Groupe de travail
d'analyse ultramétrique

Gilles Christol

Éléments algébriques

Groupe de travail d'analyse ultramétrique, tome 1 (1973-1974), exp. n° 14, p. 1-10
<http://www.numdam.org/item?id=GAU_1973-1974__1__A10_0>

Groupe de Travail d'Analyse ultramétrique
(Y. AMICE, A. ESCASSUT, P. ROBBA)
1973/74, n° 14, 10 p.

6 mai 1974

ÉLÉMENTS ALGÉBRIQUES

par Gilles CHRISTOL

Cet exposé développe et prolonge celui fait au Séminaire de Théorie des nombres [4].

1. Résumé des résultats antérieurs.

A sera l'anneau des entiers d'une extension algébrique finie de $\mathbb{Q}_p$ (on peut se placer dans le cadre un peu plus général des anneaux séparables), $\mathbb{C}_p$ désignera le complété de la clôture algébrique de $\mathbb{Q}_p$. Une A-fonction f sera une fonction analytique dans le disque $B(0 , 1^-)$, dont la série de Taylor

$$f(x) = \sum_{n=0}^{\infty} f\langle n\rangle x^n$$

est à coefficients dans A. On dira que cette A-fonction est algébrique s'il existe un polynôme P de $\mathbb{C}_p[x , y]$, non nul, et tel que

$$P(x , f(x)) = 0 \quad \text{pour tout } x \text{ de } B(0 , 1^-) .$$

DÉFINITION. - L'ensemble D(A) des A-éléments algébriques est la fermeture (pour la topologie de la convergence uniforme sur $B(0 , 1^-)$) de l'ensemble des A-fonctions algébriques.

On appelle fractions rationnelles à r variables les quotients de deux polynômes à r variables à coefficients dans $\mathbb{C}_p$ qui se développent en séries entières à coefficients dans A :

$$\frac{P(x_1 , \dots , x_r)}{Q(x_1 , \dots , x_r)} = \sum_{n_i \geq 0} \frac{P}{Q}\langle n_1 , \dots , n_r\rangle x_1^{n_1} \dots x_r^{n_r} ,$$

et on appelle diagonale de P/Q la A-fonction

$$\Delta \frac{P}{Q}(x) = \sum_{n \geq 0} \frac{P}{Q}\langle n , \dots , n\rangle x^n .$$

THÉORÈME 1. - D(A) est l'ensemble des limites uniformes de diagonales de fractions rationnelles.

Remarque. - Les diagonales de fractions rationnelles à 2 variables sont des A-fonctions algébriques et suffisent à engendrer D(A) par limite uniforme.

THÉORÈME 2. - Une A-fonction f appartient à D(A) si, et seulement si, pour tout k, les A-fonctions

$$f_{n,h}(x) = \sum_{m \geq 0} f\langle n + mp^h\rangle x^m , \quad 0 \leq n < p^h ,$$

sont en nombre fini modulo p^k.

THÉORÈME 3. - $D(A)$ est une A-algèbre complète, stable par produit de Hadamard et de Hurvitz.

Il est clair, d'après la définition, que $D(A)$ est une A-algèbre complète. Rappelons la définition du produit de Hadamard :

$$f * g(x) = \sum_{n\geq 0} f\langle n\rangle\, g\langle n\rangle\, x^n ,$$

et du produit de Hurvitz :

$$f\ H\ g(x) = \sum_{m,n\geq 0} f\langle n\rangle\, g\langle n\rangle \binom{n+m}{n} x^{n+m} .$$

Nous définissons l'opérateur U sur l'ensemble des A-fonctions par

$$Uf(x) = \sum_{n\geq 0} f\langle np\rangle\, x^n ,$$

et nous dirons que h tend multiplicativement vers l'infini ($h \longrightarrow \infty$) si h devient multiple de tout nombre fixé à l'avance (et $h \neq 0$).

THÉORÈME 4. - L'opérateur U applique $D(A)$ sur lui-même, et pour tout f de $D(A)$, la suite $U^h f$ converge vers un élément de $D(A)$, noté $\mathcal{U}f$, quand h tend multiplicativement vers l'infini.

