriété b : $\mathcal{W}$ contient la suite a car $\mathcal{V}$ contient la série F, $\mathcal{W}$ est de dimension finie sur $\overline{K}$ comme $\mathcal{V}$, et $\mathcal{W}$ est stable par les applications $b(m_1,\cdots,m_r) \to b^{1/q}(qm_1 + j_1,\cdots,qm_r + j_r)$ car $\mathcal{V}$ est stable par les $E_{j_1,\cdots,j_r}$.

- Montrons que b implique a :

Soit $\mathcal{V}_1$ l'espace vectoriel engendré sur $\overline{K}(X_1,\cdots,X_r)$ par les séries $\sum u(m_1,\cdots,m_r) X_1^{m_1} \cdots X_r^{m_r}$ où les u décrivent $\mathcal{W}$. Il est clair que $\mathcal{V}_1$ est de dimension finie sur $\overline{K}(X_1,\cdots,X_r)$ (toute $\overline{K}$-base de $\mathcal{W}$ est un $\overline{K}(X_1,\cdots,X_r)$-système générateur de $\mathcal{V}_1$). Soit alors $\mathcal{V}_2$ l'espace vectoriel engendré sur $\overline{K}(X_1,\cdots,X_r)$ par les g^q, où g décrit $\mathcal{V}_1$.
On a $\mathcal{V}_1 \subset \mathcal{V}_2$; en effet, si h est dans $\mathcal{V}_1$, alors

$$h = \sum \alpha_k(X_1,\cdots,X_r) h_k(X_1,\cdots,X_r),$$

où les α_k sont dans $\overline{K}(X_1,\cdots,X_r)$ et où

$$h_k(X_1,\cdots,X_r) = \sum u^{(k)}(m_1,\cdots,m_r) X_1^{m_1} \cdots X_r^{m_r},$$

avec des $u^{(k)}$ dans $\mathcal{W}$. On écrit alors :

$$h_k(X_1,\cdots,X_r)$$

$$=\sum u^{(k)}(m_1,\cdots,m_r)\prod_{1\le i\le r}X_i^{m_i}$$

$$=\sum_{0\le j_\ell\le q-1}\prod_{1\le i\le r}X_i^{j_i}\sum_{n_1,\cdots,n_r}u^{(k)}(qn_1+j_1,\cdots,qn_r+j_r)\prod_{1\le i\le r}X_i^{qn_i}$$

$$=\sum_{0\le j_\ell\le q-1}\prod_{1\le i\le r}X_i^{j_i}\Big(\sum_{n_1,\cdots,n_r}(u^{(k)}(qn_1+j_1,\cdots,qn_r+j_r))^{1/q}\prod X_i^{n_i}\Big)^q.$$

Les hypothèses faites sur $\mathcal{W}$ montrent que h_k est dans $\mathcal{V}_2$, donc que h est dans $\mathcal{V}_2$, autrement dit $\mathcal{V}_1\subset\mathcal{V}_2$. Mais par ailleurs on remarque qu'une $\overline{K}(X_1,\cdots,X_r)$-base de $\mathcal{V}_1$ engendre $\mathcal{V}_2$, donc

$$dim_{\overline{K}(X_1,\cdots,X_r)}\mathcal{V}_2\le\dim_{\overline{K}(X_1,\cdots,X_r)}\mathcal{V}_1<+\infty.$$

Bref on a $\mathcal{V}_1=\mathcal{V}_2$, autrement dit si h est dans $\mathcal{V}_1, h^q$ aussi. Mais alors si h est dans $\mathcal{V}_1$, les séries $h, h^q, h^{q^2},\cdots$ sont toutes dans $\mathcal{V}_1$, qui est de dimension finie sur $\overline{K}(X_1,\cdots,X_r)$; par conséquent il existe des polynômes non tous nuls α_k dans $\overline{K}[X_1,\cdots,X_r]$ tels que

$$\sum\alpha_k(X_1,\cdots,X_r)h^{q^k}(X_1,\cdots,X_r)=0,$$

c'est-à-dire h est algébrique sur $\overline{K}(X_1,\cdots,X_r)$, et donc sur $K(X_1,\cdots,X_r)$, car h est à coefficients dans K (Proposition 2).

- Montrons que b implique c :

On peut supposer que la suite a n'est pas nulle, soit alors

$$u_1=a,u_2,\cdots,u_c$$

une $\overline{K}$-base de $\mathcal{W}$.

