Nombres transcendants p-adiques

Alin RALAIVOLA
(Orsay 15 mai 1973)

Transcendance de α^β dans le cas p-adique

Soit p un nombre premier. On note $\mathbb{C}_p$ le complété de la clôture algébrique du corps p-adique $\mathbb{Q}_p$ et $|\,|_p$ la valeur absolue ultramétrique associée : je la prends normalisée c'est-à-dire $|p|_p = \frac{1}{p}$.

Dans le corps $\mathbb{C}_p$, α^β n'est autre que l'expression $\exp(\beta\log\alpha)$. D'où le besoin de restreindre β et α à des domaines particuliers qui sont ici les domaines de définition de la fonction logarithme et de la fonction exponentielle p-adiques.

Voici le théorème à démontrer :

Soient α et β deux éléments du corps $\mathbb{C}_p$ tels que $|\alpha-1|_p < 1$ et $|\beta\log\alpha|_p < p^{-\frac{1}{p-1}}$. On suppose que α et β sont algébriques sur $\mathbb{Q}$ et que β est irrationnel.

Alors : α^β est transcendant.

Pour la démonstration on aura besoin des deux lemmes suivants. On utilisera la notation suivante :

Notation : soit $f(z) = \sum a_n z^n$ une série entière dans $\mathbb{C}_p$. On note pour R réel positif $(R > 0)$ la quantité :

$$|f|_R = \sup |a_n|_p R^n .$$

Il est facile de voir que : 1) $|f+g|_R \leqslant \sup(|f|_R, |g|_R)$

2) $|\lambda f|_R \leqslant |\lambda|_p \, |f|_R$

3) $|f.g|_R = |f|_R . |g|_R$.

Supposons que pour $R > 0$, $|f|_R$ soit fini : pour R' tel que $0 < R' \leqslant R$ $|f|_{R'}$ est également fini et :

$$|f|_{R'} \leqslant |f|_R .$$

Le premier lemme nous donne une amélioration de cette inégalité.

Premier lemme dû à Schwarz (cf [1]). Soit $f(z) = \sum a_n z^n$ une série convergente dans le disque $|z|_p \leqslant R$. Soit $R' < R$, donc f converge aussi dans le disque $|z|_p \leqslant R'$. Supposons que f a h racines dans $|z|_p \leqslant R'$.

Alors : $|f|_{R'} \leqslant (\frac{R'}{R})^h . |f|_R$.

Démonstration : supposons que a soit racine de f dans $|z|_p \leqslant R'$. On peut écrire $f(z) = (z-a).f_1$ où $|f_1|_R < +\infty$. Ceci est évident pour $a = 0$ sinon on fait une translation pour se ramener à ce cas.

Par récurrence on peut écrire :

$$f(z) = P(z).g(z) \quad \text{où} \quad P(z) = \prod_{i=1}^{h} (z-a_i) \quad \text{et} \quad |g|_R < +\infty .$$

On a d'une manière évidente :

$$|P|_R = R^h \quad \text{et} \quad |P|_{R'} = R'^h .$$

Enfin :

$$|f|_{R'} = R'^h . |g|_{R'} \leqslant R'^h |g|_R = (\frac{R'}{R})^h R^h |g|_R = (\frac{R'}{R})^h . |f|_R \qquad \text{c.q.f.d.}$$

Le deuxième lemme concerne la taille d'un nombre algébrique : on verra que les expressions sont identiques dans le cas p-adique et le cas complexe.

Définition : soient K un corps de nombres, et $x \in K$. On appelle dénominateur de x le plus petit entier $D \geqslant 1$ tel que Dx soit entier sur z.

Posons :

$$\theta(x) = \sup(D, |\sigma(x)|_p)$$

où σ parcourt l'ensemble des plongements de x dans $\mathbb{C}$. On appelle taille de x, noté $t(x)$, le nombre $\operatorname{Log} \theta(x)$ c'est-à-dire :

$$t(x) = \sup(\operatorname{Log} D, \operatorname{Log}|\sigma(x)|_p).$$

Deuxième lemme (cf [1])

Soit $d = [K : \mathbb{Q}]$. Alors $\log |y|_p \geqslant -2d\, t(y)$ pour tout $y \in K^*$.

