

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

CHARLES PISOT

L'analyse p -adique en théorie des nombres

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 5 (1963-1964), exp. n° 1, p. 1-6

http://www.numdam.org/item?id=SDPP_1963-1964__5__A1_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1963-1964, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » 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/>

L'ANALYSE p-ADIQUE EN THEORIE DES NOMBRES

par Charles PISOT

La théorie des nombres a fait de grands progrès quand on y a introduit l'analyse, en particulier les fonctions de variable complexe. L'idée essentielle consiste, pour étudier une suite infinie d'entiers ou de rationnels u_n , de leur associer une "fonction génératrice" à savoir

$$f(z) = \sum_{n=0}^{\infty} u_n z^n$$

et de traduire les propriétés des u_n en propriétés de $f(z)$. Donnons un exemple très élémentaire : si u_n est le nombre de solutions en entiers $u, v \geq 0$ de l'équation $u + 2v = n$, on a

$$f(z) = \left(\sum_{u=0}^{\infty} z^u \right) \left(\sum_{v=0}^{\infty} z^{2v} \right),$$

donc

$$f(z) = \frac{1}{1-z} \cdot \frac{1}{1-z^2} = \frac{1}{(1-z)^2 (1+z)} = \frac{1}{4} \left\{ \frac{2}{(1-z)^2} + \frac{1}{1-z} + \frac{1}{1+z} \right\}.$$

D'où

$$u_n = \frac{1}{4} \{ 2(n+1) + 1 + (-1)^n \} = \left[\frac{n}{2} \right] + 1.$$

On constate cependant le fait que $z \in \mathbb{C}$ n'est pas intervenu ; on aurait pu prendre z dans un autre corps contenant \mathbb{Q} . Or \mathbb{C} est obtenu comme clôture algébrique de la complétion de \mathbb{Q} relativement à la valeur absolue ordinaire. On peut alors se demander si la valeur absolue ordinaire est la seule valeur absolue sur \mathbb{Q} . Il n'en est rien. Rappelons qu'une valeur absolue sur un corps K est une application de K dans les réels positifs vérifiant :

1° $|\alpha| \geq 0$ et $|\alpha| = 0 \iff \alpha = 0$.

2° $|\alpha\beta| = |\alpha| |\beta|$.

3° $|\alpha + \beta| \leq |\alpha| + |\beta|$.

1° et 2° montrent qu'une valeur absolue sur \mathbb{Q} est déterminée si on connaît $|p|$ pour tout nombre premier. OSTROWSKI a montré que les seules valeurs absolues sur \mathbb{Q} sont, du point de vue topologie associée, soit la valeur absolue triviale $|p| = 1$ pour tout p , $|0| = 0$, soit la valeur ordinaire, soit $|p| = \frac{1}{p}$

pour un p fixé, $|0| = 0$ et $|p'| = 1$ si $p' \neq p$. On appelle alors \mathbb{Q}_p le complété de \mathbb{Q} relativement à cette dernière valeur absolue et un élément $\alpha \in \mathbb{Q}_p$ est appelé nombre p -adique. L'inégalité 3° est remplacée par l'inégalité plus stricte :

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

dite inégalité ultramétrique.

Corps ultramétrique. - Soit K un sur-corps de \mathbb{Q}_p muni d'une valeur absolue ultramétrique notée $|\cdot|_p$ dont la restriction à \mathbb{Q}_p est celle de \mathbb{Q}_p . Considérons dans K une série de Laurent

$$f(z) = \sum_{n=-\infty}^{+\infty} a_n z^n, \quad a_n \in K, \quad z \in K.$$

Elle converge si et seulement si

$$\lim_{n \rightarrow +\infty} |a_n z^n|_p = 0.$$

Posons $|z|_p = \rho$, et supposons $\lim_{n \rightarrow +\infty} |a_n|_p \rho^n = 0$, alors

$$\mu(\rho) = \sup_{-\infty \leq n \leq +\infty} |a_n|_p \rho^n$$

est atteint pour un nombre fini de n au plus, et on aura

$$\sup_{|z|_p = \rho} |f(z)|_p \leq \mu(\rho).$$

On aura égalité si $\sup |a_n|_p \rho^n$ est atteint pour une seule valeur de n .

Géométriquement, considérons dans un système d'axes Ox, Oy la droite $y = (t - n) \log_p \rho - \log_p |a_n|_p$; elle passe par le point A_n : $t = n$, $y = -\log_p |a_n|_p$, et elle coupe Oy en un point d'ordonnée $-\log_p (|a_n|_p \rho^n)$. L'enveloppe convexe inférieure des points A_n constitue le "polygone de Newton" de $f(z)$ [3]. Sa droite d'appui, de pente $\log_p \rho$ coupe Oy au point d'ordonnée $-\log_p \mu(\rho)$. Lorsque cette pente $\log_p \rho$ est telle que la droite d'appui rencontre le polygone de Newton en un seul sommet, on a

$$|f(z)|_p = \mu(\rho), \quad \text{pour tout } z, \quad \text{avec } |z|_p = \rho.$$

Les zéros de $f(z)$ ne peuvent donc avoir pour valeur absolue que des valeurs ρ telles que $\log_p \rho$ soit la pente d'un côté du polygone. La réciproque de ceci est vraie; on a :

LEMME de HENSEL. - Si le polygone de Newton de $f(z)$ a un côté joignant les sommets A_n et A_{n+d} , $d \geq 1$, alors $f(z)$ se décompose dans K en un produit $P(z)g(z)$, où $P(z)$ est un polynôme de degré d , dont le polygone de Newton est un segment parallèle à A_n, A_{n+d} , et où $g(z)$ est une série de Laurent dont le polygone de Newton n'a pas de côté parallèle à A_n, A_{n+d} .

