INDÉPENDANCE ALGÉBRIQUE DE PUISSANCES ALGÉBRIQUES DE NOMBRES ALGÉBRIQUES

par

Michel WALDSCHMIDT

-:-:-:-

Soient α et β deux nombres algébriques, $\alpha \neq 0$, $\operatorname{Log} \alpha \neq 0$, et ℓ un entier, $0 \leq \ell \leq d-1$, où $d = [\mathbb{Q}(\beta) : \mathbb{Q}]$ est le degré de β. On cherche à minorer le degré de transcendance q_ℓ sur $\mathbb{Q}$ du corps $\mathbb{Q}(\alpha^\beta, \ldots, \alpha^{\beta^\ell})$. Le théorème de Gel'fond Schneider sur la transcendance de α^β pour β irrationnel s'énonce :

$$\ell \geq 1 \Rightarrow q_\ell \geq 1 ;$$

en 1949, après avoir montré

$$d \geq 3 \Rightarrow q_{d-1} \geq 2 ,$$

A. O. Gel'fond conjectura

$$q_{d-1} = d-1 ,$$

ce qui équivaut à $q_\ell = \ell$ pour $0 \leq \ell \leq d-1$. La minoration $q_{d-1} \geq 3$ fut obtenue successivement pour $d \geq 19$ (A. A. Smelev, 1971), $d \geq 15$ (D. Brownawell, 1971), et $d \geq 7$ (G. V. Čudnovskij, 1973). Nous esquissons ici la méthode de Čudnovskij, après avoir rappelé rapidement celle de Gel'fond.

§. 1. - La méthode de Gel'fond Schneider

Soient m et k deux entiers rationnels, $1 \leq k \leq d-1$, $0 \leq m \leq d-1$. On considère une base de transcendance $(x_1, \ldots, x_q)$ sur $\mathbb{Q}$ du corps

$$K = \mathbb{Q}(\alpha^{\beta}, \alpha^{\beta^2}, \ldots, \alpha^{\beta^{m+k}}) ;$$

remarquons que

$$K = \mathbb{Q}(\alpha^{\beta}, \ldots, \alpha^{\beta^{\ell}}),$$

avec $\ell = \inf(d-1 ; m+k)$; donc $q = q_{\ell}$.

La méthode de Gel'fond Schneider permet de démontrer le résultat suivant.

PROPOSITION 1. 1. - Il existe une suite $(\xi_N)_{N \geq 1}$ d'éléments non nuls de $\mathbb{Z}[x_1, \ldots, x_q]$ vérifiant

$$t(\xi_N) \leq N$$

et

$$\operatorname{Log} |\xi_N| \ll -N^{\frac{(m+2)(k+1)}{m+k+2}} \cdot (\operatorname{Log} N)^{\frac{m+1}{m+k+2}} \quad \text{pour } N \to \infty .$$

(Si $\xi \in \mathbb{Z}[x_1, \ldots, x_q]$, $\xi \neq 0$, la taille $t(\xi)$ de ξ est le maximum du degré total de ξ et du logarithme des valeurs absolues des coefficients de ξ.)

La démonstration de la proposition 1. 1. sera utile dans la suite, car elle est à la base de la méthode de Cudnovskij.

Démonstration de la proposition 1. 1.

Notons A l'anneau $\mathbb{Z}[x_1, \ldots, x_q]$. Les symboles $c_o, c_1, \ldots, c_6$ désigneront des constantes (indépendantes de N), tandis que K , L , M seront des entiers fonctions de N , que nous expliciterons à la fin de la démonstration.

Premier pas : On construit une suite de polynômes non nuls $\Phi_N \in A[X, Y_o, \ldots, Y_m]$:

$$\Phi_N = \sum_{\lambda=0}^{L-1} \sum_{\mu_o=0}^{M-1} \cdots \sum_{\mu_m=0}^{M-1} \varphi_N(\lambda, \mu_o, \ldots, \mu_m) X^{\lambda} Y_o^{\mu_o} \cdots Y_m^{\mu_m} ,$$

