Séminaire BOURBAKI Novembre 1996
49ème année, 1996-97, n° 824

SUR LA NATURE ARITHMÉTIQUE DES VALEURS DE FONCTIONS MODULAIRES

par **Michel WALDSCHMIDT**

INTRODUCTION

La fonction modulaire j est définie dans le demi-plan supérieur et prend des valeurs algébriques quand l'argument τ est quadratique. Les nombres quadratiques imaginaires sont les seuls nombres complexes tels que τ et $j(\tau)$ soient simultanément algébriques : cela a été prouvé par Schneider en 1937. La démonstration repose sur une variante elliptique de la méthode qui a permis à Gel'fond et Schneider de résoudre le septième problème de Hilbert.

Soit J la fonction, méromorphe dans le disque unité, définie par $J(e^{2i\pi\tau}) = j(\tau)$. La question, posée par Mahler, de la transcendance de $J(q)$ quand q est un nombre algébrique satisfaisant $0 < |q| < 1$, a été résolue en 1995 par une équipe stéphanoise : Barré-Sirieix, Diaz, Gramain et Philibert. Ces derniers ont résolu en même temps le problème analogue p-adique, qui avait été posé par Manin.

La méthode de démonstration est inspirée de certains travaux de Mahler, et ouvre de nouvelles perspectives. En 1996, Nesterenko a démontré que pour tout nombre complexe q satisfaisant $0 < |q| < 1$, le degré de transcendance sur $\mathbb{Q}$ du corps $\mathbb{Q}\big(q, P(q), Q(q), R(q)\big)$ est au moins égal à 3. Les fonctions P, Q, R (notations de Ramanujan) sont les séries d'Eisenstein de poids 2, 4 et 6 respectivement. On en déduit notamment l'indépendance algébrique des trois nombres π, e^{π} et $\Gamma(1/4)$, ainsi que la transcendance du nombre $\sum_{n\geq 1} 2^{-n^2}$.

1. TRANSCENDANCE

1.1. La fonction modulaire j

La fonction j (encore appelée *invariant modulaire*) est analytique dans le demi-plan supérieur

$$\mathfrak{H} = \{\tau \in \mathbb{C}\,;\, \Im m(\tau) > 0\}$$

et y vérifie

$$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau) \quad \text{pour} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

À une constante additive près, elle est caractérisée par cette propriété avec la normalisation suivante : j a un pôle simple à l'infini de résidu 1. Comme $j(\tau+1) = j(\tau)$, il existe une fonction J, analytique dans le disque unité pointé $\{z \in \mathbb{C}, 0 < |z| < 1\}$, telle que $J(e^{2i\pi\tau}) = j(\tau)$ pour $\tau \in \mathfrak{H}$. Le développement de Laurent de la fonction J à l'origine s'écrit

$$J(z) = \frac{1}{z} + 744 + 196\,884 z + 21\,493\,760 z^2 + 864\,299\,970 z^3 + \cdots + c(n) z^n + \cdots,$$

avec des entiers positifs $c(n)$. Cette série définit aussi, pour tout nombre premier p, une fonction analytique dans le disque unité pointé $\{z \in \mathbb{C}_p ; 0 < |z|_p < 1\}$ du complété $\mathbb{C}_p$ d'une clôture algébrique de $\mathbb{Q}_p$. On désignera dans la suite par $\mathcal{C}$ soit le corps $\mathbb{C}$ des nombres complexes, soit un corps $\mathbb{C}_p$, p premier ; la valeur absolue sur $\mathcal{C}$ sera notée $|\cdot|$.

