BULLETIN DE LA S. M. F.

J.-P. ALLOUCHE
M. MENDÈS-FRANCE
A.J. VAN DER POORTEN

Indépendance algébrique de certaines séries formelles

Bulletin de la S. M. F., tome 116, n° 4 (1988), p. 449-454
<http://www.numdam.org/item?id=BSMF_1988__116_4_449_0>

Bull. Soc. math. France,
116, 1988, p. 449–454.

INDÉPENDANCE ALGÉBRIQUE DE CERTAINES SÉRIES FORMELLES

PAR

J.-P. ALLOUCHE, M. MENDÈS FRANCE
ET A.J. VAN DER POORTEN (*)

RÉSUMÉ. — Soit $f = 1+\sum_{k=1}^{\infty} f_k X^k$ une série formelle non constante à coefficients dans un corps fini $\mathbb{F}$ de caractéristique p, algébrique sur $\mathbb{F}(X)$. Soient $\lambda_1, \lambda_2, \ldots, \lambda_s$ des entiers p-adiques. On montre que les séries $f^{\lambda_1}, \ldots, f^{\lambda_s}$ sont algébriquement indépendantes sur le corps des fractions rationnelles $\mathbb{F}(X)$ si et seulement si $1, \lambda_1, \ldots, \lambda_s$ sont linéairement indépendants sur $\mathbb{Z}$.

ABSTRACT. — Let $f = 1 + \sum_{k=1}^{\infty} f_k X^k$ be a non-constant formal power series over a finite field $\mathbb{F}$ with characteristic p, algebraic over $\mathbb{F}(X)$. Let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be p-adic integers. We prove that $f^{\lambda_1}, f^{\lambda_2}, \ldots, f^{\lambda_s}$ are algebraically independent over the field of rational functions $\mathbb{F}(X)$ if and only if $1, \lambda_1, \ldots, \lambda_s$ are $\mathbb{Z}$-linearly independent.

1. Un résultat d'indépendance

Soit p un nombre premier et soit $\mathbb{F}$ un corps fini de caractéristique p. Pour tout entier p-adique λ,

$$\lambda = \sum_{i=0}^{\infty} \lambda^{(i)} p^i \qquad 0 \leq \lambda^{(i)} \leq p-1,$$

on définit l'élément $(1+X)^\lambda$ du corps des séries formelles $\mathbb{F}((X))$ par :

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

où

(*) Texte reçu le 5 juin 1987, révisé le 27 octobre 1987.

J.-P. ALLOUCHE et M. MENDÈS FRANCE, Université Bordeaux I, UER de Mathématiques et Informatique, 351 Cours de la Libération, 33405 Talence Cedex, France.

A.-J. VAN DER POORTEN, School of Mathematics, Physics, Computing and Electronics, Macquarie University, NSW 2109, Australie.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/1988/449/$ 5.00

$$\binom{\lambda}{n} = \prod_{i=0}^{\infty} \binom{\lambda^{(i)}}{n^{(i)}}$$

et où

$$n = \sum_{i=0}^{\infty} n^{(i)} p^i \qquad 0 \leq n^{(i)} \leq p-1,$$

(les $n^{(i)}$ sont nuls à partir d'un certain rang).

On rappelle que $(1+X)^{\lambda}$ est transcendant sur le corps des fractions rationnelles $\mathbb{F}(X)$, à moins que l'exposant λ soit élément de $\mathbb{Q} \cap \mathbb{Z}_p$, (voir [3]).

Dans cette note nous étendons ce résultat :

THÉORÈME 1. — *Soient $\lambda_1, \lambda_2, \ldots, \lambda_s$ des entiers p-adiques. Les séries formelles $(1+X)^{\lambda_j}$, $j = 1, 2, \ldots, s$, sont algébriquement indépendantes sur le corps des fractions rationnelles $\mathbb{F}(X)$ si et seulement si $1, \lambda_1, \ldots, \lambda_s$ sont linéairement indépendants sur $\mathbb{Z}$.*

Notre preuve s'appuie essentiellement sur des propriétés simples des automates finis (voir paragraphe 3).

2. Réduction et extension

Supposons que $1, \lambda_1, \ldots, \lambda_s$ soient linéairement indépendants sur $\mathbb{Z}$. Le théorème affirme alors qu'il n'existe aucun polynôme non trivial en les variables X, $(1+X)^{\lambda_1}, \ldots, (1+X)^{\lambda_s}$ qui s'annule identiquement. En d'autres termes, aucune somme finie de la forme :

$$b_0(X) + \sum_{i=1}^{t} b_i(X)(1+X)^{\mu_i}$$

(où les b_i sont dans $\mathbb{F}[X]$ et ne sont pas tous nuls), ne peut s'annuler identiquement. Comme les polynômes $b_i(X)$ peuvent s'exprimer linéairement en fonctions de monômes $(1+X)^d$, l'énoncé du théorème se déduit finalement de l'énoncé suivant (où les μ_i sont des combinaisons linéaires sur $\mathbb{Z}$ des λ_i).