2. Lien avec les automates (il s'agit d'une interprétation du théorème 2).

k étant donné, nous raisonnons mod p^k. Soit f appartenant à $D(A)$, nous considérons l'ensemble (fini) des $f_{n,h}$ et, sur cet ensemble, nous faisons agir les opérateurs U_i $(0 \leq i \leq p-1)$, définis par

$$U_i\, f(x) = \sum_{n\geq 0} f\langle i + pn\rangle\, x^n ,$$

la relation évidente

$$U_i\, f_{n,h} = f_{n+ip^h,h+1}$$

montre que les $f_{n,h}$ s'obtiennent à partir de f par application d'un produit de U_i.

Etant donné un nombre a de $A/p^k A$, nous pouvons définir l'automate (voir [5] pour la définition) dont les états sont les $f_{n,h}$, les transitions les U_i, l'état initial f $(= f_{0,0})$ et les états finaux les $f_{n,h}$ tels que

$$f_{n,h}(0) = a(\mathrm{mod}\ p^k) .$$

Si on identifie alors $\underset{\sim}{N}$ avec le monoïde libre engendré par l'ensemble

$$\{0 , 1 , \ldots , p-1\}$$

par l'application (non injective) :

$$n_0\, n_1\, n_2 \ldots n_h \longrightarrow n_0 + n_1\, p + \ldots + n_h\, p^h$$

on voit que les nombres de $\underset{\sim}{N}$, reconnus par l'automate, sont les n tels que, pour $p^h > n$, $f_{n,h}(0) = a(\mathrm{mod}\ p^k)$.

Remarque. - Nous utilisons le développement "p-adique" des entiers, contrairement à [5] qui utilise le développement "en base p ", mais les deux manières de lire (gauche à droite ou droite à gauche) donnent les mêmes ensembles p-reconnaissables (en inversant les U_i).

D'autre part, l'automate que nous avons construit a p transitions, et est tel que l'ensemble de ses états finaux ainsi que le complémentaire de cet ensemble sont stables par U_0 (ce qui revient à dire que l'on peut ajouter autant de zéro qu'on veut à droite du développement p-adique d'un entier sans le changer). Ces propriétés sont naturelles pour des automates qui doivent reconnaître des entiers. Etant donné un automate $\mathcal{A}$ qui possède ces propriétés, nous allons montrer que la $\underset{\sim}{Z}_p$-fonction

$$f(x) = \sum_{n\in R} x^n ,$$

où $R \subset N$ est l'ensemble des entiers reconnus par l'automate $\mathcal{A}$, appartient à $D(\underset{\sim}{Z}_p)$. Pour cela, nous remarquons que

$$f_{n,h} = \sum_{m\in R, m=n+kp^h} x^k = \sum_{k\in R_n} x^k ,$$

où R_n est l'ensemble reconnu par l'automate $\mathcal{A}_n$ qui a mêmes états, mêmes transitions, mêmes états finaux que $\mathcal{A}$, mais dont l'état initial est le transformé de l'état initial de $\mathcal{A}$ par l'opération associée au développement p-adique de n écrit (avec des 0 à droite) de façon que ce développement comporte h termes. Le nombre d'états de l'automate étant fini, il en résulte que les $\mathcal{A}_n$, donc les $f_{n,h}$ sont en nombre fini, donc que $f \in D(\underset{\sim}{Z}_p)$.

THÉORÈME 5. - f appartient à D(A) si, et seulement si, pour tout k et tout a de A , l'ensemble des n de N tels que $f\langle n\rangle = a \pmod{p^k}$ est p-reconnaissable.

Moyennant le théorème de COBHAM [5], on peut énoncer le corollaire suivant.

COROLLAIRE. - Si f(x) appartient à $\underset{\sim}{Z}[[x]]$, est algébrique (racine d'un polynôme à coefficients dans $\underset{\sim}{Z}[x]$), et a ses coefficients bornés (donc en nombre fini), c'est une fraction rationnelle (dont les pôles sont des racines de l'unité).

