GROUPE DE TRAVAIL
D'ANALYSE ULTRAMÉTRIQUE

DANIEL BERTRAND

Transcendance dans le domaine *p*-adique

Groupe de travail d'analyse ultramétrique, tome 1 (1973-1974), exp. nº 10, p. 1-7
<http://www.numdam.org/item?id=GAU_1973-1974__1__A7_0>

TRANSCENDANCE DANS LE DOMAINE p-ADIQUE

par Daniel BERTRAND

Nous nous proposons de donner une version simplifiée de la démonstration de K. MAHLER [2] sur l'équivalent p-adique du théorème de Gel'fond-Schneider (si α et β sont deux nombres algébriques, $\alpha \neq 0 , 1$; $\beta \notin \underset{\sim}{Q}$, alors α^{β} est transcendant).

I. Préliminaires

1. Nombres algébriques sur $\underset{\sim}{Q}$ dans $\underset{\sim}{C}_p$.

Soit $\underset{\sim}{C}_p$ le complété de la clôture algébrique Ω_p du corps des nombres p-adiques $\underset{\sim}{Q}_p$, pour la valeur absolue, non archimédienne canonique prolongeant celle de $\underset{\sim}{Q}_p$. Nous la notons $|\ |_p$, et la normalisons par : $|p|_p = \frac{1}{p}$.

Soient x un élément de $\underset{\sim}{C}_p$ algébrique sur $\underset{\sim}{Q}$, K un corps de nombres de degré n sur $\underset{\sim}{Q}$ contenant x , Σ l'ensemble des plongements de K dans $\underset{\sim}{C}$, corps des nombres complexes. Si D est le dénominateur de x , i. e. le plus petit entier positif tel que Dx soit un entier algébrique, nous poserons :

$$s(x) = \sup_{\sigma\in\Sigma} (\log D \ , \ \log |\sigma x|_{\infty}) \ ,$$

où log désigne le logarithme népérien, et $|\ |_{\infty}$ la valeur absolue usuelle sur $\underset{\sim}{C}$. s(x) s'appelle la taille du nombre algébrique x . Elle est positive, ou nulle si x est racine de l'unité.

PROPOSITION 1. - Pour tout x élément non nul d'un corps de nombres K , on a

$$- 2[K : Q]\, s(x) \leqslant \log |x|_p \ .$$

Démonstration (cf. SERRE [3]). - Soit D le dénominateur de x . y = Dx est un entier algébrique vérifiant $|y|_p \leqslant |x|_p$, car $|D|_p \leqslant 1$. Sa norme $N_{K/\underset{\sim}{Q}}\, y$ est un élément de $\underset{\sim}{Z}$, divisible par y dans l'anneau des entiers de K . Donc

$$|y|_p \geqslant |N_{K/\underset{\sim}{Q}}\, y|_p \ .$$

Mais d'après la formule du produit sur $\underset{\sim}{Q}$, et le fait que $N_{K/\underset{\sim}{Q}}\, y \in \underset{\sim}{Z}$, a une valuation q-adique $\geqslant 0$ pour tout nombre premier q , on a, y étant non nul

$$|N_{K/\underset{\sim}{Q}}\, y|_p \geqslant \frac{1}{|N_{K/\underset{\sim}{Q}}\, y|_{\infty}} \ .$$

Or

$$|N_{K/\underset{\sim}{Q}}\, y|_{\infty} = \prod_{\sigma\in\Sigma} |\sigma y|_{\infty} \leqslant [\sup_{\sigma} |D.\sigma(x)|_{\infty}]^{[K:\underset{\sim}{Q}]}$$

soit

$$\log |N_{K/\mathbb{Q}}\, y|_\infty \leq 2[K : \mathbb{Q}]\, s(x) ,$$

d'où la proposition.