Soit $U=\begin{pmatrix}u_1\\ \vdots\\ u_c\end{pmatrix}$ la suite à valeurs dans $\overline{K}^c$ de composantes les suites u_i. Pour $1\le k\le c$ et $0\le j_1,\cdots,j_r\le q-1$, la suite

$$u_k^{1/q}(qn_1+j_1,\cdots,qn_r+j_r)$$

est dans $\mathcal{W}$, donc c'est une $\overline{K}$-combinaison linéaire des $u_\ell(n_1, \cdots, n_r)$. En d'autres termes, pour chaque r-uple $(j_1, \cdots, j_r)$ d'éléments de $[0, q-1]^r$, il existe une matrice carrée à c lignes et c colonnes, soit $A_{j_1,\cdots,j_r}$, telle que :

$$U^{1/q}(qn_1 + j_1, \cdots, qn_r + j_r) = A_{j_1,\cdots,j_r} U(n_1, \cdots, n_r),$$

(l'élévation d'un vecteur à la puissance $1/q$ ayant lieu composante à composante dans la base canonique de $\overline{K}^c$). De plus, si φ est la première projection de $\overline{K}^c$ sur $\overline{K}$, on a :

$$\varphi(U) = u_1 = a.$$

- Montrons enfin que c implique b :

Notons $\mathfrak{M}_c(\overline{K})$ l'ensemble des matrices carrées à c lignes et c colonnes à coefficients dans $\overline{K}$, et soit

$$\mathcal{W} = \{\varphi(AU) \ ; \ A \in \mathfrak{M}_c(\overline{K})\},$$

où φ représente toujours la première projection de $\overline{K}^c$ sur $\overline{K}$. L'espace $\{AU; A \in \mathfrak{M}_c(\overline{K})\}$ est de dimension finie sur $\overline{K}$ comme $\mathfrak{M}_c(\overline{K})$, il en est donc de même de $\mathcal{W}$. La suite a est dans $\mathcal{W}$, car $a = \varphi(U) = \varphi(I.U)$. Il reste à prouver que $\mathcal{W}$ est stable par les applications

$$b(m_1, \cdots, m_r) \to b^{1/q}(qm_1 + j_1, \cdots, qm_r + j_r), \ 0 \leq j_1, \cdots, j_r \leq q-1.$$

Pour cela, il suffit de prouver que l'espace $\{AU; A \in \mathfrak{M}_c(\overline{K})\}$ est stable par les applications

$$V(m_1, \cdots, m_r) \to V^{1/q}(qm_1 + j_1, \cdots, qm_r + j_r).$$

Mais si l' on note $A^{1/q}$ la matrice obtenue à partir de A en élevant chaque élément à la puissance $1/q$, on a :

$$\begin{aligned}(AU(qm_1 + j_1, \cdots, qm_r + j_r))^{1/q} &= A^{1/q} U^{1/q}(qm_1 + j_1, \cdots, qm_r + j_r) \\ &= (A^{1/q} A_{j_1,\cdots,j_r}) U(m_1, \cdots, m_r)\end{aligned}$$

ce qui achève la démonstration du théorème.

4 - Applications - Compléments - Généralisation de la notion de substitution.

1) Produit de Hadamard et diagonales de séries algébriques :

THÉORÈME. *Soient deux séries formelles à coefficients dans un corps de caractéristique strictement positive, et à un nombre fini de variables. Si ces deux séries sont algébriques, alors il en est de même de leur produit de Hadamard.*

THÉORÈME. *Soit une série formelle à coefficients dans un corps de caractéristique strictement positive, et à un nombre fini de variables. Si elle est algébrique, toutes ses diagonales sont aussi algébriques.*

D'après la proposition 1, il suffit de prouver le premier de ces théorèmes. Pour cela on utilise le théorème fondamental du paragraphe précédent, et plus précisément la condition b : si $\mathcal{W}$ et $\mathcal{W}'$ sont deux $\overline{K}$-espaces associés par la condition b aux séries formelles considérées, alors $\mathcal{W}\mathcal{W}' = \{uv; u \in \mathcal{W}, v \in \mathcal{W}'\}$ est un $\overline{K}$-espace vectoriel de dimension finie sur $\overline{K}$, qui contient la suite produit des suites des coefficients des deux séries (autrement dit la suite des coefficients du produit de Hadamard des deux séries), et qui est stable par les applications décrites dans le b, d'où l'algébricité du produit de Hadamard des deux séries considérées.

Remarques :

- Le premier théorème a été donné par Furstenberg [13] dans le cas d'un corps fini et de séries à une seule variable, puis par Fliess [10] pour une variable et un corps parfait de caractéristique strictement positive (Fliess ayant remarqué que la démonstration de Furstenberg était aussi valable pour un corps dont l'application de Frobenius est surjective, autrement dit pour un corps parfait). Pour le cas d'un corps fini, et pour le rapport avec les automates finis, on consultera l'article de Christol, Kamae, Mendès France et Rauzy [7] pour des séries à une variable, et celui de Salon [23] pour des séries à plusieurs variables. Pour un corps quelconque de caractéristique strictement positive, les deux théorèmes ci-dessus ont été donnés par Deligne [8], puis par Denef et Lipshitz [9]. La démonstration que nous donnons est très proche de celle de Sharif et Woodcock [26], et de celle de Harase [14] qui s'intéresse aussi à d'autres produits de séries formelles comme le produit de Hurwitz et celui de Lamperti (à ce sujet voir aussi l'article de Fliess [11]).

