Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Monique Nonnotte

Approximations rationnelles des nombres algébriques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 2 (1967-1968), exp. n° G5, p. G1-G9

<http://www.numdam.org/item?id=SDPP_1967-1968__9_2_A11_0>

Groupe d'Etudes de
THÉORIE DES NOMBRES
Année 1967/68, n° 5

8 janvier 1968

APPROXIMATIONS RATIONNELLES DES NOMBRES ALGÉBRIQUES

par Monique NONNOTTE

1. Introduction.

(A). - Le problème initial a été celui-ci : Soient $\alpha \in \underset{\sim}{R}$, algébrique de degré $n \geqslant 2$, et $f : \underset{\sim}{N} \to \underset{\sim}{R}^+$ une application donnée ; peut-on étudier alors les rationnels $\frac{h}{q} \in Q$ (avec $(h , q) = 1$ et $q > 0$), vérifiant $|\alpha - \frac{h}{q}| \leqslant f(q)$?

L'intérêt s'est porté plus particulièrement sur $f(q) = \frac{K}{q^\rho}$ (avec $\rho \in \underset{\sim}{R}^+$), et sur le nombre de solutions éventuelles.

La question a été posée ainsi :

Si $|\alpha - \frac{h}{q}| \leqslant \frac{K}{q^\rho}$ a une infinité de solutions, que peut-on dire de ρ ?

Or, dès que α est irrationnel, les réduites de son développement en fraction continue, sont en nombre infini et vérifient toutes

$$|\alpha - \frac{h_K}{q_K}| \leqslant \frac{1}{q_K^2} ,$$

donc on ne pourra obtenir mieux que $\rho \leqslant 2$.

LIOUVILLE, en 1844, prouve que

$$|\alpha - \frac{h}{q}| > \frac{A(\alpha)}{q^n} , \qquad \forall \frac{h}{q} \in Q , \quad \alpha \text{ algébrique de degré } n \geqslant 2 ,$$

donc $\rho \leqslant n$.

Puis les résultats, de plus en plus précis, ont été obtenus :

THUE (1908) : $\rho \leqslant \frac{1}{2} n + 1$;

SIEGEL (1921) : $\rho \leqslant s + \frac{n}{s+1}$ pour $s = 1 , 2 , \ldots , n - 1$, donc $\rho \leqslant 2\sqrt{n}$;

DYSON (1947) : $\rho \leqslant \sqrt{2n}$.

SIEGEL conjecture le premier : $\rho \leqslant 2$.

ROTH le démontre en 1955 ([4]).

(B). - De nombreuses généralisations ont été faites :

- soit en astreignant h , ou q , à une condition arithmétique supplémentaire,
- soit en recherchant les approximations rationnelles d'un nombre α algébrique p-adique, ou g-adique, ou g^*-adique.

Ainsi, RIDOUT [3], élève de ROTH, a suivi sa méthode et a démontré que :

Si $n \geqslant 2$, si $f(x) = a_0 x^n + \ldots + a_n \in \underset{\sim}{Z}[x]$ a un zéro $\zeta \in \underset{\sim}{R}$, $\zeta_1 \in \underset{\sim}{Q}_{p_1}$, $\zeta_r \in \underset{\sim}{Q}_{p_r}$, et si

$$|\zeta - \frac{h}{q}|^* \prod_{j=1}^{r} (h - q\zeta_j|^*_{p_j} \leqslant [\max(|h| , q)]^{-\rho}$$

a une infinité de solutions, alors $\rho \leqslant 2$ $[M^* = \min(1 , M)]$.

Et MAHLER [2], par une méthode légèrement différente, donne une généralisation plus large :

Soit $(p_1 , \ldots , p_r , p_{r+1} , \ldots , p_{r+r'} , p_{r+r'+1} , \ldots , p_{r+r'+r''})$ un système fixé de $r + r' + r''$ nombres premiers distincts (r , r' , r'' peuvent être nuls); soient ξ réel algébrique, ξ_1 p_1-adique algébrique (tous $\neq 0$), ξ_r p_r-adique algébrique, alors, si

$$|\xi - \frac{h}{q}|^* \prod_{j=1}^{r} |\xi_j - \frac{h}{q}|^*_{p_j} \prod_{j=r+1}^{r+r'} |h|_{p_j} \prod_{r+r'+1}^{r+r'+r''} |q|_{p_j} \leqslant K[\max(|h| , q)]^{-\rho}$$

a une infinité de solutions, $\rho \leqslant 2$.