Remarque. - On peut améliorer cette inégalité de la façon suivante. Soit M_K l'ensemble des valeurs absolues normalisées de K. La valeur absolue $|\ |_p$ de Ω_p induit sur K une valeur absolue non normalisée correspondant à l'un des idéaux premiers $\mathfrak{p}_i$ au-dessus de p dans l'anneau des entiers de K. On a

$$|x|_p = \|x\|_{\mathfrak{p}_i}^{1/n_i} ,$$

où n_i désigne le degré local $[K_{\mathfrak{p}_i} : \mathbb{Q}_p]$.

L'élément Dx étant entier sur $\mathbb{Q}$, on a, pour toute valeur absolue de M_K, $\|Dx\|_q \leq 1$. La formule du produit sur K, qui s'écrit :

$$\prod_{q \text{ places finies}} \|Dx\|_q \times \prod_{v \text{ places finies}} \|Dx\|_v = 1$$

entraîne alors

$$1 \leq \|Dx\|_{\mathfrak{p}_i} \times 1 \times [\sup_{\sigma\in\Sigma} D|\sigma(x)|_\infty]^{[K:\mathbb{Q}]} ,$$

soit

$$\log |Dx|_p \geq 2\,\frac{n}{n_i}\, s(x) .$$

Autrement dit, on a le résultat suivant.

PROPOSITION 1 bis. - Soient x un élément de $\mathbb{C}_p$ non nul, K un corps de nombres de degré n le contenant. Si γ désigne le plus petit degré local au-dessus de p, on a

$$- 2\,\frac{n}{\gamma}\, s(x) \leq \log |x|_p .$$

Cas particulier. - Soit K une extension galoisienne de $\mathbb{Q}$ contenant x. Le groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$ échangeant les places $\mathfrak{p}_j$ au-dessus de p, tous les degrés locaux $[K_{\mathfrak{p}_j} : \mathbb{Q}_p]$ sont égaux, et l'on a $n = gn_i$. L'inégalité s'écrit alors :

$$- 2gs(x) \leq \log|x|_p ,$$

où g désigne le nombre d'idéaux au-dessus de p dans sa décomposition dans l'anneau des entiers de K.

2. Un "lemme de Schwarz".

Nous construirons une fonction analytique ayant beaucoup de zéros, et nous aurons besoin de majorer la valeur qu'elle prend en un point de son domaine de convergence. On a pour cela la proposition suivante.

PROPOSITION 2. - Soit f une fonction analytique convergeant dans le disque

$D(0\ ,\ R^+)$ <u>de</u> $\underset{\sim}{C}_p$, <u>et ayant les racines dans le disque</u> $D(0\ ,\ R')$, $R' < R$.
<u>Alors</u> :

$$|f|_{R'} \leq \left(\frac{R'}{R}\right)^h |f|_R ,$$

<u>où</u> $|f|_\rho$ <u>désigne la fonction</u> $\sup_{|z|_p \leq \rho} |f(z)|_p$.

<u>Démonstration</u>. - Nous utiliserons la méthode du polygôme de Newton (cf. LAZARD [1]). Si $f(z) = \sum_{n \in \underset{\sim}{N}} a_n z^n$, nous posons, $\forall \mu \in \underset{\sim}{R}$,

$$v(f\ ,\ \mu) = \inf_{n \in \underset{\sim}{N}} (v(a_n) + n\mu) ,$$

où v désigne la valuation de $\underset{\sim}{C}_p$, et nous considérons, pour $\xi \in \underset{\sim}{N}$, la fonction de Newton :

$$Nw(f\ ,\ \xi) = \sup_{\mu \in \underset{\sim}{R}} (v(f\ ,\ \mu) - \mu\xi) ,$$

dont le graphe est le polygone de Newton de f . Si $n(f\ ,\ \mu')$ (resp. $N(f\ ,\ \mu')$) désigne le plus petit (resp. le plus grand) entier i tel que $v(f,\mu') = v(a_i) + i\mu'$ on a, pour tout $\xi \in [n(f\ ,\ \mu')\ ,\ N(f\ ,\ \mu')]$:

$$Nw(f\ ,\ \xi) = v(f\ ,\ \mu') - \mu'\xi \geq v(f\ ,\ \mu) - \mu\xi , \qquad \forall \mu \in \underset{\sim}{R} .$$