- Chacun de ces deux théorèmes est faux en général pour un corps de caractéristique nulle. Considérons en effet comme Furstenberg dans [13] la série $\sum_{n\geq 0} \binom{2n}{n} X^n = (1-4X)^{-1/2}$, qui est à coefficient dans $\mathbb{Q}$ (et donc dans le sous-corps premier de tout corps K de caractéristique nulle). Son carré de Hadamard est égal à $\sum_{n\geq 0} \binom{2n}{n}^2 X^n$. Si cette dernière série

était algébrique sur $K(X)$, elle le serait aussi sur $\mathbf{Q}(X)$, et la série entière définie par $\sum_{n\geq 0} \binom{2n}{n}^2 x^n$, pour $|x| < 1$, serait une fonction algébrique, ce qui n'est pas car $\sum_{n\geq 0} \binom{2n}{n}^2 x^n = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{d\theta}{(1-16x\cos^2\theta)^{1/2}}$ prend des valeurs transcendantes pour x algébrique (voir [16],[24] ou [28]).

Cette remarque montre que la proposition 1 peut être complétée en ajoutant que chacune des propriétés énoncées dans cette proposition équivaut au fait que le corps K est de caractéristique strictement positive.

2) Compléments :

On peut se demander, pour un corps commutatif quelconque, si le produit de Hadamard de deux séries rationnelles est algébrique (ou même rationnel), ou si la diagonale d'une série formelle rationnelle est algébrique. Voici des réponses à ces questions :

a) le produit de Hadamard de deux séries formelles rationnelles à une seule variable est rationnel (le résultat est dû à Borel cité par Jungen dans [16] pour la caractéristique nulle, il est immédiat dans le cas d'un corps fini, et il est dû à Sharif et Woodcock [27] pour un corps de caractéristique strictement positive).

b) le produit de Hadamard de deux séries formelles rationnelles à deux variables, et à coefficients dans un corps de caractéristique nulle, est algébrique (Sharif et Woodcock [27]).

c) la diagonale d'une série formelle rationnelle à deux variables, à coefficients dans $\mathbf{C}$*, est une série formelle algébrique (Furstenberg [13]).*

Remarques :

- l'assertion *a* est fausse pour des séries à plus d'une variable ; en caractéristique différente de 2, Sharif et Woodcock donnent dans [27] le contre-exemple suivant :

$$\sum_{m,n\geq 0} \binom{m+n}{m} X^m Y^n = \frac{1}{1-X-Y}$$

et le carré de Hadamard de cette série est égal à

$$\sum_{m,n\geq 0} \binom{m+n}{m}^2 X^m Y^n = [(1-X-Y)^2 - 4XY]^{-1/2}.$$

- l'assertion *b* est fausse si l'on suppose l'une des séries algébrique, et l'autre rationnelle, Sharif et Woodcock proposent dans [27] le contre- exemple suivant : le produit de Hadamard de la série

$$\sum_{m,n\geq 0} \binom{m+n}{m}^2 X^m Y^n = [(1-X-Y)^2 - 4XY]^{-1/2},$$

et de la série $\sum_{n\geq 0} (XY)^n = \frac{1}{1-XY}$, est égal à la série $\sum_{n\geq 0} \binom{2n}{n}^2 (XY)^n$ dont on a évoqué plus haut la transcendance.

- l'assertion *b* est fausse pour plus de deux variables : Sharif et Woodcock considèrent dans [27] les deux séries

$$\sum_{a,b,c\geq 0} \binom{a+b+c}{a,b,c} X^a Y^b Z^c = \frac{1}{1-X-Y-Z} \text{ et } \sum_{n\geq 0} (XYZ)^n = \frac{1}{1-XYZ},$$

dont le produit de Hadamard est la série formelle $\sum_{n\geq 0} \binom{3n}{n,n,n} X^n$ qui est transcendante (voir par exemple [28]).

- pour le quotient de Hadamard en caractéristique nulle, on pourra consulter l'article de van der Poorten [20], mais aussi la rédaction soigneuse de Rumely [22], sans oublier l'article de Pourchet [21].

- l'assertion *c* est fausse pour plus de deux variables, comme le montre Furstenberg dans [13] en indiquant l'idée de la construction d'un contre-exemple dans $\mathbf{C}$.