Démonstration : soit D le dénominateur de y. Notons $z = Dy$: z est entier sur $\mathbb{Q}$ et $|D|_p \leqslant 1$, donc $|y|_p \geqslant |z|_p$. Soit $N(z)$ la norme de z : c'est un entier, divisible par z, donc $|z|_p \geqslant |N(z)|_p$. La formule du produit donne $|N(z)|_p \geqslant \frac{1}{|N(z)|_\infty}$ en notant $|\ |_\infty$ la valeur absolue usuelle. Or $N(z)$ est le produit des conjugués de z et la norme usuelle de ceux-ci est majorée par $D.\theta(y)$, donc :

$$|N(z)|_p \geqslant D^{-d}\theta(y)^{-d} \geqslant \theta(y).^{-2d} \qquad \text{c.q.f.d.}$$

Démonstration du théorème : faisons une remarque préliminaire

Remarque 1 : soit β tel que $|\beta|_p = p^{-k}$ où $k \in Z$. Multiplions β par p^k : il est clair alors que $|\beta p^k|_p = 1$ donc appartient au disque $|z|_p \leqslant 1$. Donc quitte à multiplier β et $\log \alpha$ par des puissances de p, on peut supposer que $i + j\beta$ appartient au disque $|z|_p \leqslant 1$ (i et j sont des entiers positifs) et que la fonction $\alpha^z = \exp(z \log \alpha)$ est convergente dans $|z|_p \leqslant R$ où $R > 1$.

Raisonnons donc par l'absurde. Supposons que α^β est algébrique et considérons le corps $K = \mathbb{Q}(\alpha, \beta, \alpha^\beta)$.

Déterminons les coefficients $p(\lambda,\mu)$ du polynôme à deux variables de $K[X,Y]$ noté $P(X,Y)$ tel que si :

$$P(X,Y) = \sum_{\lambda=0}^{p(N)-1} \sum_{\mu=0}^{q(N)-1} p(\lambda,\mu)\, X^\lambda\, \varphi^\mu$$

la fonction

$$F(z) = P(z, \alpha^z) \quad \text{où} \quad z \in \mathbb{C}_p$$

ait des racines aux points $i + j\beta$ où $0 \leqslant i,j \leqslant S(N) - 1$.

(Les quantités $p(N)$, $q(N)$, $S(N)$ dépendent proportionnellement du nombre N qu'on suppose très grand et qu'on fera tendre à l'infini à la fin de la démonstration).

On a donc un système d'équations définies par :

$$F(i+j\beta) = \sum_{\nu} \sum_{\mu} p(\lambda,\mu)\, (i+j\beta)^\lambda . \alpha^{i\mu} . (\alpha^\beta)^{j\mu} = 0 \qquad (1)$$

pour $0 \leqslant i,j \leqslant S(N)-1$ $\quad 0 \leqslant \lambda \leqslant p(N)-1$ $\quad 0 \leqslant \mu \leqslant q(N)-1$.

Les inconnues sont les $p(\lambda,\mu)$ et les coefficients sont donnés par :

$(i+j\beta)^\lambda \alpha^{i\mu}\, \beta^{j\mu}$.

<u>MAJORATION de la taille des coefficients</u>

Soit d un dénominateur commun de α , β , α^β : alors $d^{p(N)+2q(N).\delta(N)}$ est un dénominateur du coefficient $(i+j\beta)^\lambda . \alpha^{i\mu} . (\alpha^\beta)^{j\mu}$, puisque :

$$d^{p(N)+2q(N).S(N)} . (i+j\beta)^\lambda\, \alpha^{i\mu}\, (\alpha^\beta)^{j\mu} = (di+jd\beta)^\lambda . (d\alpha)^{i\mu} (d.\alpha^\beta)^{j\mu} . d^{p(N)-\lambda+2q(N)\delta(N)-i\mu-j\mu}$$

est un produit d'entiers de K , donc lui-même entier de K .

Pour tout plongement σ de ce coefficient dans $\mathbb{C}$ on a :

$$|\sigma(\text{coefficient})|_p \leqslant |i+j\sigma(\beta)|_p^{\lambda} . |\sigma(\alpha)|^{i\mu} . |\sigma(\alpha^\beta)|_p^{j\mu} \leqslant |S(N)|_p^{p(N)} . (j+|\sigma(\beta)|_p)^{p(N)} .$$

$$. |\sigma(\alpha)|_p^{p(N).S(N)} . |\sigma(\alpha^\beta)|^{q(N).S(N)} .$$

Comme $|S(N)|_p \leqslant 1$, la taille des coefficients est majorée par :

$$t(\text{coefficient}) << p(N) + 2q(N).S(N).$$

D'après le lemme de Siegel, pour que le système d'équations (1) ait des relations il suffit que le nombre d'inconnues soit supérieur au nombre d'équations c'est-à-dire $p(N)q(N) > S(N)^2$.