<u>telle que les fonctions</u>

$$F_N(z) = \Phi_N(z, \alpha^z, \alpha^{\beta z}, \dots, \alpha^{\beta^m z})$$
$$= \sum_\lambda \sum_{\underline{\mu}} \varphi_N(\lambda, \underline{\mu}) \, z^\lambda \, \alpha^{(\mu_o + \mu_1 \beta + \dots + \mu_m \beta^m) z}$$

<u>vérifient</u> :

$$F_N(j_o + j_1 \beta + \dots + j_k \beta^k) = 0 \quad \text{pour} \quad 0 \leq j_s \leq K-1, \quad (0 \leq s \leq k) .$$

Pour cela on doit résoudre un système de K^{k+1} équations à $L.M^{m+1}$ inconnues, à coefficients dans le corps $K(\alpha, \beta)$, qui est une extension algébrique du corps $\mathbb{Q}(x_1, \dots, x_q)$. A condition que $L.M^{m+1}$ soit plus grand que K^{k+1}, on peut résoudre ce système dans A, avec

$$\max_{(\lambda, \underline{\mu})} t(\varphi_N(\lambda, \underline{\mu})) \ll L \operatorname{Log} N + M.K .$$

On remarquera que les coefficients $\varphi_N(\lambda, \underline{\mu})$ peuvent être choisis premiers entre eux dans leur ensemble dans A (ceci sera utile pour la méthode de Čudnovskij). Enfin, pour minimiser la taille de ces coefficients, on choisira $L \operatorname{Log} N$ de l'ordre de MK, et $L.M^{m+1}$ de l'ordre de $c_1 K^{k+1}$, c_1 étant une constante suffisamment grande. Dans ces conditions, si on choisit L tel que $L \gg\ll \frac{N}{\operatorname{Log} N}$, on a :

$$L \gg\ll N.(\operatorname{Log} N)^{-1} ,$$

$$K^{m+k+2} \gg\ll N^{m+2} (\operatorname{Log} N)^{-1} ,$$

$$M^{m+k+2} \gg\ll N^k \operatorname{Log} N .$$

<u>Deuxième pas</u> : <u>On montre l'existence d'une constante</u> $c_2 > 1$ <u>telle que l'un des nombres</u>

$$F_N(h_o + h_1 \beta + \dots + h_k \beta^k) , \quad -c_2 K \leq h_s \leq c_2 K , \quad (0 \leq s \leq k)$$

<u>ne soit pas nul</u> (on notera γ_N l'un de ces nombres non nul).

Ce résultat repose sur une majoration, due à R. Tijdeman :

$$(1.2) \qquad \max_{(\lambda,\underline{\mu})} |\varphi_N(\lambda,\underline{\mu})| \leq N^{c_3 K^{k+1}} \cdot \max_{|\underline{h}|\leq c_2 K} |F_N(\underline{h}.\underline{\beta})| .$$

Pour démontrer (1.2), on peut par exemple majorer

$$\max_{1\leq t\leq L.\, M^{\ell+1}} |F_N^{(t-1)}(0)|$$

en fonction de $\max\limits_{|\underline{h}|\leq c_2 K} |F_N(\underline{h}.\underline{\beta})|$, (où $\underline{h}.\underline{\beta} = h_o+h_1\beta+\ldots+h_k\beta^k$, et $|\underline{h}| = \max\limits_{0\leq s\leq k} |h_s|$), grâce à la formule intégrale de Cauchy. On exprime ensuite les $\varphi_N(\lambda,\underline{\mu})$ en fonction des $F_N^{(t-1)}(0)$ par un calcul de déterminant et de cofacteurs.

<u>Troisième pas</u> : <u>On majore</u> γ_N par le lemme de Schwarz, grâce au fait que la fonction F_N a au moins K^{k+1} zéros :

$$\text{Log } |\gamma_N| \leq -\frac{1}{c_4} K^{k+1} \text{ Log } N .$$

<u>Quatrième pas</u> : On multiplie γ_N par un dénominateur (pour que le produit soit entier sur A) et on prend sa norme ξ_N sur K . Alors $\xi_N = \gamma_N . \gamma'_N$, avec $\gamma'_N \in K(\alpha,\beta)$, et ξ_N vérifie :

$$\xi_N \in A \ , \ \xi_N \neq 0 \ , \ \text{Log } |\xi_N| \leq -\frac{1}{c_5} K^{k+1} \text{ Log } N ,$$