3. Exemples.

L'exponentielle : soit π un nombre tel que $\pi^{p-1} = p$, alors la fonction $e^{\pi x}$ appartient à $D(\underset{\sim}{Z}_p[x])$.

Il est bien connu, et facile de vérifier, que

$$e^{\pi x} = \sum \frac{\pi^n}{n!} x^n$$

converge dans $B(0 , 1^-)$. La relation $e^{\pi p^n x} = 1 + \pi p^n x \pmod{p^{2n}}$ permet alors de construire, par récurrence, une suite de fonctions f_n de $\underset{\sim}{Z}[[x]]$, dont la réduction modulo p est algébrique sur le corps à p éléments, et telle que

$e^{\pi x} = \sum \pi^n f_n$. On en déduit le résultat annoncé. Par exemple, il est clair que $f_0 = 1$, par suite f_1 doit vérifier : $(\pi f_1 + 1)^p = 1 + \pi p\, x \pmod{p^2}$, ce qui conduit à $(f_1)^p + f_1 = x \pmod p$, c'est-à-dire à $f_1(x) = \sum_n (-1)^n x^{p^n}$, ce qui peut encore s'écrire

$$e^{\pi x} = 1 + \pi \sum_{n=0}^{\infty} (-1)^n x^{p^n} \pmod{\pi^2} ,$$

ce qui se démontre facilement directement.

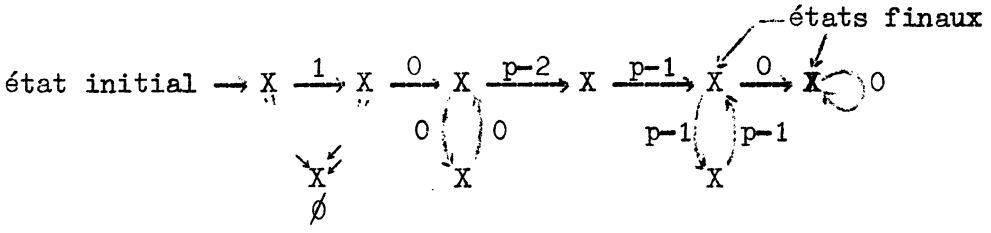
Les fonctions θ : Nous allons démontrer que l'ensemble n^2 n'est pas reconnaissable, c'est-à-dire que $\theta(x) = \sum x^{n^2}$ n'appartient pas à $D(Z_p)$; nous suivrons la méthode de [6], où le cas $p = 2$ est traité, et nous supposerons que $p \neq 2$.

LEMME. - L'ensemble des nombres de la forme $1 - 2p^{2\ell} + p^{2k}$, avec $0 < \ell < k$ est reconnaissable.

On a : $1 - 2p^{2\ell} + p^{2k} = 1 + (p-2)p^{2\ell} + \sum_{i=2\ell+1}^{2k-1} (p-1)p^i$

$$= \underbrace{1\,0\,\ldots\,0}_{2\ell-1}\,(p-2)\,\underbrace{(p-1)\,\ldots\,(p-1)}_{2(k-\ell)-1}\,0\,\ldots\,0$$

l'ensemble considéré est donc reconnu par l'automate suivant, où les flèches manquantes ont pour extrémité l'élément $\emptyset$:



LEMME. - L'ensemble des nombres de la forme $1 - 2p^{2\ell} + p^{4\ell}$ n'est pas reconnaissable.

Nous allons démontrer que $f(x) = \sum_{\ell=1}^{\infty} x^{1-2p^{2\ell}+p^{4\ell}}$ n'appartient pas à $D(Z_p)$. On a en effet :

$$f_{1,2h}(x) = \sum_{\ell=h} x^{-2p^{2(\ell-h)}+p^{4(\ell-h)+2h}}$$

$$= \sum_{\ell=0} x^{p^{2\ell}(p^{2\ell+2h}-2)} = x^{p^{2h}-2} + \ldots$$

qui sont toutes des fonctions différentes (modulo p !).