La fonction modulaire j joue un rôle central dans la théorie de la multiplication complexe concernant l'arithmétique des corps quadratiques imaginaires. Si $\tau \in \mathfrak{H}$ est algébrique de degré 2, alors le nombre $j(\tau)$ est algébrique et le corps de nombres $\mathbb{Q}\big(\tau, j(\tau)\big)$ est le corps de classes de Hilbert du corps quadratique imaginaire $\mathbb{Q}(\tau)$. En 1937, Schneider [4] a montré que, pour τ quadratique, ces nombres $j(\tau)$ ("singular moduli"), sont les seules valeurs algébriques de la fonction j en des points algébriques :

Théorème 1. – *Soit $\tau \in \mathfrak{H}$. Si τ et $j(\tau)$ sont tous deux algébriques, alors τ est quadratique.*

La seule démonstration connue de cet énoncé est celle de Schneider [4] qui utilise les fonctions elliptiques. Supposons que les nombres τ et $j(\tau)$ soient tous deux algébriques. On pose $q = e^{2i\pi\tau}$, $\omega_1 = 2\pi\Delta(q)^{1/12}$ et $\omega_2 = \tau\omega_1$, où $\Delta(q)^{1/12}$ est une quelconque des racines douzièmes du nombre

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Alors la fonction elliptique $\wp$ de Weierstraß, attachée au réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, vérifie une équation différentielle

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3,$$

avec des invariants g_2 et g_3 algébriques. En effet, si on pose

$$G_{2k}(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}} (m+n\tau)^{-2k}, \qquad (k>1),$$

on a

$$g_2 = 60G_4(\tau)/\omega_1^4, \qquad g_3 = 140G_6(\tau)/\omega_1^6,$$
$$g_2^3 - 27g_3^2 = 1 \quad \text{et} \quad 1728g_2^3 = j(\tau).$$

Les fonctions $f_1(z) = \wp(z)$ et $f_2(z) = \wp(\tau z)$ prennent donc simultanément des valeurs algébriques au point $z = \omega_1/2$: le corps $K = \mathbb{Q}\big(g_2, g_3, \tau, \wp(\omega_1/2), \wp(\omega_2/2)\big)$ est un corps de nombres. Schneider utilise les propriétés suivantes :

— les deux fonctions f_1 et f_2 sont méromorphes dans $\mathbb{C}$, chacune étant quotient de deux fonctions entières d'ordre fini ;

— l'anneau $K[f_1, f_2, f_1', f_2']$ est laissé stable par la dérivation d/dz, et pour $i = 1, 2$, la dérivée $f_i' = (d/dz)f_i$ de la fonction f_i est algébrique sur le corps $K(f_i)$;

— les quatre fonctions f_1, f_2, f_1', f_2' prennent simultanément des valeurs dans K en une infinité de points, i.e. les points $z = (m + 1/2)\omega_1$, $(m \in \mathbb{Z})$.

Ces propriétés permettent à Schneider de conclure que les deux fonctions f_1 et f_2 sont algébriquement dépendantes sur K (on déduit maintenant ce fait du *critère de Schneider-Lang* ; cf. [5] et [47]).

Le fait que les deux fonctions $\wp(z)$ et $\wp(\tau z)$ soient algébriquement dépendantes sur $\mathbb{C}$ entraîne que la courbe elliptique associée à $\wp$ possède des endomorphismes non triviaux, donc que τ est quadratique.

Cette démonstration soulève une question, qui a été proposée par Schneider dans la liste des huit problèmes ouverts à la fin de son livre [5], et qui n'est toujours pas résolue :

Deuxième problème de Schneider. – *Démontrer le théorème sur la transcendance des valeurs de la fonction modulaire $j(\tau)$ par une étude directe de cette fonction, et non par l'étude des $\wp$-fonctions.*

Bertrand [31] a remarqué que les résultats de Schneider peuvent aussi s'exprimer en termes de valeurs de fonctions modulaires. Ainsi de la transcendance de ω/π (quand ω est une période non nulle d'une fonction elliptique de Weierstraß d'invariants g_2 et g_3 algébriques) il déduit que pour $q \in \mathbb{C}$ vérifiant $0 < |q| < 1$, l'une au moins des deux

séries d'Eisenstein E_4, E_6 (qui seront définies et étudiées un peu plus loin : § 2.1) prend une valeur transcendante au point q. Si, de plus, $J(q) \notin \{0, 1728\}$, alors il en est de même de l'un au moins des deux nombres $J(q)$ et $qJ'(q)$.

1.2. Le théorème stéphanois sur J

Le théorème suivant [1] répond à une question posée d'abord par Mahler (dans le cas complexe [6], [43]), puis par Manin ([7], §4.12, qui s'intéresse surtout au cas p-adique).