$$t(\xi_N) \leq c_6 \text{ L Log } N .$$

On choisit

$$L = \left[\frac{1}{c_6} N(\text{Log } N)^{-1}\right] ,$$

ce qui conduit à définir K et M par les relations

$$K = \left[c_1^{-\frac{1}{m+k+2}} \cdot \left(\frac{N}{c_6}\right)^{\frac{m+2}{m+k+2}} \cdot (\text{Log } N)^{-\frac{1}{m+k+2}}\right],$$

et

$$M = \left[c_1^{\frac{1}{m+k+2}} \cdot \left(\frac{N}{c_6}\right)^{\frac{k}{m+k+2}} \cdot (\text{Log } N)^{\frac{1}{m+k+2}}\right] .$$

Avec ce choix des fonctions K, L, M, si on note

$$c_0 = c_1^{\frac{k+1}{m+k+2}} \cdot c_5 \cdot c_6^{\frac{(m+2)(k+1)}{m+k+2}} ,$$

on a

$$\text{Log} |\xi_N| \leq -\frac{1}{c_0} N^{\frac{(m+2)(k+1)}{m+k+2}} \cdot (\text{Log } N)^{\frac{m+1}{m+k+2}} ,$$

et

$$t(\xi_N) \leq N ,$$

ce qui démontre la proposition 1. 1.

§. 2. - Le septième problème de Hilbert sur la transcendance de α^β

Les nombres ξ_N de la proposition 1. 1. ne peuvent être tous dans $\mathbb{Z}$ (sinon ils vérifieraient $\text{Log } |\xi_N| \geq 0$). Par conséquent $q \neq 0$; c'est-à-dire :

THÉORÈME 2. 1. (Gel'fond, Schneider) - Si α et β sont algébriques, $\alpha \neq 0$, $\text{Log}\, \alpha \neq 0$, $\beta \notin \mathbb{Q}$, alors $\alpha^\beta = \exp(\beta . \text{Log } \alpha)$ est transcendant.

Autrement dit

$$\ell \geq 1 \Rightarrow q_\ell \geq 1 .$$

§. 3. - Indépendance algébrique de deux nombres (d'après Gel'fond)

Supposons $q_\ell = 1$, et cherchons à majorer ℓ. Les éléments ξ_N de la proposition 1. 1. appartiennent alors à $\mathbb{Z}[x_1]$, avec $x_1 = \alpha^\beta$ par exemple.

a) Utilisation d'une mesure de transcendance de α^β

Si on veut utiliser la méthode du paragraphe 2 pour majorer ℓ, on doit minorer les nombres $P(\alpha^\beta)$, pour $P \in \mathbb{Z}[X]$, $P \neq 0$. On connait effectivement de telles minorations (obtenues en raffinant la méthode des paragraphes 1 et 2), la meilleure étant actuellement due à P. L. Cijsouw :

$$(3.1) \qquad \operatorname{Log} |P(\alpha^{\beta})| \geq -c(\operatorname{Log}\alpha, \beta, \varepsilon)\,[t(P)]^{4}\,[\operatorname{Log} t(P)]^{-1+\varepsilon}$$

pour tout $\varepsilon > 0$. On déduit ainsi de la proposition 1.1. (avec $m = k = \ell$) l'inégalité $\ell < 6$ (autrement dit $\ell \geq 6 \Rightarrow q_{\ell} \geq 2$).

b) Un critère de Gel'fond

A. O. Gel'fond a obtenu un résultat bien meilleur dans cette direction:

THÉORÈME 3.2. - Soient α et β deux nombres algébriques, $\alpha \neq 0$; $\operatorname{Log}\alpha \neq 0$, et $[\mathbb{Q}(\beta) : \mathbb{Q}] \geq 3$. Alors deux des nombres

$$\alpha^{\beta}, \ \alpha^{\beta^2}, \ \alpha^{\beta^3}, \ \alpha^{\beta^4}$$

sont algébriquement indépendants.

COROLLAIRE 3.3. - Soit α un nombre algébrique ($\alpha \neq 0$, $\operatorname{Log}\alpha \neq 0$) et soit β un irrationnel cubique. Alors les deux nombres

$$\alpha^{\beta}, \ \alpha^{\beta^2}$$

sont algébriquement indépendants.