LEMME. - Si $n^2 = 1 - 2p^{2\ell} + p^{2k}$ $(0 < \ell < k)$, alors $n = 1 - p^{2\ell}$ et $k = 2\ell$.

On a d'une part $n < p^k$, et d'autre part $(n-1)(n+1) = p^{2\ell}(p^{2(k-\ell)} - 2)$, c'est-à-dire $(p \neq 2)$ que $p^{2\ell}$ divise $n-1$ ou $n+1$ et donc $p^{2\ell} - 1 \leqslant n$, ce qui conduit à $2\ell \leqslant k$. D'après $(p^k - n)(p^k + n) = 2p^{2\ell} - 1$, comme $p^k - n \geqslant 1$ et $p^k + n \geqslant p^{2\ell} + n$, on a $2p^{2\ell} - 1 \geqslant p^{2\ell} + n$, c'est-à-dire $n \leqslant p^{2\ell} - 1$, et donc $p^{2k} \leqslant p^{4\ell}$.

L'ensemble des ensembles reconnaissables étant stable par intersection (ce qui

est équivalent à la stabilité de $D(A)$ par produit de Hadamard), il en résulte que, si $\{n^2\}$ était reconnaissable, il en serait de même de $\{1 - 2p^{2\ell} + p^{4\ell}\}$, ce qui n'est pas le cas.

4. Intégration sur les entiers.

L'ensemble des ensembles d'entiers (positifs) p-reconnaissable est une algèbre au sens de la théorie de l'intégration, c'est-à-dire est stable par union, intersection et complémentaire, dans ce cadre le théorème 5 signifie que les fonctions de $D(A)$ sont les A-fonctions réglées pour cette algèbre (limite uniforme de fonctions en escalier, c'est-à-dire constantes sur des éléments de l'algèbre et ne prenant qu'un nombre fini de valeurs). Nous allons donner un exemple d'intégrale de ce type sur les entiers.

V_k désignera l'ensemble des racines p^k-ième de l'unité, l'étude du polygone de Newton du polynôme $(x + 1)^{p^k} - 1$ montre que, si u appartient à V_k, et si v désigne la valuation p-adique $(v(p) = 1)$, alors

$$v(u - 1) \geq 1/p^{k-1}(p - 1) .$$

LEMME. - *Pour tout élément* f *de* $D(A)$, *la suite*

$$\frac{1}{p^k} \sum_{u \in V_k} f(u - 1)$$

converge lorsque k *tend multiplicativement vers l'infini.*

Nous avons :

$$\frac{1}{p^k} \sum_{u \in V_k} f(u - 1) = \sum_{n=0} f\langle n \rangle \sum_{u \in V_k} (u - 1)^n / p^k .$$

Si on remarque alors que

$$\sum_{u \in V_k} u^m = \begin{cases} 0 & \text{si } p^k \text{ ne divise pas } m \\ 1 & \text{si } p^k \text{ divise } m \end{cases}$$

en utilisant la valuation de $u - 1$, il vient

$$v\Big[\frac{1}{p^k} \sum_{u \in V_k} f(u - 1) - \sum_{n=0}^{Np^k} f\langle n \rangle \sum_{m=0}^{N} (-1)^{n-m} \binom{n}{mp^k}\Big] \geq N \frac{p}{p - 1} - k .$$

Les applications, définies sur chaque k, étant bornées (le calcul précédent le montre), il suffit de démontrer que la limite existe sur un sous-ensemble dense de $D(A)$ pour établir le lemme, nous allons le montrer pour les diagonales de fractions rationnelles de deux variables : nous supposons donc que $f(x) = \Delta f(x , y)$, et nous considérons la fraction rationnelle :

$$\frac{f(t , z)}{(1 + x - xy)(1 - xtz)} = g(x , y , t , z) .$$

Il est facile de vérifier que

$$g(x , y , t , z) = \sum_{n,m,r,s,q \geq 0} (-1)^{n-m} \binom{n}{m} f\langle s , r \rangle x^{n+q} y^m t^{s+q} z^{r+q} ,$$