Par exemple : $p(N) = 2N^3$, $q(N) = N$ et $S(N) = N^2$.

Puisque $p(N)$ et $q(N).S(N)$ sont du même ordre de grandeur on a donc :

$$t(\text{coefficient}) << N^3 .$$

Il existe donc un ensemble $\{p(\lambda,\mu)\}$ de solutions non triviales du système d'équations et, de plus,

$$t(p(\lambda,\mu)) << N^3 \qquad \forall\lambda \, . \, \forall\mu$$

Les fonctions z et α^z sont algébriquement indépendantes puisque z et e^z le sont. La fonction $F(z)$ n'est donc pas identiquement nulle. D'après la remarque 1 les points $i+j\beta$ sont dans le disque $|z|_p \leqslant 1$ $(0 \leqslant i,j \leqslant N^2-1)$.

C'est encore vrai pour tout indice $\underbrace{i,j}$ plus grand que N^2 . Soit donc $M(N)$ le plus petit entier tel que :

$$F(i+j\beta) = 0 \qquad \text{pour} \quad 0 \leqslant i,j \leqslant M(N)-1$$

et

$$F(i_o+j_o\beta) \neq 0 \quad \text{pour} \quad 0 \leqslant i_o,j_o \leqslant M(N) .$$

Evidemment $M(N)$ est un entier supérieur ou égal à N^2 .

Existence de $M(N)$. La fonction $F(z)$ est une série entière et on sait que le zéro d'une série entière est isolé. Dans le compact $|z|_p \leqslant 1$, les zéros de $F(z)$ ne sauraient être infinité puisque 0 deviendrait un point d'accumulation (limite de p^n lorsque $n \to \infty$) et ceci contredirait le fait d'être isolé.

On pourra utiliser aussi le théorème suivant pour l'existence de $M(N)$ (cf [2]).

Théorème : soit f une fonction méromorphe dans un disque $\mathfrak{D}$ et (z_n) une suite de points différents convergeant vers $z_o \in \mathfrak{D}$. Supposons que pour tout i, $i = 0,1....z_i$ pas pôle de f et $f(z_i) = 0$ pour $i = ,...,n$. Alors f est identiquement nulle.

Notons γ l'élément $F(i_o+j_o\beta)$.

Majoration de la taille de γ.

γ s'écrit :

$$\gamma = F(i_o+j_o\beta) = \sum_{\nu} \sum_{\mu} p(\lambda,\mu)(i_o+j_o\beta)^{\lambda}\, \alpha^{i_o\mu}(\alpha^{\beta})^{j_o\mu} .$$

Donc γ est un élément algébrique sur $\mathbb{Q}$ comme étant une somme de produits d'éléments algébriques.

Pour tout plongement σ de γ dans le corps de complexes $\mathbb{C}$ on a :

$$|\sigma(\gamma)|_p \leqslant \sup_{(\lambda,\mu)} |\sigma(p(\lambda,\mu))|_p . |i_o+j_o\ \sigma(\beta)|_p^{\lambda} . |\sigma(\alpha)|_p^{i_o\mu} . |\sigma(\alpha^{\beta})|_p^{j_o\mu}$$

de $t(p(\lambda,\mu)) << N^3$ je déduis que $|\sigma(p(\lambda,\mu))|_p << e^{N^3}$

donc :

$$|\sigma(\gamma)|_p << e^{N^3} . (1, |\sigma(\beta)|_p)^{2N^3} . |\sigma(\alpha)|_p^{M(N).N} : |\sigma(\alpha^{\beta})|_p^{M(N)N} . |M(N)|_p^{2N^3} .$$

Puisque $|M(N)|_p \leqslant 1$:

$$\operatorname*{Max}_{\sigma} |\sigma(\gamma)|_p << N^3 + 2N^3 . \operatorname*{Max}_{\sigma} . \operatorname{Log}(1+|\sigma(\beta)|_p) + M(N).N \operatorname*{Max}_{\sigma} (\operatorname{Log}|\sigma(\alpha)|_p + \operatorname{Log}|\sigma(\alpha^{\beta})|_p) - 2N^3 .$$

Remarque 2 : puisque $|\alpha-1|_p < 1$ on a $|\alpha|_p = |\alpha-1+1|_p \leqslant \sup(|\alpha-1|_p, 1) = 1$ donc $|\alpha|_p = 1$.