2. Plan de la démonstration de MAHLER.

Dans le cas où $r' = r'' = 0$, c'est-à-dire dans les hypothèses mêmes du théorème de Roth :

$$|\alpha - \frac{h}{q}| \leqslant Kq^{-\rho}$$

a une infinité de solutions.

Principe général : A m solutions choisies grandes, ordonnées (et m bien sûr aussi grand que l'on veut), associer un polynôme à coefficients entiers, à m variables, vérifiant certaines conditions aux points rationnels qui nous intéressent. Puis faire une démonstration par l'absurde en supposant $\rho = 2 + 4\varepsilon$ $(\varepsilon > 0)$.

(A) Théorème de l'index.

Définition. - Soit $A(X_1 , \dots , X_m) \in \underset{\sim}{Z}[X_1 , \dots , X_m]$, $A \not\equiv 0$. On note

$$A_{j_1,\dots,j_m} = \frac{1}{j_1! \dots j_m!} \frac{\partial^{j_1+\dots+j_m}}{\partial X_1^{j_1} \dots \partial X_m^{j_m}} A \ .$$

Index de A au point $(\frac{P_i}{Q_i})$, par rapport aux entiers > 0 (ρ_i) :

$$J(A \ ; \ \rho_i \ ; \ \frac{P_i}{Q_i}) = \min_{(j_h)} \ (\sum_{h=1}^{m} \frac{j_h}{r_h})$$

pour les systèmes (j_h) tels que $A_{j_1,\dots,j_m}(\frac{P_1}{Q_1} , \dots , \frac{P_m}{Q_m}) \not\equiv 0$.

On voit facilement que :

$$J(A) = 0 \iff A(\frac{P_1}{Q_1} , \dots , \frac{P_m}{Q_m}) \not\equiv 0 \ ,$$

$$J(A \pm B) \geqslant \min(J(A) , J(B)) \ ,$$

$$J(AB) = J(A) + J(B) \ ,$$

$$J(A_{\ell_1,\dots,\ell_m}) \geqslant \max(0 , J(A) - \sum_{h=1}^{m} \frac{\ell_h}{\rho_h}) \ .$$

A l'aide de deux lemmes, le théorème de l'index prouvera que, pour des polynômes à coefficients bornés, en des points bien choisis, l'index pris par rapport aux $\rho_i = r_i = (\text{degré } A)/X_i$ n'est pas trop grand.

Un opérateur $\frac{1}{i_1! \dots i_m!} (\frac{\partial}{\partial X_1})^{i_1} \dots (\frac{\partial}{\partial X_m})^{i_m}$ sera dit d'ordre μ , et noté Δ_μ, si $i_1 + i_2 + \dots + i_m = \mu$.

Si $\varphi_0 , \dots , \varphi_{\ell-1} \in \underset{\sim}{Z}[X_1 , \dots , X_m]$, soit $\Delta_0 , \dots , \Delta_{\ell-1}$ un choix quelconque de ℓ opérateurs d'ordre $\leqslant 0 , \dots , \ell - 1$,

$$G(X_1 , \dots , X_m) = \det[\Delta_\mu \varphi_\nu(X_1 , \dots , X_m)] , \qquad \mu , \nu = 0 , \dots , \ell - 1 \ ,$$

s'appelle un wronskien généralisé.

LEMME 1. - Si les φ_i sont linéairement indépendants, sur $\underset{\sim}{Z}$, alors il existe un wronskien généralisé non identiquement nul.

Le lemme est vrai pour des polynômes d'une variable, on s'y ramènera.

LEMME 2. - $A \in \underset{\sim}{Z}[X_1 , \ldots , X_m]$, $m \geqslant 2$, $A \neq 0$, $(\deg A)/X_i = r_i$.

(a) Alors il existe un ℓ , $1 \leqslant \ell \leqslant r_m + 1$, et des opérateurs $\Delta_0 , \ldots , \Delta_{\ell-1}$ des variables $X_1 , \ldots , X_{m-1}$, tels que, si

$$F(X_1 , \ldots , X_m) = \det(\Delta_\mu \frac{1}{\nu!} (\frac{\partial}{\partial X_m})^\nu A) ,$$

alors :

(1) $F \in \underset{\sim}{Z}[X_1 , \ldots , X_m]$, $F \neq 0$;

(2) $F = U(X_1 , \ldots , X_{m-1}) V(X_m)$, avec $U \in \underset{\sim}{Z}[X_1 , \ldots , X_{m-1}]$, $V \in \underset{\sim}{Z}[X_m]$, $(\deg U)/X_i \leqslant \ell r_i$ et $(\deg V)/X_m \leqslant \ell r_m$.