Le théorème 3.2., qu'on peut énoncer sous la forme

$$d \geq 3 \ \text{ et } \ \ell \geq \min(d-1, 4) \Rightarrow q_{\ell} \geq 2 ,$$

est une conséquence immédiate de la proposition 1.1. et du critère de transcendance suivant.

CRITÈRE 3.4. - Soit θ un nombre complexe. On suppose qu'il existe une suite $(P_N)_{N \geq 1}$ de polynômes non nuls de $\mathbb{Z}[X]$ vérifiant

$$t(P_N) \leq N$$

et

$$\operatorname{Log} |P_N(\theta)| \leq -12\,N^2 .$$

Alors θ est algébrique.

La démonstration de ce critère est très instructive pour la suite. En voici une esquisse.

Pour N suffisamment grand, comme $P_N(\theta)$ est très petit, θ est proche d'une racine α de P_N (donc loin des autres, car les racines de P_N sont algébriques). Par conséquent, si Q_N est la plus grande puissance du polynôme minimal de α qui divise P_N, le nombre $Q_N(\theta)$ est aussi très petit

$$\operatorname{Log} |Q_N(\theta)| \leq -9N^2 ,$$
$$t(Q_N) \leq 2N .$$

Maintenant le résultant de Q_N et Q_{N+1} est un entier rationnel, majoré par

$$[\,|Q_N(\theta)| + |Q_{N+1}(\theta)|\,].\exp\{2t(Q_N).\,t(Q_{N+1})\} < 1 .$$

Donc Q_N et Q_{N+1} sont puissances d'un même polynôme irréductible R, qui est ainsi indépendant de N. Ecrivons

$$Q_N = R^{r_N} .$$

Nous aurons

$$r_N \operatorname{Log} R(\theta) \leq -8N^2 ,$$

et

$$r_N < \frac{4}{t(R)} . N ;$$

on en déduit $R(\theta) = 0$, donc θ est algébrique, et $P_N(\theta) = 0$ pour tout N suffisamment grand.

§. 4. - Indépendance algébrique de trois nombres (d'après Brownawell)

Pour obtenir une majoration de ℓ quand $q_\ell = 2$, en utilisant la méthode du §. 3. a, il faudrait connaître une mesure d'indépendance algébrique de deux nombres (x_1, x_2). Les résultats connus sont beaucoup trop faibles pour être utilisés ici.

La méthode du §. 3. b donne des résultats, à condition de généraliser le critère 3. 4. aux polynômes P_N à coefficients dans $\mathbb{Z}[\alpha^\beta]$, en utilisant (3. 1.). L'implication

$$d \geq 15\ ,\quad \ell \geq \min(d-1,\ 28)\ \Rightarrow\ q_\ell \geq 3$$

est une conséquence de la proposition 1. 1 (avec $m = k = 14$) et du critère suivant, dû à Brownawell.

CRITÈRE 4. 1. - Soient α un nombre algébrique, $\alpha \neq 0$, $\operatorname{Log} \alpha \neq 0$, et β un nombre algébrique irrationnel. Il existe une constante $C = C(\operatorname{Log} \alpha, \beta)$ ayant la propriété suivante.

Soit θ un nombre complexe. On suppose qu'il existe une suite $(P_N)_{N\geq 1}$ de polynômes non nuls de $\mathbb{Z}[X, Y]$, vérifiant

$$t(P_N) \leq N$$

et

$$\operatorname{Log} |P_N(\alpha^\beta,\ \theta)| \leq -C\, N^8\ .$$

Alors θ est algébrique sur $\mathbb{Q}(\alpha^\beta)$.

§. 5. - Indépendance algébrique de trois nombres (d'après Čudnovskij)

Nous allons présenter la démonstration, par Cudnovskij [1], du résultat suivant :

$$d \geq 7\ ,\ \text{et}\ \ \ell \geq \min(d-1,\ 12)\ \Rightarrow\ q_\ell \geq 3\ .$$

THÉORÈME 5. 1. - Soient α et β deux nombres algébriques, $\alpha \neq 0$, $\operatorname{Log} \alpha \neq 0$, et $[\mathbb{Q}(\beta) : \mathbb{Q}] \geq 7$. Alors trois des nombres $\alpha^\beta, \alpha^{\beta^2}, \dots, \alpha^{\beta^{12}}$ sont algébriquement indépendants sur $\mathbb{Q}$.