- remarquons enfin que Furstenberg, après avoir prouvé dans [13] une partie du second théorème du paragraphe précédent :

la diagonale d'une série rationnelle à coefficients dans un corps de caractéristique strictement positive est une série algébrique,

en donne une sorte de réciproque :

une série formelle algébrique, à une variable, à coefficients dans $\mathbf{C}$, *ou dans un corps parfait de caractéristique strictement positive, est la diagonale d'une série rationnelle.*

(Comme nous l'avons déjà dit Fliess a remarqué que la démonstration de Furstenberg est valable non seulement pour un corps fini comme indiqué, mais aussi pour un corps parfait). Sur le sujet passionnant des diagonales de séries formelles rationnelles sur un corps quelconque, on pourra se reporter avec profit aux travaux de Christol (voir par exemple [6]).

3) Généralisation de la notion de substitution :

La condition c du théorème fondamental ci-dessus montre comment définir la généralisation d'une p-substitution (voir [7] pour le cas unidimensionnel et [23] pour le cas multidimensionnel, lorsque l'alphabet est fini) :

DÉFINITION. *Soit $a(n_1,\cdots,n_r)$ une suite à valeurs dans un corps K de caractéristique p. Soit $\overline{K}$ une extension parfaite de K (par exemple la clôture algébrique ou la clôture radicielle de K). Soit s un entier supérieur ou égal à 1 et soit $q = p^s$. La suite a est dite engendrée par q-substitution s'il existe un entier $c \geq 1$, une famille de matrices carrées à c lignes et c colonnes $\{A_{j_1,\cdots,j_r}\ ;\ 0 \leq j_1,\cdots,j_r \leq q-1\}$ et une suite $(U(n_1,\cdots,n_r))$ à valeurs dans $\overline{K}^c$ tels que :*

i) $\varphi(U) = a$, où φ est la première projection canonique de $\overline{K}^c$ sur $\overline{K}$,

ii) $\forall(j_1,\cdots,j_r) \in [0,q-1]^r, \forall(n_1,\cdots,n_r) \in \mathbb{N}^r$, on a :

$$U^{1/q}(qn_1 + j_1,\cdots,qn_r + j_r) = A_{j_1,\cdots,j_r}U(n_1,\cdots,n_r).$$

Remarques :

- Le théorème fondamental implique qu'une suite est engendrée par p^s-substitution si et seulement si elle est engendrée par p^t−substitution (t entier quelconque non nul).

- Le théorème fondamental peut se reformuler de la façon suivante : une série formelle à coefficients dans un corps de caractéristique p est algébrique si et seulement si la suite de ses coefficients est engendrée par une p-substitution.

- Si l'on compare notre définition à la définition traditionnelle dans le cas où le corps de base est fini (voir [7] et [23] par exemple), on voit que les applications $A_{j_1,\cdots,j_r}$ sont supposées ici *linéaires* (mais on peut ajouter cette condition dans le cas habituel, voir [17] par exemple). De plus, dans le cas d'un corps fini, il n'y a pas l'exposant $1/q$ (voir *ii)* dans la définition ci-dessus), mais si on applique le théorème fondamental en choisissant t tel que p^t soit justement le cardinal du corps, l'élévation à la puissance $1/q$ est l'identité.

- Remarquons enfin que l'on peut construire U par itération de ii), connaissant les matrices $A_{j_1,\cdots,j_r}$ et la valeur initiale $U(0,\cdots,0)$; on passe d'un mot multidimensionnel de taille $(q^n)^r$ à un mot de taille $(q^{n+1})^r$ en appliquant d'abord les $A_{j_1,\cdots,j_r}$, puis en élevant à la puissance q, par exemple

pour $r = 1, q = 2, U(0) = a$, $A_0 = f$, $A_1 = g$, on obtient successivement :

$$a \to (f(a))^2(g(a))^2 \to [f((f(a))^2)]^2[g((f(a))^2)]^2[f((g(a))^2)]^2 [g((g(a))^2)]^2 \to \ldots$$

5 - Retour sur l'indépendance algébrique de certaines séries formelles.

Nous nous proposons dans ce paragraphe de revenir sur un résultat démontré dans [2] (et généralisant [19]). Commençons par rappeler que si λ est un entier p-adique, et K un corps de caractéristique p, on peut définir l'élévation de $(1+X)$ à la puissance λ par :

$$(1+X)^\lambda = \sum_{n=0}^{+\infty} \binom{\lambda}{n} X^n \in K((X)),$$

où $\binom{\lambda}{n} = \dfrac{\lambda(\lambda-1)\cdots(\lambda-n+1)}{n!}$, qui appartient a priori à $\mathbb{Z}_p$, est naturellement à prendre modulo p.

Remarques :

- Cette définition du coefficient binomial $\binom{\lambda}{n}$ coïncide avec celle donnée dans [2] ou [19] dans le cas où λ est un entier naturel (c'est une propriété bien connue), donc dans le cas général (par continuité par exemple).