THÉORÈME 1'. — *Si $\mu_1, \mu_2, \ldots, \mu_r$ sont des entiers p-adiques deux à deux distincts et si $a_1, \ldots, a_r$ sont des éléments non nuls du corps $\mathbb{F}$, alors la série formelle $\sum_{i=1}^{r} a_i(1+X)^{\mu_i}$ est algébrique sur $\mathbb{F}(X)$ si et seulement si tous les μ_i sont rationnels.*

Nous démontrerons cette assertion au paragraphe 4. Avant d'en présenter la preuve, notons que l'énoncé initial peut être étendu comme suit.

Remarquons d'abord que si $f = f(X) = 1+\sum_{n=1}^{\infty} f_n X^n$ est un élément de $\mathbb{F}((X))$, alors f^λ est bien défini pour tout λ dans $\mathbb{Z}_p$. Le passage de $(1+X)$ à f calqué sur celui proposé dans [3] permet alors d'énoncer le corollaire (équivalent au THÉORÈME 1) :

COROLLAIRE. — *Soit* $f = 1 + \sum_{n=1}^{\infty} f_n X^n$ *une série formelle non constante à coefficients dans* $\mathbb{F}$, *et algébrique sur* $\mathbb{F}(X)$. *Alors* $f^{\lambda_1}, f^{\lambda_2}, \ldots, f^{\lambda_s}$ *sont algébriquement indépendants sur* $\mathbb{F}(X)$ *si et seulement si les entiers p-adiques* $1, \lambda_1, \lambda_2, \ldots, \lambda_s$ *sont linéairement indépendants sur* $\mathbb{Z}$.

3. Un théorème préliminaire

Rappelons qu'une suite $\alpha = (\alpha(n))$, $n = 1, 2, 3, \ldots$, est dite p-multiplicative si :

$$\forall n \geq 0 \quad \forall k \geq 0 \quad \forall r \in [0, p^k - 1] \qquad \alpha(np^k + r) = \alpha(np^k)\alpha(r).$$

Ces suites ont été introduites dans la littérature mathématique en 1967 par A.O. GELFOND [2].

Rappelons aussi qu'une suite $\beta = (\beta(n))$, $n = 1, 2, \ldots$ est dite p-automatique s'il existe un p-automate qui l'engendre, et que les suites p-automatiques vérifient les trois importantes propriétés suivantes (voir [1]) :

PROPRIÉTÉ 1. — *La suite* β *est p-automatique si et seulement si l'ensemble des sous-suites* $n \to \beta(np^k + t)$, *avec* $k \geq 0$ *et* $t \in [0, p^k - 1]$, *est fini.*

PROPRIÉTÉ 2. — *Soit* β *une suite à valeurs dans le corps fini* $\mathbb{F}$ *de caractéristique p. Alors la suite* β *est p-automatique si et seulement si la série formelle* $\sum_{n=0}^{\infty} \beta(n) X^n$ *est algébrique sur* $\mathbb{F}(X)$.

PROPRIÉTÉ 3. — *Si* β *est p-automatique, alors la suite* $(\beta(p^n))$ *est ultimement périodique.*

Nous nous proposons dans ce paragraphe de prouver le théorème suivant :

THÉORÈME 2. — *Soient* $\alpha_1 = (\alpha_1(n))$, $\alpha_2 = (\alpha_2(n)), \ldots, \alpha_s = (\alpha_s(n))$ *des suites p-multiplicatives à valeurs dans le corps fini* $\mathbb{F}$ *de caractéristique p. On suppose que ces suites sont linéairement indépendantes sur* $\mathbb{F}$. *S'il existe des éléments non nuls* $a_1, \ldots, a_s$ *de* $\mathbb{F}$ *tels que la suite* $a_1\alpha_1 + \cdots + a_s\alpha_s$ *soit p-automatique, alors chacune des suites* α_i *est p-automatique.*

Preuve. — Comme les suites α_i sont indépendantes, il existe des entiers $t_1, \ldots, t_s$ tels que le déterminant dét $(\alpha_i(t_j))$ soit différent de 0.