et donc que le coefficient du terme $(txz)^N y^m$ de cette fonction est

$$g\langle N , m , N , N\rangle = \sum_{n=0}^{N}(-1)^{n-m}\binom{n}{m} f\langle n , n\rangle ,$$

soit encore :

$$U^k g\langle N , m , N , N\rangle = \sum_{n=0}^{Np^k}(-1)^{n-m}\binom{n}{mp^k} f\langle n , n\rangle ,$$

c'est-à-dire enfin

$$v\left[\frac{1}{p^k}\sum_{u\in V_k} f(u-1) - \frac{U^k g}{1-y}\langle N , N , N , N\rangle\right] \geq N\frac{p}{p-1} - k .$$

Or on sait, d'après un théorème analogue au théorème 4, que, pour toute fraction rationnelle, la suite $U^k g$ converge uniformément lorsque k tend multiplicativement vers l'infini vers une limite $\mathcal{U}g$, il en résulte que, dans les mêmes conditions, $\Delta(U^k g)/(1-y)$ converge vers un élément de $D(A)$. Etant donné A , si nous choisissons k assez grand multiplicativement pour que $v(U^k g - \mathcal{U}g) \geq A$, et assez grand pour que $p^k\frac{p}{p-1} - k \geq A$, nous avons donc :

$$v\left[\Delta\frac{\mathcal{U}g}{1-y}\langle p^k\rangle - \frac{1}{p^k}\sum_{u\in V_k} f(u-1)\right] \geq A .$$

Comme $\Delta[\mathcal{U}g/(1-y)]$ appartient à $D(A)$, nous pouvons choisir k suffisamment grand multiplicativement pour que $v[U^k[A[\mathcal{U}g/(1-y)]] - \mathcal{U}[\Delta[\mathcal{U}g/(1-y)]]] \geq A$. Il vient donc :

$$\lim_{k\to\infty}\frac{1}{p^k}\sum_{u\in V_k} f(u-1) = \mathcal{U}[\Delta[\mathcal{U}g/(1-y)]]\langle 1\rangle .$$

THÉORÈME 6. - Si f appartient à $D(A)$, la mesure μ_f associée est à densité faible sur $\underset{\sim}{Z}_{(p)} = \underset{\sim}{Z}_p \cap Q$.

On sait en effet que la mesure μ_f vérifie (voir [1] ou [2])

$$\langle\mu_f , B(a , p^k)\rangle = \frac{1}{p^k}\sum_{u\in V_k} u^a f(u-1) ,$$

il suffit donc d'appliquer le lemme à la fonction $(1+x)^a f(x)$ en remarquant que, si a appartient à $\underset{\sim}{Z}_{(p)}$

$$(1+x)^a = \sum\binom{a}{n} x^n$$

est bien une $\underset{\sim}{Z}_p$-fonction algébrique donc appartient à $D(A)$.

5. Prolongement des éléments de $D(A)$.

Nous nous intéressons à de nouvelles formes linéaires sur $D(A)$, leurs rapports avec celle du paragraphe précédent serait instructif (voir [2]). Nous étudions ici le prolongement au voisinage de 1 , il est clair que les résultats s'étendent aux voisinages des autres points a $(|a| = 1)$. Nous utiliserons enfin la convention $f\langle n\rangle = 0$ pour $n < 0$.

LEMME. - Si f appartient à $D(A)$, pour tout n de $\underset{\sim}{Z}$, la suite

$$\sum_{k=1}^{p^h-1} f\langle n + kp^h\rangle = R(f , n , h)$$

converge quand h tend multiplicativement vers l'infini.

Il suffit de vérifier la formule :

$$R(f , n , h) = U^h[\frac{1}{1 - x} U^h(x^{p^h - n} f)]\langle 1\rangle - f\langle n\rangle ,$$

et d'appliquer le théorème 4.

Nous noterons

$$R(f , n) = \lim_{h\to\infty} R(f , n , h) .$$

DEFINITION. - f est dite prolongeable (en 1) si $R(f , n) = 0$ pour tout n de $\mathbb{Z}$.

PROPOSITION. - Si f est prolongeable, il en est de même de xf et f' .