Choisissons alors $\mu < \mu' \in \mathrm{Conv}(f)$ de façon que

$$\begin{cases} R' < 1/p^{\mu'} < 1/p^{\mu} < R . \\ v(f\ ,\ \mu) = \inf_{v(z)=\mu} v(f(z)) . \end{cases}$$

C'est possible puisque le groupe de valuation de $\underset{\sim}{C}_p$, $\underset{\sim}{Q}$, est dense dans $\underset{\sim}{R}$, où l'on a choisi $R' < R$.

Soit $\xi = N(f\ ,\ \mu')$. Le nombre h de racines de f dans $D(0\ ,\ R')$ est inférieur ou égal à ξ .

De $v(f\ ,\ \mu') - \mu'\xi \geq v(f\ ,\ \mu) - \mu\xi$, on tire :

$$p^{-v(f,\mu')} \times (p^{\mu'})^\xi \leq p^{-v(f,\mu)} \times (p^{\mu})^\xi .$$

f étant analytique dans $D(0\ ,\ R)$,

$$|f|_{R'} \leq |f|_{p^{-\mu'}} \leq p^{-v(f,\mu')} .$$

D'où

$$|f|_{R'} \times (p^{\mu'})^\xi \leq |f|_{p^{-\mu}} \times (p^{\mu})^\xi .$$

Si R n'est pas une valeur exceptionnelle de f , on conclut par continuité :

$$|f|_{R'} \times \left(\frac{1}{R'}\right)^\xi \leq |f|_R \times \left(\frac{1}{R}\right)^\xi .$$

Sinon, on choisit une suite $(R_n) < R$, R_n non exceptionnelle, et on procède de la même façon. h étant inférieur ou égal à ξ , on a déduit la proposition.

3. <u>La fonction</u> α^z .

On considère les séries :

$$\exp z = 1 + z + \frac{z^2}{2!} + \dots + \frac{z^n}{n!} + \dots$$
$$- \log z = (1 - z) + \dots + \frac{(1 - z)^n}{n} + \dots$$

exp converge dans le disque $D(0\ ,\ [p^{-1/(p-1)}[)= D$, log dans le disque $D(1\ ,\ 1^-)$ et dans le disque $1 + D$, on a :

$$\exp(\log z) = z\ .$$

exp définit un isomorphisme du groupe additif D sur le sous-groupe multiplicatif $1 + D$ du groupe des unités p-adiques de $\underset{\sim}{C}_p$. C'est un caractère que l'on peut "étendre" de façon multiforme à $\underset{\sim}{C}_p$, en posant, pour $z \notin D$, mais $p^k z \in D$

$$\exp z = (\exp p^k z)^{1/p^k}\ .$$

On peut parler encore de valeurs algébriques prises par ce "prolongement", ce qui permet de généraliser les énoncés qui suivent.

Nous définissons, pour $\alpha \in 1 + D$, la fonction :

$$\alpha^z = \exp(z \log \alpha)\ ,\ \text{pour}\ |z \log \alpha|_p < p^{-1/(p-1)}\ ,$$

c'est-à-dire, puisque $|\log \alpha|_p = |\log(1 - (1 - \alpha))|_p = |1 - \alpha|_p$, $|1 - \alpha|_p$ étant inférieur à $p^{-1/(p-1)}$:

$$|z|_p \cdot |1(1 - \alpha)|_p < p^{-1/(p-1)}\ .$$

Posons $\ell = \log \alpha$. Nous aurons à considérer les fonctions analytiques sur $D(0\ ,\ p^{-1/(p-1)} \times |\ell|_p^{-1})$:

$$z \to z \quad \text{et} \quad z \to \exp(\ell z)\ .$$

Pour $\ell \neq 0$, ces fonctions sont algébriquement indépendantes. Dans la suite, nous supposerons toujours la condition $\log \alpha \neq 0$ remplie. Cela revient à supposer que, $\forall\, s$, α n'est pas racine p^s-ième de l'unité.