COROLLAIRE 5. 2. - Si β est irrationnel de degré 7, trois des six nombres

$$\alpha^\beta, \dots, \alpha^{\beta^6}$$

sont algébriquement indépendants.

Démonstration du théorème 5. 1.

Supposons $d \geq 7$, et $q_\ell = 2$, avec $\ell = \min(d-1\ ,\ 12)$. La proposition 1. 1., avec $m = k = 6$, prouve l'existence d'une suite $(\xi_H)_{H\geq 1}$ d'éléments non nuls de $\mathbb{Z}[x_1, x_2]$, vérifiant

$$t(\xi_H) \leq H ,$$

et

$$\text{Log } |\xi_H| \leq -\frac{1}{c_o} H^4 (\text{Log } H)^{\frac{1}{2}} .$$

Soit N un entier suffisamment grand. Nous allons construire un polynôme $P_N \in \mathbb{Z}[X]$, non nul, vérifiant

$$(5.3) \quad \begin{cases} \text{Log } |P_N(x_1)| \leq -c_7 N^4 (\text{Log } N)^{\frac{1}{2}} \\ t(P_N) \leq c_8 N^2 . \end{cases}$$

Comme x_1 est transcendant, le critère 3.4 donnera alors une contradiction.

Pour effectuer cette construction, on reprend la démonstration de la proposition 1.1. en considérant deux cas.

<u>Premier cas</u> : $\max_{|\underline{h}| \leq c_2 K} |F_N(\underline{h}.\underline{\beta})| \leq N^{-(c_3+1)K^7}$:

On déduit alors de (1.2) :

$$\max_{(\lambda, \underline{\mu})} |\varphi_N(\lambda, \underline{\mu})| \leq N^{-K^7} .$$

Pour chaque $(\lambda, \underline{\mu})$, on considère une puissance d'un facteur irréductible de $\varphi_N(\lambda, \underline{\mu})$ dans $\mathbb{Z}[x_1, x_2]$; notons $\psi_N^{(1)}$, $\psi_N^{(2)}$ deux de ces puissances correspondant à des facteurs irréductibles distincts (car les $\varphi_N(\lambda, \underline{\mu})$ sont premiers entre eux dans leur ensemble) ; on aura

$$\text{Log } |\psi_N^{(i)}(x_1, x_2)| \leq -c_9 N^4 (\text{Log } N)^{\frac{1}{2}} , \quad (i = 1, 2) ,$$

et

$$t(\psi_N^{(1)}) . t(\psi_N^{(2)}) \leq c_{10} N^4 .$$

Le résultant de $\psi_N^{(1)}$ et $\psi_N^{(2)}$ par rapport à x_2 est un élément non nul de $\mathbb{Z}[x_1]$ satisfaisant (5.3).

<u>Deuxième cas</u> : $\max_{|\underline{h}|\leq c_2 K} |F_N(\underline{h}.\underline{\beta})| > N^{-(c_3+1)K^7}$.

On commence par se ramener au cas où l'élément ξ_N , construit à la proposition 1.1, vérifie

$$-c_{11}\, N^4 (\mathrm{Log}\, N)^{\frac{1}{2}} \leq \mathrm{Log}\, |\xi_N| \leq -\frac{1}{c_o}\, N^4\, (\mathrm{Log}\, N)^{\frac{1}{2}} .$$

On considère ensuite l'élément ξ_H , avec

$$H = [\frac{1}{\varepsilon} \,.\, N^2\, t_N^{-1}]$$

où $\varepsilon = \min\{1 \,;\, (\frac{1}{8c_o\, c_{11}})^{\frac{1}{3}}\}$, et $t_N = t(\xi_N)$.