Il en résulte qu'un polynôme irréductible de \mathbb{Q}_p a nécessairement son polygone de Newton réduit à un seul segment et que, par suite, la seule manière de prolonger la valeur absolue de \mathbb{Q}_p à une extension algébrique de degré n de \mathbb{Q}_p , est de poser

$$|\alpha|_p = |N(\alpha)|_p^{1/n}.$$

On vérifie alors sans peine que l'on a ainsi une valeur absolue. On passe ainsi à la clôture algébrique Ω_p . Cette clôture n'est pas complète; en la complétant, on obtient un nouveau corps $\hat{\Omega}_p$ complet, et on montre qu'il est algébriquement clos. Les valeurs absolues dans $\hat{\Omega}_p$ sont toutes de la forme p^r où $r \in \mathbb{Q}$.

L'ensemble des α d'une extension algébrique de \mathbb{Q}_p vérifiant $|\alpha|_p \leq 1$ constitue un anneau A , dans lequel l'ensemble des α avec $|\alpha|_p < 1$ constitue un idéal premier maximal P ; le corps $k = A/P$ est de caractéristique p et s'appelle corps des restes. Pour \mathbb{Q}_p , on a $k = \mathbb{Z}_p$ et pour une extension finie de \mathbb{Q}_p , le corps k est une extension finie de \mathbb{Z}_p , donc a un nombre fini d'éléments. On en déduit que A est compact dans ces corps, tandis que A n'est plus compact dans les extensions infinies de \mathbb{Q}_p . Les extensions finies de \mathbb{Q}_p ressemblent donc au corps \mathbb{R} , tandis que les extensions infinies ressemblent à \mathbb{C} .

Dans ces dernières, en particuliers dans Ω_p et dans $\hat{\Omega}_p$ on peut montrer que si l'on pose

$$M(\rho) = \sup_{|z|_p = \rho} |f(z)|,$$

on a

$$\mu(\rho) = M(\rho),$$

même si $\log_p \rho$ est la pente d'un côté du polygone de Newton de la série de Laurent $f(z)$.

Il en résulte que dans Ω_p , et aussi dans $\hat{\Omega}_p$, les inégalités de Cauchy sont valables :

$$|a_n|_p \leq \frac{M(\rho)}{\rho^n}.$$

De même, le polygone de Newton de $f(z)$ montre que, quel que soit a , $f(z) = a$ a au plus un nombre fini de solutions dans tout domaine $0 < r \leq |z|_p \leq R$, où $f(z)$ converge pour $r \leq |z|_p \leq R$.

Applications.

THÉORÈME de MAHLER [5]. - Soit

$$u_n = \sum_{i=1}^s \lambda_i \alpha_i^n,$$

où λ_i, α_i sont des nombres algébriques d'une extension de \mathbb{Q} . On peut toujours choisir p tel que p ne divise pas $\prod_{i=1}^s [N(\alpha_i)]$, alors, dans une certaine extension finie de \mathbb{C}_p , on aura

$$|\alpha_i|_p = 1 \text{ pour } i = 1, \dots, s.$$

Comme (mod P), il y a un nombre fini de classes, il existe un exposant entier m tel que

$$|\alpha_i^m - 1|_p \leq \frac{1}{p} \text{ pour } i = 1, \dots, s.$$

La série

$$f_i(z) = (1 + \beta_i)^z = 1 + \frac{z}{1} \beta_i + \frac{z(z-1)}{2!} \beta_i^2 + \dots$$

où $\beta_i = \alpha_i^m - 1$ est alors convergente pour $|z|_p \leq 1$, et on peut l'écrire comme une série de Taylor. Si $u_n = 0$ pour une infinité de n , il existe au moins un entier a tel que $u_n = 0$ pour une infinité de n de la forme $hm + a$. Considérons alors la fonction

$$f(z) = \sum_{i=1}^s \lambda_i \alpha_i^a f_i(z),$$

elle est nulle pour une infinité de z dans $|z|_p \leq 1$ à savoir pour les valeurs de $z = h$ précédentes. Comme la boule unité est compacte, ces zéros auraient une valeur d'accumulation dans $|z|_p \leq 1$, ce qui entraîne que $f(z)$ est identiquement nul, donc $u_n = 0$ pour tout $n \equiv a \pmod{m}$.