- Donnons ici un lemme qui sera utilisé plus loin :

LEMME. *Soient λ et λ' deux entiers p-adiques. Si pour tout entier naturel n on a $\binom{\lambda}{n} \equiv \binom{\lambda'}{n}$ modulo p, alors $\lambda = \lambda'$.*

En effet on a $(1+X)^\lambda = (1+X)^{\lambda'}$; si $\lambda - \lambda' = p^k\beta$ avec $\beta \not\equiv 0\ (mod.p)$, on en déduit $(1+X^{p^k})^\beta = 1$, c'est-à-dire $\beta \equiv 0\ (mod.p)$, ce qui n'est pas.

- L'élévation à la puissance λ a toutes les propriétés attendues, et elle coïncide avec l'opération usuelle lorsque λ est un entier naturel.

Plus généralement, si F est une série formelle dans $K[[X_1, \cdots, X_r]]$, non constante et sans terme constant,

$$\text{(c'est-à-dire } F = \sum_{n_i \geq 0} a(n_1, \cdots, n_r) X_1^{n_1} \cdots X_r^{n_r}, \text{ avec } a(0, \cdots, 0) = 0),$$

la même définition permet d'écrire :

$$(1+F)^\lambda = \sum_{n=0}^{+\infty} \binom{\lambda}{n} F^n$$

ceci définissant un élément de $K[[X_1, \cdots, X_r]]$.

Mendès France, van der Poorten et l'auteur ont prouvé dans [2] le résultat suivant :

Soit $F(X)$ une série formelle à une variable, à coefficients dans un corps fini K, non constante, sans terme constant et algébrique sur $K(X)$. Soient $\lambda^{(1)}, \cdots, \lambda^{(s)}$ des entiers p-adiques (où p est la caractéristique du corps K). Les séries formelles $(1+F)^{\lambda^{(1)}}, \cdots, (1+F)^{\lambda^{(s)}}$ sont algébriquement indépendantes sur $K(X)$ si et seulement si $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ sont $\mathbb{Z}$-linéairement indépendants.

La preuve que nous donnons dans [2] utilise les automates finis. Henniart nous a indiqué [15] qu'on doit pouvoir trouver une démonstration sans automates, un peu comme le théorème d'Artin sur l'indépendance des caractères, Bezivin nous a donné [3] une démonstration sans automate qui utilise des dérivations de séries formelles. Nous nous proposons ici de donner une démonstration un peu intermédiaire dans le cas où $F(X) = X$, puis de montrer comment le passage de X à une $F(X)$ algébrique qui nous a été suggéré par Fresnel [12] (et différent de celui proposé dans [19] et [2]) permet de donner une démonstration générale dans le cas d'une série formelle à plusieurs variables, à coefficients dans un corps de caractéristique strictement positive. Dans un premier temps nous avions cherché à démontrer un tel résultat général soit en utilisant le théorème fondamental ci-dessus et la généralisation de la notion de substitution, soit en utilisant une proposition du type de la propriété 2 donnée au début de cet article et permettant de passer d'un corps à un surcorps pour l'indépendance algébrique de séries formelles. Nous préférons l'approche ci-dessous qui nous paraît à la fois plus simple et plus algébrique :

THÉORÈME. *Soient K un corps de caractéristique p et $F(X_1, \cdots, X_r)$ une série formelle à r variables non constante et sans terme constant, algébrique sur $K(X_1, \cdots, X_r)$, et soient $\lambda^{(1)}, \cdots, \lambda^{(s)}$ des entiers p-adiques. Les séries formelles $(1+F)^{\lambda^{(1)}}, \cdots, (1+F)^{\lambda^{(s)}}$ sont algébriquement indépendantes sur $K(X_1, \cdots, X_r)$ si et seulement si $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ sont linéairement indépendants sur $\mathbb{Z}$.*

La démonstration sera faite en deux étapes : prouver le résultat pour $r = 1$ et $F(X) = X$, puis passer de X à une série F algébrique. Aussi bien pour X que pour un F algébrique l'une des implications est immédiate :

si $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ sont linéairement liés sur $\mathbb{Z}$, il est clair que les séries $(1+X)^{\lambda^{(1)}}, \cdots, (1+X)^{\lambda^{(s)}}$ (respectivement $(1+F)^{\lambda^{(1)}}, \cdots, (1+F)^{\lambda^{(s)}}$)

sont algébriquement liés sur $K(X)$ (respectivement sur $K(X_1, \cdots, X_r)$).