(b) Si $\boxed{A} = \sup|\text{coefficients}| \leqslant a$, alors

$$\boxed{F} , \boxed{U} , \boxed{V} \leqslant [\prod_1^m (r_i + 1)]^\ell \ell! a^\ell 2^{\ell(r_1+\ldots+r_m)} .$$

On choisit, parmi les décompositions de A de la forme :

$$A(X_1 , \ldots , X_m) \equiv \varphi_0(X_m) \psi_0(X_1 , \ldots , X_{m-1}) + \ldots + \varphi_{\ell-1}(X_m) \psi_{\ell-1}(X_1 , \ldots , X_{m-1}) ,$$

celle pour laquelle ℓ est le plus petit. Alors les (φ_μ) et les (ψ_ν) sont deux familles de polynômes indépendants, et on utilise le lemme 1 en prenant deux wronskiens leur correspondant. $F(X_1 , \ldots , X_m)$ sera leur produit.

Le (b) résulte d'un calcul.

THÉORÈME de l'index. - Soient $0 < t \leqslant 1$, $a \geqslant 1$, r_i et $H_i > 0$, vérifiant

$$r_{h+1} \leqslant t r_h , \qquad r_h \log H_h \geqslant r_1 \log H_1 ,$$

$$H_1 \geqslant 2^{(1/t)m(2m+1)(m-1)} , \qquad a \leqslant H_1^{r_1 t} .$$

Soient

$$A(X_1 , \ldots , X_m) = \sum_{i_1=0}^{r_1} \ldots \sum_{i_n=0}^{r_m} a_{i_1,\ldots,i_m} X_1^{i_1} \ldots X_m^{i_m} , \text{ avec } |a_{i_1,\ldots,i_m}| \leqslant a ,$$

$$\frac{P_i}{Q_i} = \text{des rationnels tels que } \max(|P_i| , Q_i) \leqslant H_i .$$

Alors il existe $(j_1 , \ldots , j_m)$ $(j_h \in \underset{\sim}{N})$ tels que

$$\sum_1^m \frac{j_h}{r_h} \leqslant 2^{m+1}\, t^{2^{-(m-1)}} \qquad \underline{\text{et}} \qquad A_{j_1,\dots,j_m}\left(\frac{P_1}{Q_1}, \dots, \frac{P_m}{Q_m}\right) \neq 0 \ .$$

Il s'agit de majorer $J(A\ ;\ r_i\ ;\ \frac{P_i}{Q_i})$ pour A, (r_i), $(\frac{P_i}{Q_i})$ vérifiant toutes les hypothèses. On construit $F(X_1, \dots, X_m)$, introduit au lemme 2, et on étudie $J(F\ ;\ \ell r_i\ ;\ \frac{P_i}{Q_i})$. Puis on montre

$$J(F) \geqslant \sum_{\nu=1}^{\ell} \max\left(0\ ,\ J(A) - t - \frac{\nu - 1}{r_m}\right) \ .$$

B. Polynôme d'approximation : Première utilisation de l'algébricité de α.

LEMME 3. - $P(X) = c_0 X^n + c_1 X^{n-1} + \dots + c_n$, $c_0 c_n \neq 0$, $c_i \in \underset{\sim}{Z}$; $P(X)$ sans facteur multiple.

Soient $c = 2\max|c_i|$, $r_1, \dots, r_m \in \underset{\sim}{N}$, $s \in \underset{\sim}{R}$ tel que $s \geqslant 4n\sqrt{2m}$.

Alors il existe $A(X_1, \dots, X_m) \not\equiv 0$, à coefficients $a_{i_1,\dots,i_m}$ entiers, vérifiant :

(1) $|a_{i_1,\dots,i_m}| \leqslant 5(4c)^{r_1+\dots+r_m}$, et $a_{i_1,\dots,i_m} = 0$ dès que

$$\frac{1}{2}(m - s) \leqslant \sum_{h=1}^{m} \frac{i_h}{r_h} < \frac{1}{2}(m + s) \ ;$$

(2) $A_{j_1,\dots,j_m}(X, \dots, X)$ est divisible par $P(X)$ dès que

$$\sum_{h=1}^{m} \frac{j_h}{r_h} < \frac{1}{2}(m - s) \ ;$$

(3) $\overline{|A_{j_1,\dots,j_m}|} \leqslant 5(8c)^{r_1+\dots+r_m}$.