La suite $a_1\alpha_1 + \cdots + a_s\alpha_s$ est p-automatique donc l'ensemble de sous-suites

$$E = \{n \longmapsto \sum_{i=1}^{s} a_i\alpha_i(p^k n + t)\,;\ k \geq 0,\ 0 \leq t \leq p^k - 1\}$$
$$= \{n \longmapsto \sum_{i=1}^{s} a_i\alpha_i(p^k n)\alpha_i(t)\,;\ k \geq 0,\ 0 \leq t \leq p^k - 1\}$$

est fini, donc sont aussi finis les s ensembles

$$E_j = \{n \longmapsto \sum_{i=1}^{s} a_i\alpha_i(p^k n)\alpha_i(t_j)\,;\ k \geq (\operatorname{Log} t_j)/(\operatorname{Log} p)\}.$$

Comme le déterminant dét $(\alpha_i(t_j))$ est non nul, on en déduit la finitude des ensembles

$$F_i = \{n \longmapsto \alpha_i(p^k n)\,;\ k \geq 0\}.$$

Dès lors, comme les α_i sont à valeurs dans un ensemble fini, chaque ensemble de sous-suites

$$n \longmapsto \alpha_i(p^k n + t) = \alpha_i(p^k n)\alpha_i(t)$$

est aussi fini quand k parcourt les entiers positifs et t les entiers entre 0 et $p^k - 1$. Les suites α_i sont donc p-automatiques.

4. Preuve du théorème 1′

Ce paragraphe débute par un lemme.

LEMME. — *Soient $\mu_1, \ldots, \mu_s$ des entiers p-adiques deux à deux distincts. Alors les suites $\binom{\mu_i}{n}$ sont linéairement indépendantes sur $\mathbb{F}$.*

Pour prouver ce lemme, il suffit de montrer que si $\mu_1, \ldots, \mu_s$ sont deux à deux distincts, on peut trouver un entier n tel que les $\binom{\mu_i}{n}$ soient tous nuls sauf un qui vaille 1.

Posons $\mu_i = \sum_k \mu_i^{(k)} p^k$ avec $0 \leq \mu_i^{(k)} \leq p - 1$. On définit alors:

$$D_0 = \{1, 2, \ldots, s\} \qquad \text{et} \quad n^{(0)} = \max_{j \in D_0} \mu_j^{(0)},$$

puis si D_k et $n^{(k)}$ sont définis :

$$D_{k+1} = \{j \in D_k\,;\ \mu_j^{(k)} = n^{(k)}\} \qquad \text{et} \quad n^{(k+1)} = \max_{j \in D_{k+1}} \mu_j^{(k+1)}.$$

On remarque que si i est dans D_k, alors j est aussi dans D_k si et seulement si les $k-1$ premiers chiffres p-adiques de μ_i et μ_j coïncident.

Par construction la suite D_k est décroissante, donc stationnaire :

$$\exists k_0 \; \exists D \; \forall k \geq k_0 \; D_k = D.$$

Comme D_k n'est jamais vide, D ne l'est pas non plus. De plus tous les éléments de D ont tous leurs chiffres p-adiques égaux, donc sont égaux. Par conséquent D est réduit à un élément, soit $D = \{j_0\}$.

L'entier n défini par

$$n = \sum_0^{k_0} n^{(j)} p^j$$

vérifie :

$$\binom{\mu_{j_0}}{n} = \prod_i \binom{\mu_{j_0}^{(i)}}{n^{(i)}} = 1,$$

et pour chaque j différent de j_0, il y a au moins un indice i tel que $n^{(i)} > \mu_j^{(i)}$, d'où

$$\binom{\mu_j^{(i)}}{n^{(i)}} = 0 \qquad \text{et donc} \quad \binom{\mu_j}{n} = 0.$$

Nous sommes maintenant en mesure de prouver le THÉORÈME 1'. Notons d'abord que pour μ dans $\mathbb{Z}_p$, la suite $\binom{\mu}{n}$ est p-multiplicative. Soit alors :

$$g = g(X) = \sum_{i=1}^{r} a_i (1+X)^{\mu_i} = \sum_{i=1}^{r} a_i \sum_{n=0}^{\infty} \binom{\mu_i}{n} X^n$$

d'où

$$g = \sum_{n=0}^{\infty} X^n \left(\sum_{i=1}^{r} a_i \binom{\mu_i}{n} \right).$$

Si g est algébrique sur $\mathbb{F}(X)$, alors la suite

$$n \longmapsto \sum_{i=1}^{r} a_i \binom{\mu_i}{n}$$

est p-automatique. Le THÉORÈME 2 et le LEMME ci-dessus montrent que les r suites $n \mapsto \binom{\mu_i}{n}$ sont p-automatiques. Dès lors les r suites $n \longmapsto \binom{\mu_i}{p^n}$ sont ultimement périodiques, ce qui implique $\mu_i \in \mathbb{Q} \cap \mathbb{Z}_p$ pour $i = 1, 2, \ldots, r$.

Par conséquent si $\sum_{i=1}^{r} a_i(1+X)^{\mu_i}$ est algébrique, alors les μ_i sont rationnels. La réciproque est immédiate.

BIBLIOGRAPHIE

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

[2] GELFOND (A.O.). — Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.*, t. **13**, 1967–68, p. 259–265.

[3] MENDÈS FRANCE (M.) et VAN DER POORTEN (A.J.). — Automata and the arithmetic of formal power series, *Acta Arith.*, t. **46**, 1986, p. 211–214.