Soient donc $\lambda^{(1)}, \cdots, \lambda^{(s)}$ des entiers p-adiques tels que $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ soient linéairement indépendants sur $\mathbb{Z}$, et supposons qu'il existe une relation de dépendance algébrique entre

$$(1+X)^{\lambda^{(1)}}, \cdots, (1+X)^{\lambda^{(s)}}$$

sur $K(X)$. Il existe donc des polynômes $a_1(X), \cdots, a_s(X)$ dans $K[X]$ et des entiers p-adiques $\mu^{(1)}, \cdots, \mu^{(s)}$ qui sont combinaisons linéaires à coefficients entiers des $\lambda^{(j)}$ tels que

$$\sum a_j(X)(1+X)^{\mu^{(j)}} = 0.$$

En développant les $a_j(X)$ dans la base $\{(1+X)^k \ ; \ k \in \mathbb{N}\}$, on obtient une relation :

$$(*) \qquad \sum_{j=1}^{d} c_j(1+X)^{\theta^{(j)}} = 0,$$

où les c_j sont dans K, les $\theta^{(j)}$ combinaisons linéaires à coefficients entiers des $\mu^{(j)}$ donc des $\lambda^{(j)}$ et tous distincts. Comme $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ sont linéairement indépendants sur $\mathbb{Z}$, et que la relation initiale de dépendance algébrique est non triviale, la relation $(*)$ est aussi non triviale. Aux notations près on peut supposer qu'elle est de longueur minimale (ce qui implique la non-nullité de chaque c_j et le fait que d est au moins égal à 2). Soit Y une autre variable (autrement dit X et Y sont algébriquement indépendants sur K), alors $(*)$ implique

$$\sum_{j=1}^{d} c_j(1+(X+Y+XY))^{\theta^{(j)}} = 0$$

autrement dit

$$0 = \sum_{j=1}^{d} c_j((1+X)(1+Y))^{\theta^{(j)}} = \sum_{j=1}^{d} c_j(1+X)^{\theta^{(j)}}(1+Y)^{\theta^{(j)}}$$

d'où, en soustrayant la relation $(*)$ préalablement multipliée par $(1+Y)^{\theta^{(1)}}$:

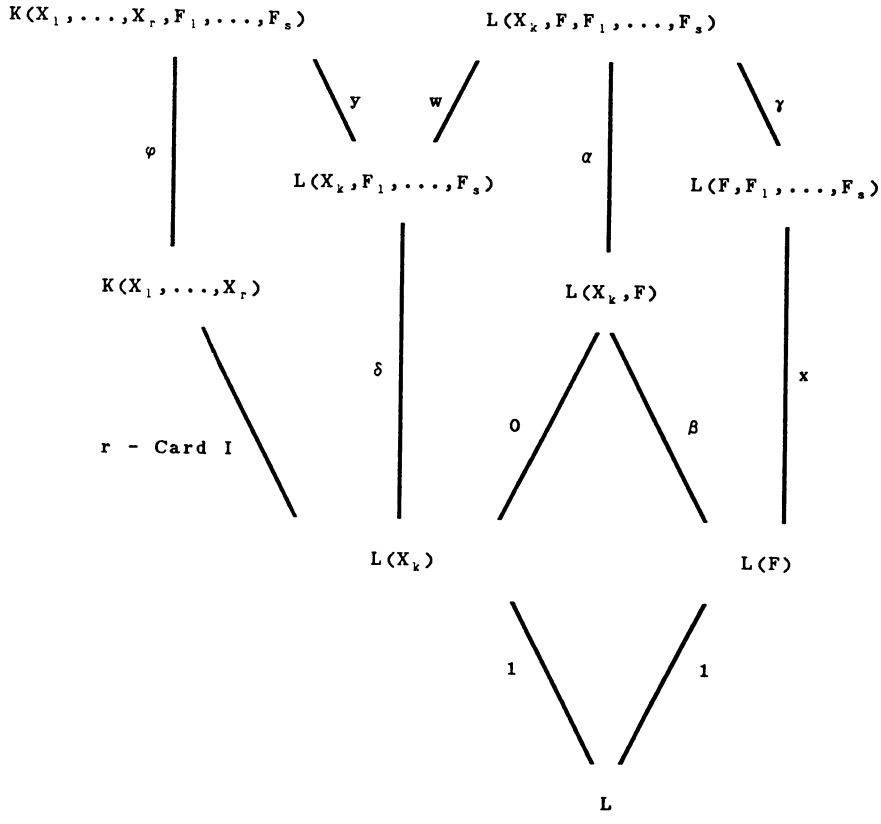
$$\begin{aligned} 0 &= \sum_{j=2}^{d} c_j(1+X)^{\theta^{(j)}}((1+Y)^{\theta^{(j)}} - (1+Y)^{\theta^{(1)}}) \\ &= \sum_{j=2}^{d} c_j(1+X)^{\theta^{(j)}} \sum_{n=0}^{+\infty} \left(\binom{\theta^{(j)}}{n} - \binom{\theta^{(1)}}{n} \right) Y^n. \end{aligned}$$