Principe de la démonstration. - On montre que le nombre de polynômes "admissibles" B, qui vérifient la 2e condition de (1), est supérieur à :

$$M = ([a] + 1)^{1/2(r_1+1)\dots(r_m+1)} \ .$$

Pour un tel B, on évalue le nombre de $B_{j_1,\dots,j_m}(\xi_\psi, \dots, \xi_\psi)$, pour toutes

les racines ξ_ψ de $P(X)$, et pour tous les (j_h) tels que

$$\sum_1^m \frac{j_h}{r_h} < \frac{1}{2}(m - s) \quad ;$$

ce nombre est inférieur à

$$M^* = [5a(4c)^{r_1+\ldots+r_m}]^{1/4(r_1+1)\ldots(r_m+1)} .$$

Alors, en choisissant $a = 5(4c)^{r_1+\ldots+r_m}$, on obtient $M > M^*$.

Le "principe des tiroirs" permet de conclure :

Il existe $\overline{B}$ et $\overline{\overline{B}}$, avec le même système de dérivées : $A = \overline{B} - \overline{\overline{B}}$ est un polynôme convenable.

C. Le théorème. - On a donc une suite infinie $(\frac{P_i}{Q_i})$ $[(P_i , Q_i) = 1 , Q_i > 0 , \max(|P_i| , Q_i) = H_i]$, avec

$$|\alpha - \frac{P_i}{Q_i}| \leqslant KH_i^{-\rho} ,$$

et

$$P(X) = 0 = c_0 \alpha^n + c_1 \alpha^{n-1} + \ldots + c_n , \qquad c = 2\max|c_i| .$$

On pose

$$\rho = 2 + 4\varepsilon , \qquad m = [2(\frac{24n}{\varepsilon})^2] + 1 , \qquad s = \frac{\varepsilon m}{6} .$$

On a ainsi bien assuré $s \geqslant 4n\sqrt{2m}$. Soit t vérifiant

$$0 < t \leqslant 1 , \qquad 2^{m+1} t^{2^{-(m-1)}} \leqslant \frac{\varepsilon m}{6} .$$

Préliminaires : On se restreint à une sous-suite de solutions vérifiant :

$$\log H_{h+1} \geqslant \frac{2}{t} \log H_h ,$$

$$H_1 \geqslant \max[(20c)^{m^2/t} , 2^{(1/t)m(m-1)(2m+1)} , T] ,$$

où T reste à déterminer, et c'est ce qui permettra de conclure.

Choisissons les r_i de telle manière qu'on obtienne immédiatement :

$r_1 \log H_1 \leqslant r_h \log H_h \leqslant (1 + \varepsilon) r_1 \log H_1 , \quad r_{h+1} \leqslant r_h t , \quad r_1 > r_2 > \ldots > r_m .$

Etapes de la preuve.

1° Il existe $A \in \underset{\sim}{Z}[X_1, \ldots, X_m]$, d'après le lemme 3.

2° De plus,

$$5(4c)^{\sum r_i} \leqslant (20c)^{mr_1} \leqslant H_1^{(1/m)r_1 t} .$$

On a donc les hypothèses du théorème de l'index :

$$\exists\, \ell_1, \ldots, \ell_m, \quad \sum_{h=1}^{m} \frac{\rho_h}{r_h} \leqslant 2^{m+1} t^{2^{-(m-1)}} \leqslant \frac{\varepsilon m}{6}, \quad A_{\ell_1,\ldots,\ell_m}\left(\frac{P_1}{Q_1}, \ldots, \frac{P_m}{Q_m}\right) \neq 0 .$$

On pose

$$A_{\ell_1,\ldots,\ell_m}\left(\frac{P_1}{Q_1}, \ldots, \frac{P_m}{Q_m}\right) = A_{(\ell)} .$$

3° Dernière étape : Majorer et minorer $|A_{(\ell)}|$ en fonction de H_1, en déduire une minoration de H_1, ce qui est absurde.