On a $(xf)\langle n\rangle = f\langle n - 1\rangle$ et $f'\langle n\rangle = (n + 1) f\langle n + 1\rangle$, un calcul simple montre que

$$R(xf , n , h) = R(f , n - 1 , h) ,$$

c'est-à-dire $R(xf , n) = R(f , n - 1)$ d'une part, et que

$$R(f' , n , h) = (n + 1) R(f , n + 1 , h) \pmod{p^h} ,$$

c'est-à-dire $R(f' , n) = (n + 1) R(f , n + 1)$ d'autre part ; on en déduit la proposition.

LEMME. - Si f appartient à D(A) , la suite

$$\sum_{k=1}^{p^h-1} \sum_{n=0}^{kp^h-1} f\langle n\rangle = \sum_{n=0}^{p^{2h}-p^h-1} f\langle n\rangle([\frac{n}{p^h}] + 1) = P(f , h)$$

converge quand h tend multiplicativement vers l'infini.

Le résultat provient de la relation $P(f , h) = R(\frac{xf}{1 - x} , 0 , h)$. Nous noterons P(f) la limite ainsi trouvée.

PROPOSITION. - f étant une fonction de D(A) , la fonction de y , définie par $f(1 + y) = P(f((1 + y)x))$ pour y dans $B(0 , 1^-)$, est analytique dans ce disque.

Nous avons

$$\begin{aligned} P(f((1 + y)x) , h) &= \sum_{k=1}^{p^h-1} \sum_{n=0}^{kp^h-1} (1 + y)^n f\langle n\rangle \\ &= \sum_{m=0}^{p^{2h}-p^h-1} \sum_{k=1}^{p^h-1} \sum_{n=0}^{kp^h-1} \binom{n}{m} f\langle n\rangle y^m \\ &= \sum_{m=0}^{p^{2h}-p^h-1} P(\frac{x^m}{(1 - x)^m} * f , h) y^m \end{aligned}$$

Comme $x^m/(1 - x)^m$ appartient à D(A) , d'après le lemme, les coefficients du polynôme en y : $P(f((1 + y)x) , h)$ convergent quand $h \longrightarrow \infty$, cette suite de polynômes converge donc uniformément dans toute boule $B(0 , r)$ $(r < 1)$, ce qui

démontre la proposition. $f(1 + y)$, ainsi définie, s'appellera le prolongement de f à la boule $B(1 , 1^-)$, ce prolongement a la propriété suivante :

THÉORÈME 7. - Si f est prolongeable, pour tout y de $B(0 , 1^-)$, on a

$$(xf)(1 + y) = (1 + y)\, f(1 + y)$$

$$f'(1 + y) = df(1 + y)/dy .$$

On remarque, en effet, que

$$P((xf)((1 + y)x) , h) = (1 + y)\, P(f((1 + y)x) , h) - \sum_{k=1}^{p^h-1} (1 + y)^{kp^h} f\langle kp^h - 1\rangle$$

par suite, il vient

$$(xf)(1 + y) = (1 + y)\, f(1 + y) - R(f , - 1) ,$$

ce qui donne la première partie du théorème.

D'autre part,

$$P(f'((1 + y)x) , h) = \frac{d}{dy} P(f(1 + y)x) , h) + \sum_{k=1}^{p^h-1} kp^h (1 + y)^{kp^h-1} f\langle kp^h\rangle ,$$

ce qui conduit, par passage à la limite, à la deuxième partie du théorème.

COROLLAIRE. - Si f est prolongeable et solution de l'équation différentielle linéaire à coefficients polynômes

$$P(x , d/dx).f = 0 ,$$

alors $f(1 + y)$ est solution de l'équation différentielle

$$P(1 + y , d/dy).f(1 + y) = 0 .$$

Ce corollaire découle des propositions précédentes en remarquant que le prolongé de 0 est encore 0 .

En particulier, on voit que, si une fraction rationnelle est prolongeable, sa prolongée l'est elle-même, or on vérifie [4] qu'une fraction rationnelle est prolongeable si, et seulement si, elle n'a pas de pôles dans $B(1 , 1^-)$, on a donc retrouvé le prolongement "à la Krasner".