- D'autre part, $|\alpha^\beta|_p = |\alpha^\beta-1+1|_p \leqslant \sup(|\alpha^\beta-1|_p, 1)$; il suffit donc de démontrer que $|\alpha^\beta-1|_p$ est supérieur strictement à 1 pour déduire que $|\alpha^\beta|_p > 1$.

D'après [3] (p. 49-50) on a $|\exp(x)-1|_p = |x|_p$

donc :

$$|\alpha^\beta-1|_p = |\beta \operatorname{Log} \alpha|_p .$$

D'après la remarque 1 on suppose $|\beta|_p = 1$ donc $|\beta \operatorname{Log} \alpha|_p = |\operatorname{Log} \alpha|$. Toujours d'après cette même remarque, α^z converge dans $|z|_p \leqslant R$ où $R > 1$, on peut supposer que $|\operatorname{Log} \alpha|_p > 1$ et par conséquent $|\alpha^\beta|_p > 1$.

On déduit donc de cette remarque 2 et du fait que $M(N) \geqslant N^2$:

$$\operatorname{Log} |\bar{\gamma}|_p \ll N^3 .$$

Si d est un dénominateur commun de α, β et α^β , d^{3N^3} est un dénominateur de γ car :

$$d^{3N^3}\gamma = \sum_\lambda \sum_\mu p(\lambda,\mu)\ (di_o+j_o d\beta)^\lambda (d\alpha)^{i_o\mu} . (d\alpha^\beta)^{j_o\mu}\ d^{3N^3-\lambda-i_o\mu-j_o\mu}$$

est une somme de produits d'éléments entiers sur $\mathbb{Q}$, donc est entier lui-même. On déduit donc une majoration de la taille de γ soit : taille de $\gamma \ll N^3$.

Majoration de $|\gamma|_p$.

D'après la remarque 1, F est convergente dans $|z|_p \leqslant R$ où $R > 1$ et s'annulle aux $M(N)^2$ points $i+j\beta$ de $|z|_p \leqslant 1$.

Il est clair que :

$$|\gamma|_p = |F(i_o+j_o\beta)|_p \leqslant |F|_1 .$$

Le premier lemme donne :

$$|F|_1 \leqslant \left(\frac{1}{R}\right)^{M(N)^2} |F|_R \,.$$

Et comme $M(N) \geqslant N^2$ et $R > 1$

$$|F|_1 \leqslant \left(\frac{1}{R}\right)^{N^4} . |F|_R \qquad (2)$$

Réécrivons la quantité $F(z)$:

$$F(z) = \sum_{\nu=0}^{p(N)-1} \sum_{\mu=0}^{q(N)-1} p(\lambda,\mu)\, z^{\lambda} (\alpha^z)^{\mu} \,.$$

Les fonctions z et α^z sont continues dans le compact $|z|_p \leqslant R$, donc bornées par conséquent :

$$|F|_R \leqslant p(N).q(N) |p(\lambda,\mu)|_p . c_1^{p(N)}\, c_2^{q(N)} \leqslant c_3^{N^3}$$

où c_1, c_2, c_3 sont des constantes positives indépendantes de N.

De l'expression (2) on obtient :

$$|F|_1 \leqslant \left(\frac{1}{R}\right)^{N^4} c_3^{N^3} \leqslant c_4^{-N^4}$$

où c_4 est une autre constante positive supérieure à 1 strictement. Cette dernière majoration se déduit du fait que $N^4 > N^3$ dès que $N \geqslant 2$.

<u>Conclusion</u>. Utilisons le deuxième lemme $\mathrm{Log}|\gamma|_p \geqslant -2d\, t(\gamma)$ où $d = [K : \mathbb{Q}]$.

On obtient alors la contradiction suivante : $N^4 << N^3$ et le théorème est démontré.

Bibliographie

[1] Les dépendances d'exponentielles p-adiques par Jean-Pierre Serre, séminaire Delange Pisot Poitou 7e année 1965-66 n° 15.

[2] Un théorème plus général de transcendance p-adique fut démontré par W. Adams dans American Journal of Mathematics, 1966 (88) pages 279-308.

[3] Georges BACHMAN. Introduction to p-adic numbers and valuation theory. Academic Press.