Remarquons dès à présent les égalités :

$$\sup_{|z|_p \leq \rho} |z^k| = \rho^k \quad \text{et} \quad \sup_{|z|_p \leq \rho} |\exp \ell z|_p = 1$$

qui seront utiles lors de l'application du lemme de Schwarz.

II. Le théorème de Mahler

1. Enoncés.

THÉORÈME. - Soient α et β deux éléments de $\underset{\sim}{C}_p$ algébriques sur $\underset{\sim}{Q}$, tels que $\alpha \neq 0$, α non racine de l'unité, et $\beta \notin \underset{\sim}{Q}$. Si $|\alpha - 1|_p$ et $|\beta(\alpha - 1)|_p$ sont inférieurs à $p^{-1/(p-1)}$, le nombre p-adique α^β est transcendant sur $\underset{\sim}{Q}$.

De façon équivalente, on peut énoncer le théorème suivant.

THEOREME. - Soient ξ et η deux éléments de $\underset{\sim}{C}_p$ algébriques sur $\underset{\sim}{Q}$, tels que $|\xi - 1|_p$ et $|\eta - 1|_p$ soient inférieurs à $p^{-1/(p-1)}$. Alors :

$(\log \xi)/(\log \eta)$ est un nombre rationnel ou transcendant.

(Il suffit de considérer $\eta^{\log \xi/\log \eta}$, et d'utiliser le premier énoncé avec $\beta = (\log \xi)/(\log \eta)$, $\alpha = \eta$, en remarquant que $\exp \log \xi = \xi$, car $\xi \in 1 + D$.)

Remarque. - On peut donner divers énoncés géométriques de ce théorème (cf. WALDSCHMIDT [4]). Par exemple :

Soit G un groupe linéaire sur $\overline{\mathbb{Q}}$, $\varphi : D \to G(\mathbb{C}_p) = G \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$ un sous-groupe à un paramètre défini sur le disque $D = D(0, p^{-1/(p-1)})$ de $\mathbb{C}_p$. On suppose que φ ne paramétrise pas localement une courbe algébrique, autrement dit, que $\varphi(t)$ n'est pas une fraction rationnelle de t. Cela revient à dire que la matrice $\varphi'(0)$ n'est pas nilpotente. Si λ est une de ses valeurs propres non nulles, le théorème de Mahler permet de montrer, au moyen de la fonction $t \to \exp(\lambda t)$, que si γ_1 et γ_2 sont deux nombres de D algébriques sur $\mathbb{Q}$, tels que les points $\varphi(\gamma_1)$ et $\varphi(\gamma_2)$ sont sur $G_{\overline{\mathbb{Q}}}$, alors γ_1 et γ_2 sont $\mathbb{Q}$-linéairement dépendants (Prendre $\alpha = \exp(\lambda\gamma_1)$, $\beta = \gamma_1/\gamma_2$.

2. Constructions auxiliaires.

Nous allons maintenant démontrer le théorème au moyen de la "méthode de Schneider".

Supposons que α^β soit algébrique, et soit K le corps de nombres engendré sur $\mathbb{Q}$ par α, β, et α^β, $\mathcal{O}_K$ son anneau d'entiers.