Un autre exemple est celui de l'exponentielle : on a vu que, $\bmod \pi^2$,

$$e^{\pi x} = 1 + \sum_n (- 1)^n x^{p^n} ,$$

or $(e^{\pi x})' = \pi\, e^{\pi x}$, on vérifie alors que la condition de prolongeabilité est vérifiée, modulo π^2 , et que l'on a $e^{\pi(1+y)} = e^{\pi y} \pmod{\pi^2}$.

Remarque. - On a vérifié ci-dessus que cette théorie du prolongement marchait bien sur $D(A)$, mais il est clair qu'elle marchera pour toute fonction prolongeable pour laquelle la suite, définissant le prolongement, converge.

6. Eléments algébriques et équations différentielles.

PROPOSITION. - Si f est algébrique, f est solution d'une équation différen-

tielle linéaire à coefficients polynômes [1]

On a en effet $P(x , f) = 0$, comme $\partial P/\partial y \neq 0$, on trouve $f' = -(\partial P/\partial x)/(\partial P/\partial y)$, c'est-à-dire que f' appartient à $\underset{\sim}{C}_p(x , f)$, donc il existe un polynôme en f à coefficients fractions rationnelles en x : $Q_1(x , f) = f'$ avec deg Q_1 inférieur à deg P . On vérifie de même que $f^{(h)} = Q_h(x , f)$, il suffit alors d'éliminer $f^2 , \ldots , f^{\deg P - 1}$ dans ce système linéaire, puis de chasser les dénominateurs pour obtenir le résultat cherché.

COROLLAIRE. - Si f est algébrique, la suite $f\langle n\rangle$ vérifie une récurrence linéaire à coefficients polynômes en n .

Nous cherchons maintenant une réciproque à cette proposition : nous considérons une suite de nombres de A vérifiant

$$P(n)\, f\langle n\rangle = P_1(n)\, f\langle n - 1\rangle + \ldots + P_k(n)\, f\langle n - k\rangle ,$$

et nous supposons que les coefficients des P_i sont dans les entiers de $\underset{\sim}{C}_p$ (ce qui est toujours possible).

PROPOSITION. - Si $P(.)$ n'a pas de racine dans $\underset{\sim}{Z}/p\underset{\sim}{Z}$ la fonction

$$f(x) = \sum f\langle n\rangle\, x^n$$

est un élément analytique.

Dans ce cas, $P(n)$ est une unité de $\underset{\sim}{C}_p$ pour tout n . De la récurrence, on déduit une matrice $A(n)$ dont les coefficients sont des combinaisons de termes $P_i(n + a)/P(n + a)$, telle que

$$\begin{pmatrix} f\langle n + p^h\rangle \\ f\langle n + p^h + 1\rangle \\ \vdots \\ f\langle n + p^{2h} - 1\rangle \end{pmatrix} = A(n) \begin{pmatrix} f\langle n\rangle \\ f\langle n + 1\rangle \\ \vdots \\ f\langle n + p^h - 1\rangle \end{pmatrix}$$

on vérifie alors que $A(n + p^h) = A(n) \mod p^h$, A n'ayant qu'un nombre fini d'éléments modulo p^h , il en résulte qu'il existe m et m' tels que

$$f\langle m' p^h\rangle = f\langle mp^h\rangle , f\langle m' p^h + 1\rangle = f\langle mp^h + 1\rangle \ldots f\langle m' p^h + p^h - 1\rangle = f\langle mp^h + p^h - 1\rangle \mod p^h ,$$

cela montre donc que $f\langle n + mp^h + \lambda(m' - m)p^h\rangle = f\langle n + mp^h\rangle$ pour tout n et λ , c'est-à-dire que f est périodique modulo p^h pour tout h , ce qui démontre la proposition.