Et donc, quel que soit n positif

$$(**) \qquad \sum_{j=2}^{d} c_j \left(\binom{\theta^{(j)}}{n} - \binom{\theta^{(1)}}{n} \right) (1+X)^{\theta^{(j)}} = 0.$$

Comme les $\theta^{(j)}$ sont tous distincts, on a en particulier $\theta^{(2)} \neq \theta^{(1)}$, donc il existe un entier n pour lequel $\binom{\theta^{(2)}}{n} \neq \binom{\theta^{(1)}}{n}$, (d'après le lemme donné plus haut en remarque). Bref la relation $(**)$ est plus courte que la relation $(*)$ et non triviale, ce qui fournit la contradiction recherchée. Ainsi l'indépendance linéaire sur $\mathbb{Z}$ de $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ implique l'indépendance algébrique sur $K(X)$ de $(1+X)^{\lambda^{(1)}}, \cdots, (1+X)^{\lambda^{(s)}}$. Maintenant si F est une série formelle dans $K[[X_1, \cdots, X_s]]$, non constante et sans terme constant, F est transcendante sur K (on se convainc aisément que toute expression polynomiale à coefficients dans K, $\sum_{0}^{t} e_j F^j$ avec $e_0 \neq 0$, est une série formelle non nulle en regardant le terme de F de plus bas degré total) donc si $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$ sont $\mathbb{Z}$-linéairement indépendants, alors les séries $(1+F)^{\lambda^{(1)}}, \cdots, (1+F)^{\lambda^{(s)}}$ sont algébriquement indépendantes sur $K(F)$.

Supposons de surcroît que F est algébrique sur $K(X_1, \cdots, X_r)$ et soit I le sous-ensemble de $\{1, \cdots, r\}$ des indices des variables X_i qui figurent effectivement dans F : alors F est algébrique sur $K((X_i)_{i \in I})$. Comme F est non constante, d'après la remarque précédente I est de cardinal supérieur ou égal à 1, soit $\hat{I}$ un sous-ensemble de I obtenu en enlevant un élément k à I. Par construction de I, F est transcendante sur $K((X_i)_{i \in \hat{I}})$ car elle est non constante sur ce corps. Posons pour simplifier les notations $K((X_i)_{i \in \hat{I}}) = L$, de sorte que $K((X_i)_{i \in I}) = L(X_k)$, et $F_j = (1+F)^{\lambda^{(j)}}$ Examinons alors les degrés de transcendance des extensions suivantes :



On a entre ces degrés de transcendance les relations :

* $x = s$ (on a vu que $F_1, \cdots, F_s$ sont algébriquement indépendantes sur $L(F)$ dès que F est transcendante sur L),

* $\beta + 1 = 0 + 1$, d' où $\beta = 0$,

* $\gamma \leq \beta$ d'où $\gamma = 0$,

* $\alpha + \beta = \gamma + x$, d'où $\alpha = x = s$,

* $w = 0$, (car F est algébrique sur $L(X_k)$, donc sur $L(X_k, F_1, \cdots, F_s)$),

* $w + \delta = \alpha + 0$, d'où $\delta = \alpha = s$,

* en reprenant un argument précédent, si l'on note $X'_1, \cdots, X'_t$ les X_j pour j n'appartenant pas à I, on voit que X'_1 est une série formelle non constante sur $M = L(X_k, F_1, \cdots, F_s)$, ($X'_1$ ne figure ni dans F, ni dans les F_j), donc est transcendant sur M, puis que X'_2 est transcendant sur $M(X'_1), \cdots$, bref que l'on a $y = t = r - Card\ I$,

* enfin $\delta + y = \varphi + r - Card\ I$, c'est-à-dire $\varphi = \delta = s$, ce qui signifie exactement que $F_1, \cdots, F_s$ sont algébriquement indépendantes sur $K(X_1, \cdots, X_r)$.

Remarque :

Comme nous l'a fait remarquer J. Fresnel [12], la considération des homomorphismes $(1 + SF(S)) \to (1 + SF(S))^\lambda$ permet d'appliquer directement le lemme d'Artin dans la démonstration qui précède ; de plus cette démonstration permet d'établir en fait le résultat suivant :

Soient K et F comme dans le théorème ci-dessus. Soient a et b les degrés de transcendance respectifs sur le corps $K(X_1, \cdots, X_r)$ des extensions $K(X_1, \cdots, X_r, F)$ et $K(X_1, \cdots, X_r, F, (1+X)^{\lambda^{(1)}}, \cdots, (1+X)^{\lambda^{(s)}})$. Soit enfin σ la dimension sur $\mathbb{Z}$ du $\mathbb{Z}$- module engendré par $1, \lambda^{(1)}, \cdots, \lambda^{(s)}$, alors on a : $b = a + \sigma - 1$.