Quitte à multiplier $\ell = \log \alpha$ par une puissance de p, on peut supposer que la série $\exp(\ell_z) = \alpha^z$ converge sur le disque $D(0, R^+)$, avec $R > 1$. De même, quitte à multiplier β par une puissance de p, on peut le supposer entier dans Ω_p, et alors, l'ensemble

$$A[m] = \{z = i + j\beta \text{, où } i \text{ et } j \text{ sont des entiers, } 0 \leq i , j < m\}$$

est, pour tout m, entièrement contenu dans le disque unité. β étant supposé non rationnel, le cardinal de cet ensemble est m^2.

Soit N le carré d'un entier (que l'on fera tendre vers $+\infty$). Montrons le lemme ci-après.

LEMME. - Il existe un polynôme non nul $P_N \in \mathcal{O}_K[X_1, X_2]$, de degré $R_1 \leq N^{3/2}$ par rapport à X_1, de degré $R_2 \leq 2N^{1/2}$ par rapport à X_2

$$P_N(X_1, X_2) = \sum_{\lambda_1=0,\dots,R_1-1,\ \lambda_2=0,\dots,R_2-1} p_{\lambda_1,\lambda_2} X_1^{\lambda_1} X_2^{\lambda_2}$$

tel que

$$\max_{\lambda_1,\lambda_2} s(p_{\lambda_1,\lambda_2}) \leq C_1 N^{3/2} \log N$$

et que la fonction analytique sur $D(0, R^+)$: $F_N(z) = P_N(z, e^{\ell z})$ vérifie

$$F_N(z) = 0, \quad \forall z \in A[N].$$

(C_i , $i = 1 , \dots , 7$ désignent, dans tout ce qui suit, diverses constantes ne dépendant que de α , β , α^β et R . Elles sont positives ou supérieures à 1 suivant les cas.)

Démonstration. - Il s'agit de résoudre dans $\mathcal{O}_K$ un système linéaire de $\# A[N]=N^2$ équations à $R_1 R_2$ inconnues p_{λ_1,λ_2} , dont les coefficients sont les

$$\{z^{\lambda_1} \exp(\ell z)^{\lambda_2} , \quad z \in A[N] , \quad (\lambda_1 , \lambda_2) \in [(0 , R_1 - 1) \times (0 , R_2 - 1)]\} .$$

Ce sont des éléments de K d'après l'équation fonctionnelle vérifiée par $\exp$. Leur dénominateur commun est majoré par $\mathrm{den}(\beta)^{R_1} \times \mathrm{den}(\alpha)^{NR_2} \times \mathrm{den}(\alpha^\beta)^{NR_2}$. On en déduit, par un calcul similaire, que leur taille est majorée par s , avec

$$s \leq R_1 \log N(s(\beta) + R_2 N(s(\alpha) + s(\alpha^\beta)) .$$
$$\leq C_2(R_1 \log N + R_2 N) .$$

Or, d'après DIRICHLET, SIEGEL, et autres, il existe une solution non triviale dans $\mathcal{O}_K$ de ce système, dès que $R_1 R_2 > N^2$, et cette solution vérifie :

$$\max_{\lambda_1,\lambda_2}[\sup_{\sigma\in\Sigma}|\sigma(p_{\lambda_1,\lambda_2})|_\infty] \leq C_3(C_4 R_1 R_2 \times e^{2s})^{N^2/R_1R_1-N^2} ,$$

soit

$$s(p_{\lambda_1,\lambda_2}) \leq C_5 \frac{N^2}{R_1 R_2 - N^2} (\log R_1 R_2 + 2s) .$$

Le choix $R_1 = N^{3/2}$, $R_2 = 2N^{1/2}$ donne le résultat du lemme (l'exposant $N^2/(R_1 R_2 - N^2)$ étant alors égal à 1).