Comme $1 \leq t_N \leq N$, on a

$$\frac{N}{\varepsilon} \leq H \leq \frac{N^2}{\varepsilon} ,$$

et

$$\mathrm{Log}\, |\xi_H| \leq -\frac{1}{c_o} N^4\, (\mathrm{Log}\, N)^{\frac{1}{2}}$$

$$t(\xi_N)\,.\,t(\xi_H) \leq c_{12}\, N^4 .$$

On en déduit que ξ_N et ξ_H ont un résultant nul par rapport à x_2 . Supposons pour simplifier que ξ_N et ξ_H soient des puissances d'un même polynôme irréductible $R \in \mathbb{Z}[x_1, x_2]$:

$$\xi_N = R^{\sigma_N} , \quad \xi_H = R^{\sigma_H} .$$

On a :

$$\frac{-\,\mathrm{Log}\, |\xi_N|}{-\,\mathrm{Log}\, |\xi_H|} = \frac{\sigma_N}{\sigma_H} \geq \frac{1}{4}\, \frac{t(\xi_N)}{t(\xi_H)} ,$$

d'où

$$\frac{c_{11}\, N^4\, (\mathrm{Log}\, N)^{\frac{1}{2}}}{\frac{1}{c_o}\, H^4\, (\mathrm{Log}\, H)^{\frac{1}{2}}} \geq \frac{1}{4}\, \frac{t_N}{H} ,$$

et, par un calcul facile,

$$N \leq \varepsilon^{3/2} . (4.\, c_o .\, c_{11})^{\frac{1}{2}} .\; t_N ,$$

ce qui est impossible avec le choix de ε .

Pour que la démonstration soit complète, il reste à préciser deux points :

- montrer que, dans le deuxième cas, on peut supposer

$$\operatorname{Log} |\xi_N| \geq - c_{11} N^4 (\operatorname{Log} N)^{\frac{1}{2}} ;$$

- considérer le cas où ξ_N et ξ_H ne sont pas puissances d'un même polynôme irréductible.

Ces deux passages sont de caractère technique ; on pourra soit consulter l'article original de Čudnovskij [1], soit appliquer directement les lemmes 2. 8 et 2. 4 de [2].

§. 6. - Compléments

Il est possible de généraliser la démonstration précédente (§. 5) pour démontrer le résultat suivant ([2] théorème 4. 2).

PROPOSITION 6. 1. - Avec les notations de la proposition 1. 1, on suppose $mk \geq m+2$ (autrement dit, $m \geq 2$, $k \geq 2$, ou $m = 1$, $k \geq 3$). Alors il existe une suite $(\varkappa_N)_{N \geq 1}$ d'éléments non nuls de $\mathbb{Z}[x_1, \ldots, x_{q-1}]$, vérifiant :

$$t(\varkappa_N) \leq N$$

et

$$\operatorname{Log} |\varkappa_N| \ll -N^{\frac{(m+2)(k+1)}{2(m+k+2)}} . (\operatorname{Log} N)^{\frac{m+1}{m+k+2}} \quad \text{pour } N \to \infty .$$

On en déduit trivialement le théorème 3. 2, tandis que le critère 3. 4. permet d'en déduire le théorème 5. 1. Quand on utilise le critère 4. 1., (avec $m = k = 30$), on obtient :

$$d \geq 31 \text{ et } \ell \geq \min (d-1, 60) \Rightarrow q_\ell \geq 4 ,$$

Mais Čudnovskij annonce mieux [1] :

$$d \geq 15 \text{ et } \ell \geq \min (d-1, 28) \Rightarrow q_\ell \geq 4 ,$$

et, plus généralement :

$$n \geq 2 , d \geq 2^n - 1 \text{ et } \ell \geq \min(d-1, 2^{n+1} - 4) \Rightarrow q_\ell \geq n ;$$

on en déduit :

$$d \geq 2 \Rightarrow q_{d-1} \geq \frac{\operatorname{Log} (d+1)}{\operatorname{Log} 2} .$$

RÉFÉRENCES

[1] ČUDNOVSKIJ G. V., Algebraic independence of some values of the exponential function ; Mat. Zametki, 15 (1974), 661-672 [trad. angl. : Math. Notes, 15 (1974), 391-398].

[2] WALDSCHMIDT M., Indépendance algébrique par la méthode de G. V. Čudnovskij ; Sém. Delange-Pisot-Poitou, groupe d'étude de théorie des nombres, 16° année (1974-1975), n° G8.

-:-:-:-

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Mathématiques, t 45-46
4, Place Jussieu
75230 PARIS CEDEX 05