PROPOSITION. - Si $f\langle n\rangle$ satisfait à la récurrence :

$$n(n + 1) \ldots (n + k)\, f\langle n\rangle = Q(n)\, f\langle n - 1\rangle ,$$

où $Q(n)$ est un polynôme en n qui a toutes ses racines dans $\underset{\sim}{Z}_{(p)}$, alors la fonction $f(x)$ appartient à $D(A)$.

([1]) COMTET (L.). - Enseignement math., t. 10, 1964, p. 267-270.

On écrit $Q(n) = a \prod_i (n - \alpha_i)$ avec $\alpha_i \in \mathbb{Z}_{(p)}$, et on suppose que les α_i ne sont pas des entiers positifs (sinon la récurrence ne commencerait que pour $n > \alpha_i$), il vient donc

$$\frac{f\langle n\rangle}{2! \ldots k!} = a^n \frac{\prod_i \prod_{m=1}^{n} (m - \alpha_i)}{n!(n+1)! \ldots (n+k)!} f\langle 1\rangle .$$

Pour utiliser le fait que les $f\langle n\rangle$ sont dans A, donc bornés, nous montrons le lemme suivant :

LEMME. - Si β est un nombre de $\mathbb{Z}_{(p)}$ et si $0(\beta)$ désigne le nombre maximum de zéros consécutifs dans le développement p-adique de β, on a

$$- v(\beta) \leq v((\prod_{m=1}^{n} (m - \beta))/n!) \leq \log_p(n) + 0(\beta) - v(\beta) .$$

Si on pose $\beta = \beta_0 + \ldots + \beta_h p^h + \ldots$, on vérifie que $v(m - \beta) \geq h$ si, et seulement si, m est congru à $(\beta_0 + \ldots + \beta_h p^h)$ modulo p^{h+1}, un calcul élémentaire montre alors que

$$v(\prod_{m=1}^{n} (m - \beta)/n!) = \sum_{h=0}^{\infty} (\{(n - (\beta_0 + \ldots + \beta_h p^h))/p^{h+1}\} - [n/p^{h+1}]) - v(\beta) ,$$

où $[\ ]$ désigne la partie entière, et $\{\alpha\}$ vaut $[\alpha] + 1$ si $0 \leq \alpha$ et 0 si $0 > \alpha$.

La première inégalité s'en déduit immédiatement, pour la deuxième il suffit de compter le nombre de h tels que $(\beta_0 + \ldots + \beta_h p^h) \leq n$.

On remarque alors que, si β appartient à $\mathbb{Z}_{(p)}$, la suite des β_i est périodique, donc, si β n'est pas entier, $0(\beta)$ est borné. Soit donc h le nombre des racines de Q, il vient :

$$(k - h)\, v(n!) \leq h \log_p(n) + n v(a) + \text{Cte} ,$$

en particulier si $n = p^m$, et m assez grand, on trouve : $v(a) \geq (k - h)/(p - 1)$. Ceci permet alors d'écrire f comme un produit de Hadamard de $(1 + x)^{\alpha_i}$ et de $(k - h)$ fois $e^{\pi x}$, qui appartiennent à $D(A)$.

BIBLIOGRAPHIE

[1] AMICE (Yvette). - Mesures p-adiques, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 6e année, 1964/65, n° 16, 6 p.

[2] BARSKY (Daniel). - Mesures p-adiques à densité, Thèse Sc. math. Univ. Paris-VI, 1974.

[3] BERSTEL (Jean). - Ensembles reconnaissables de nombres, Université Paris-VI, Institut de Programmation, n° I.P.73.39.

[4] CHRISTOL (Gilles). - Eléments analytiques uniformes et multiformes, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 15e année, 1973/74, n° 6, 18 p.

[5] COBHAM (Alan). - On the base dependence of sets of numbers recognizable by finite automata, Math. Systems Theory, t. 3, 1969, p. 186-192.

[6] RITCHIE (Robert W.). - Finite automata and the set of squares, J. Assoc. Comp. Mach., t. 10, 1963, p. 528-531.

Gilles CHRISTOL
Résidence du Bois des Roches
Bâtiment 29, Escalier 1
91240 SAINT-MICHEL-sur-Orge

(Texte reçu le 10 juin 1974)