$\ell = \log \alpha$ étant non nul, z et $\exp(\ell z)$ sont algébriquement indépendants. Comme $P_N \not\equiv 0$, la fonction F_N n'est donc pas identiquement nulle, et n'a, dans le disque unité, qu'un nombre fini de racines (que l'on peut d'ailleurs majorer explicitement en fonction de N). Par conséquent, il existe un entier $M \geq N$ tel que

$$F_N(z) = 0 , \quad \forall z \in A[M]$$

et

$$\exists y \in A[M + 1] \dot{-} A[M] , \quad F_N(y) \neq 0 .$$

Le nombre $x = F_N(y)$ est un élément non nul de K . Nous allons majorer $|x|_p$ et $s(x)$, et obtenir une contradiction au moyen de la proposition 1.

3. Fin de la démonstration.

Soit donc $y = i_0 + j_0 \beta$, et

$$x = \sum_{\lambda_1=0,\dots,R_1-1,\lambda_2=0,\dots,R_2-1} p_{\lambda_1,\lambda_2}(i_0 + j_0 \beta)^{\lambda_1} \exp \ell(i_0 + j_0 \beta)^{\lambda_1} .$$

$[\sup(\mathrm{den}\, \alpha_1\ \mathrm{den}(\beta) , \mathrm{den}(\alpha^p)]^{R_1+2MR_2} = D^{R_1+2MR_2}$ étant un dénominateur de x , on a

$$s(x) \leq s(D^{R_1+2MR_2}\, x) + \log D^{R_1+2MR_2} ,$$

soit

$$s(x) \leq \log R_1 R_2 + \sup_{\lambda_1,\lambda_2} s(p_{\lambda_1,\lambda_2}) + R_1 \log M\, s(\beta) + R_2 M(s(\alpha) + s(\alpha^{\beta}))$$

soit

$$(*) \qquad s(x) \leq c_6\, M^{3/2} \log M \quad (\text{car } N \leq M).$$

Par ailleurs, y se trouvant dans le disque unité, on a $|x|_p \leq |F_N|_1$. Mais il y a au moins $\# A[N] = M^2$ racines de F_N dans ce disque. F_N convergeant dans le disque $D(0, R^+)$, on a alors, d'après la proposition 2 :

$$|F_N|_1 \leq (\tfrac{1}{R})^{M^2} |F_N|_R .$$

Or $F_N(z) = \sum_{\lambda_1=0,\ldots R_1-1,\lambda_2=0,\ldots,R_2-1} p_{\lambda_1,\lambda_2}\, z^{\lambda_1} (\exp \ell z)^{\lambda_2}$.

Les p_{λ_1,λ_2}, étant des entiers algébriques, ont une valuation p-adique positive. D'autre part,

$$\sup_{|z|_p \leq R} |z^{\lambda_1} (\exp \ell z)^{\lambda_2}|_p = R^{\lambda_1} .$$

Donc

$$|F_N|_R \leq R^{R_1} \quad \text{et} \quad |x|_p \leq R^{-M^2+M^{3/2}} .$$

Ainsi

$$(**) \qquad \log |x|_p \leq c_7\, M^2 .$$

Les résultats $(*)$ et $(**)$, joints au fait que x non nul vérifie dans K la proposition 1, sont contradictoires pour N (donc M) suffisamment grand.

BIBLIOGRAPHIE

[1] LAZARD (M.). - Les zéros d'une fonction analytique d'une variable sur un corps valué complet. - Paris, Presses universitaires de France, 1962 (Institut des Hautes Etudes Scientifiques. Publications mathématiques, 14, p. 47-75).

[2] MAHLER (K.). - Über transzendente P-adische Zahlen, Compositio Mathematica, Groningen, t. 2, 1935, p. 259-275.

[3] SERRE (J.-P.). - Dépendance d'exponentielles p-adiques, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 7e année, 1965/66, n° 15, 14 p.

[4] WALDSCHMIDT (M.). - Transcendance dans les variétés de groupe, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 14e année, 1972/73, n° 23, 16 p.

(Texte reçu le 18 mars 1974)

Daniel BERTRAND
Centre de Mathématiques
Ecole Polytechnique
17 rue Descartes
75230 PARIS CEDEX 05