Ce théorème est à l'origine de travaux de SKOLEM [7] et CHABAUTY [2], où, au lieu de sommes précédentes, on considère des expressions de la forme :

$$\sum_{i_1, \dots, i_q} \lambda_{i_1, \dots, i_q} \alpha_{i_1}^{n_1} \dots \alpha_{i_q}^{n_q},$$

où les λ et les α sont algébriques sur $\underline{\mathbb{Q}}$. Si de telles expressions sont nulles pour une infinité de systèmes (n_1, \dots, n_q) , il en résulte que, dans certaines conditions, elle est nulle sur toute une variété algébrique des (n_1, \dots, n_q) . Cette méthode s'applique avec succès à l'étude d'équations diophantiennes faisant intervenir les unités d'un corps algébrique, comme par exemple des équations de la forme

$$N\left(\sum_i \alpha_i x_i\right) = a \quad \text{où } a \in \underline{\mathbb{Z}}, \quad x_i \in \underline{\mathbb{Z}},$$

et les α_i sont des entiers algébriques.

Fractions rationnelles. - Une condition nécessaire et suffisante pour que

$$f(z) = \sum_{n=0}^{\infty} u_n z^n$$

soit le développement d'une fraction rationnelle est que les déterminants de Kronecker :

$$D_n = \begin{vmatrix} u_0 & u_1 & \dots & u_n \\ u_1 & u_2 & \dots & u_{n+1} \\ \dots & & & \\ u_n & u_{n+1} & \dots & u_{2n} \end{vmatrix}$$

sont nuls pour $n \geq n_0$. Cette condition est par exemple satisfaite si les u_n sont rationnels et si on peut obtenir une majoration telle que

$$|D_n| \prod_p |D_n|_p < 1 \quad \text{pour } n \geq n_0.$$

Il en est ainsi si, dans $\underline{\mathbb{C}}$, $f(z)$ est prolongeable en une fonction méromorphe dans un cercle $|z| \leq R$, et, dans chaque $\underline{\mathbb{Q}}_p$, prolongeable dans un cercle $|z|_p \leq R_p$, et que $R \prod_p R_p > 1$.

On peut déduire de ce théorème l'existence d'ensembles de nombres algébriques fermés [6].

Un résultat extrêmement important a été obtenu par DWORK [4] : soit $f(x_1, \dots, x_n) = 0$ un polynôme à coefficients dans le corps fini $K_1 = \underline{\mathbb{Z}}_p$. Soit $P = (x_1, \dots, x_n)$ un zéro de f , ses coordonnées se trouvent alors dans une certaine extension finie K_m de K_1 , où m est choisi le plus petit possible. On pose $N(P) = p^m$ nombre d'éléments de K_m . On pose

$$\zeta(s) = \prod_P \frac{1}{1 - \frac{1}{N(P)^s}}$$

ou encore avec $t = p^{-s}$:

$$Z_f(t) = \prod_p \frac{1}{1 - t^m} = \sum_{n=0}^{\infty} u_n t^n, \quad \text{avec } u_n \in \mathbb{Z}.$$

DWORK démontre que $Z_f(t)$ est, dans Ω_p , le quotient de deux séries entières convergeant pour tout $t \in \Omega_p$. Dans \mathbb{C} , $Z_f(t)$ converge pour $|t| < 1$, donc $Z_f(t)$ est une fraction rationnelle.

On peut alors se demander si les séries de Laurent sont les mieux adaptées à étudier les fonctions de Ω_p . Dans le cas des extensions finies de \mathbb{Q}_p , Mme AMICE [1] a montré que les séries d'interpolation jouent un rôle très important ; nous les avons d'ailleurs rencontrés dans la série $(1 + \beta)^{\mathbb{Z}}$. Cette méthode semble devoir conduire à de nombreux résultats nouveaux.

BIBLIOGRAPHIE

- [1] AMICE (Yvette). - Interpolation p-adique, Bull. Soc. math. France, t. 92, 1964, p. 117-180 (Thèse Sc. math. Paris, 1963).
- [2] CHABAUTY (Claude). - Sur les équations diophantienne liées aux unités d'un corps algébrique fini, Annali di Mat. pura ed appl., t. 17, 1938, p. 127-168.
- [3] DUMAS (Gustave). - Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, J. Math. pures et appl., Série 6, t. 2, 1906, p. 191-258.
- [4] DWORK (Bernard). - On the rationality of the zeta function of an algebraic variety, Amer. J. of Math., t. 82, 1935, p. 631-648.
- [5] MAHLER (Kurt). - Eine arithmetrische Eigenschaft der Taylor-Koeffizienten rationaler Functionen, Proc. nederl. Akad. Wet., t. 38, 1935, p. 51-60.
- [6] PISOT (Charles). - Familles compactes de fractions rationnelles et ensembles fermés de nombres algébriques, Ann. scient. Ec. Norm. Sup., Série 3, t. 81, 1964, p. 165-188.
- [7] SKOLEM (Thoralf). - Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen, Math. Annalen, t. 111, 1935, p. 399-424.