Je remercie J-P. Bezivin, G. Christol, J. Fresnel, G. Henniart et D. Polton pour d'intéressantes conversations pendant la préparation de cet article.

Bibliographie

[1] J-P. ALLOUCHE, *Automates finis en théorie des Nombres*, Expo. Math. . **5** (1987), 239–266.

[2] J-P. ALLOUCHE, M. MENDÈS FRANCE, et A.J. van der POORTEN, *Indépendance algébrique de certaines séries formelles*, Bull. Soc. Math. France **116** (1988), 449-454.

[3] J-P. BEZIVIN. Communication privée.

[4] G. CHRISTOL, *Ensembles presque périodiques k-reconnaissables*, Theoretical Computer Science, **9** (1979), 141–145.

[5] G. CHRISTOL, *Fonctions et éléments algébriques*, Pac. J. Math. **125** 1 (1986), 1–37.

[6] G. CHRISTOL, *Diagonales de fractions rationnelles*, Sém. de Théorie des Nombres de Paris (1986-1987), 65–90. Progress in Math., Birkhäuser.

[7] G. CHRISTOL, T. KAMAE, M. MENDÈS FRANCE et G. RAUZY, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France, **108** (1980), 401–419.

[8] P. DELIGNE, *Intégration sur un cycle évanescent*, Invent. Math. **76** (1983), 129–143.

[9] J. DENEF et L. LIPSHITZ, *Algebraic power series and diagonals*, J. Number Theory **26** (1987), 46-67.

[10] M. FLIESS, *Sur certaines familles de séries formelles*, Thèse, Paris VII (1972).

[11] M. FLIESS, *Sur divers produits de séries formelles*, Bull. Soc. Math. France **102** (1974), 181–191.

[12] J. FRESNEL. Communication privée.

[13] H. FURSTENBERG, *Algebraic functions over finite fields*, J. Algebra **7** (1967), 271–277.

[14] T. HARASE, *Algebraic elements in formal power series rings*, Israel Journal of Math. **63** **3** (1988), 281–288.

[15] G. HENNIART. Communication privée.

[16] R. JUNGEN, *Sur les séries de Taylor n'ayant que des singularités algébrico-logarithmiques sur leur cercle de convergence*, Comment. Math. Helv. **3** (1931), 266–306.

[17] P. LIARDET, *Automata and generalized Rudin-Shapiro sequences*, Salzburg Universität (1986).

[18] L. LIPSHITZ et A. J. van der POORTEN, *Rational functions, diagonals, automata and arithmetic*, in R.A. Mollin (ed.), First conference of the Canadian Number Theory Association, Banff/Can. (1988). (de Gruyter 1989).

[19] M. MENDÈS FRANCE et A.J. van der POORTEN, *Automata and the arithmetic of formal power series*, Acta Arith. **46** (1986), 211–214.

[20] A.J. van der POORTEN, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C.R. Acad. Sci. Paris t. 306, Série I (1988), 97–102.

[21] Y. POURCHET, *Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles*, C.R. Acad. Sci. Paris t. 288, série A (1979), 1055–1057.

[22] R. RUMELY, *Note on van der Poorten's proof of the Hadamard quotient theorem (Part I and II)*,, Sém. de Théorie des Nombres de Paris (1986-1987), 349–409. Progress in Math., Birkhaüser.

[23] O. SALON, *Suites automatiques à multi-indices*, Sém. de Théorie des Nombres de Bordeaux, exposé n° 4 (1986–1987), 4.01–4.36. (avec un appendice de J. SHAL-

LIT).

[24] T. SCHNEIDER, *Einführung in die Tranzendenten Zahlen*, Springer, Berlin (1957.).

[25] M.P. SCHÜTZENBERGER, *On a definition of a family of automata*, Information and Control **4** (1961), 245–270.

[26] H. SHARIF et C.F. WOODCOCK, *Algebraic functions over a field of positive characteristic and Hadamard products*, J. Lond. Math. Soc. (2) **37** (1988), 395–403.

[27] H. SHARIF et C.F. WOODCOCK, *Hadamard products of rational formal power series*. Preprint.

[28] H. SHARIF et C.F. WOODCOCK, *On the transcendence of certain series*, J. Algebra **121** (1989), 364–369.

[29] L.I. WADE, *Two types of function field transcendental numbers*, Duke Math. J. **11** (1944), 755-758..

Mots clefs : formal power series, Hadamard products, diagonals of algebraic power series, automata.

1980 *Mathematics subject classifications*: 10B40, 12E99.

C.N.R.S., U.R.A. 0226
Université Bordeaux I
U.F.R. de Mathématiques
351, cours de la Libération
33405 Talence FRANCE.