Majoration de $|A_{(\ell)}|$:

$$A_{(\ell)} = \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} A_{j_1,\ldots,j_m}(\alpha, \alpha, \ldots, \alpha)\binom{j_1}{\ell_1}\cdots\binom{j_m}{\ell_m}\left(\frac{P_1}{Q_1} - \alpha\right)^{j_1-\ell_1}\cdots\left(\frac{P_m}{Q_m} - \alpha\right)^{j_m-\ell_m},$$

avec la sommation pour (j_h) vérifiant $\sum \frac{j_h}{r} > \frac{1}{2}(m - s)$, et

$$|A_{j_1,\ldots,j_m}(\alpha, \ldots, \alpha)| \leqslant K_1^{mr_1}, \qquad \left|\frac{P_h}{Q_h} - \alpha\right| \leqslant K H_1^{-\rho} ;$$

on obtient

$$|A_{(\ell)}| \leqslant K_2^{mr_1} H_1^{-\rho r_1 S_1(m,s,t)} .$$

Minoration de $|A_{(\ell)}|$: $A_{(\ell)} = \frac{N_{(\ell)}}{D_{(\ell)}}$.

$|N_{(\ell)}| \geqslant 1$: c'est très grossier. (Dans les cas g-adique ou g^*-adique, c'est ici que MAHLER fait une distinction dans sa démonstration, par rapport au cas réel, et utilise $|\alpha_i - \frac{P}{Q}|_{P_i}$.)

$D_{(\ell)}$: chaque terme de $A_{(\ell)}$ a un dénominateur $Q_1^{i_1-\ell_1}, \ldots, Q_m^{i_m-\ell_m}$, sans oublier que

$$a_{i_1,\ldots,i_m} = 0, \qquad \text{si } \frac{1}{2}(m - s) \leqslant \sum_{h=1}^{m} \frac{i_h}{r_h} < \frac{1}{2}(m + s) ,$$

d'où

$$|D_{(\ell)}| \leqslant \text{p. p. c. m. } Q_1^{i_1-\ell_1} \dots Q_m^{i_m-\ell_m} \leqslant \max H_1^{(1+\varepsilon)r_1\left(\frac{i_1-\ell_1}{r_1}+\dots+\frac{i_m-\ell_m}{r_m}\right)} ,$$

d'où

$$|A_{(\ell)}| \geqslant H_1^{-(1+\varepsilon)r_1 S_2(m,s,t)} .$$

4° Conclusion : Alors, on voit facilement que $\rho S_1(m , s , t) - (1 - \varepsilon) S_2(m , s , t) > 0$, et même $> \frac{3\varepsilon m}{2}$, par exemple, donc

$$H_1^{3\varepsilon m/2} < K_2^m ,$$

$$H_1 < K_2^{2/3\varepsilon} ,$$

ce qui est absurde, d'où

$$\rho \leqslant 2 .$$

3. Quelques applications.

Si $f(x , y) = g(x , y)$, avec f homogène, $f \in \underset{\sim}{Z}(X , Y)$, $\deg f = n$, et $g \in \underset{\sim}{Z}(X , Y)$, $\deg g = n - K$, a un nombre infini de solutions en entiers (x , y), alors

$$K \leqslant 2 .$$

Si $|P_h - \alpha|_p \leqslant KP_h^{-\rho}$, avec α algébrique, $\alpha \in \underset{\sim}{Z}_p$, $P_h \in \underset{\sim}{N}$, a un nombre infini de solutions, alors

$$\rho \leqslant 1 .$$

Si $\rho > 2$, ROTH [1] se sert de sa propre démonstration pour obtenir une majoration du nombre, fini, de solutions de $|\alpha - \frac{h}{q}| < \frac{K}{q^{2+\zeta}}$. Cela peut se faire aussi dans le cas des entiers algébriques approchés par des entiers rationnels.

Problème posé : Ces majorations sont grossières, peut-on les obtenir plus directement ?

BIBLIOGRAPHIE

[1] DAVENPORT (H.) and ROTH (K. F.). - Rational approximations to algebraic numbers, Mathematika, London, t. 2, 1955, p. 160-167.

[2] MAHLER (Kurt). - Lectures on diophantine approximations, Part 1 : g-adic numbers and Roth's theorem. - Notre Dame (Indiana), University of Notre Dame, 1961.

[3] RIDOUT (D.). - The p-adic generalization of the Thue-Siegel-Roth theorem, Mathematika, London, t. 5, 1958, p. 40-48.

[4] ROTH (K. F.). - Rational approximations to algebraic numbers, Mathematika, London, t. 2, 1955, p. 1-20.