Théorème 2. – *Soit $\alpha \in \mathcal{C}$ un nombre algébrique vérifiant $0 < |\alpha| < 1$. Alors le nombre $J(\alpha)$ est transcendant.*

Dans le cas complexe, le théorème 2 montre qu'un déterminant de la forme

$$\text{dét}\begin{pmatrix} 2i\pi & \log\alpha \\ \omega_1 & \omega_2 \end{pmatrix}$$

(où α est un nombre algébrique non nul, $\log\alpha$ une détermination de son logarithme, et $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ un réseau attaché à des invariants g_2 et g_3 algébriques) ne s'annule pas. Il s'agit d'un des analogues elliptiques (pour trois périodes) du problème bien connu suivant :

Conjecture des quatre exponentielles. – *On considère une matrice*

$$\begin{pmatrix} \log\alpha_1 & \log\alpha_2 \\ \log\alpha_3 & \log\alpha_4 \end{pmatrix}$$

dont les coefficients sont des logarithmes de nombres algébriques. Si les deux lignes sont linéairement indépendantes sur $\mathbb{Q}$, et si les deux colonnes sont aussi linéairement indépendantes sur $\mathbb{Q}$, alors le déterminant ne s'annule pas.

Ce problème a été soulevé notamment par Schneider (c'est le premier problème de [5]) et par Lang [46], [47], ainsi que par Ramachandra [48]. Dans le cas p-adique, il a été proposé par Serre [49]. C'est un cas particulier du problème de l'indépendance algébrique de logarithmes de nombres algébriques (voir à ce sujet la conjecture de Schanuel p. 30 du Chap. III de [47]).

Remarque. Voici trois problèmes ouverts, proposés par Diaz dans [51].
1. Pour tout $z \in \mathbb{C}$ vérifiant $|z| = 1$ et $z \neq \pm 1$, le nombre $e^{2i\pi z}$ est transcendant.
2. Si q est un nombre complexe algébrique satisfaisant $0 < |q| < 1$, tel que $J(q)$ appartienne à l'intervalle réel $[0, 1728]$, alors q est réel.
3. La fonction J est injective sur l'ensemble des nombres algébriques α du domaine $0 < |\alpha| < 1$.

Dans [51], Diaz montre que la troisième conjecture entraîne les deux autres, et qu'elle est elle même conséquence aussi bien de la conjecture des quatre exponentielles que de la conjecture suivante de Bertrand ([36], conjecture 2) :

Conjecture. – *Si α_1 et α_2 sont deux nombres algébriques multiplicativement indépendants dans le domaine $\{z \in \mathcal{C}\,;\, 0 < |z| < 1\}$, alors les deux nombres $J(\alpha_1)$ et $J(\alpha_2)$ sont algébriquement indépendants.*

Cette conjecture contient le cas particulier de la conjecture des quatre exponentielles où deux des α_i sont des racines de l'unité et les deux autres ont un module $\neq 1$.

Un autre analogue elliptique (mixte) du problème des quatre exponentielles intervient à la fin du §4.12 du texte de Manin [7], avec deux périodes au lieu de trois : il s'agit de vérifier $\omega_1/\omega_2 \neq \log \alpha_1 / \log \alpha_2$.

Un analogue en caractéristique finie du théorème 2 a été démontré par Voloch ([83], théorème A ; voir aussi [82]). On peut noter que l'analogue en caractéristique nulle du théorème B de [83], proposé par Bertrand ([50] problème 2), n'est résolu que dans le cas CM ([50] corollaire 3) ; dans le cas général il s'énonce ainsi : quand on paramètre une courbe elliptique sur un corps de nombres par $\mathcal{C}^\times / q^{\mathbb{Z}}$, si $u \in \mathcal{C}^\times$ a pour image un point algébrique d'ordre infini, alors u est transcendant. C'est donc encore un analogue elliptique mixte du problème des quatre exponentielles avec deux périodes : $v/\omega \neq \log \alpha / 2i\pi$, où $u = \exp(2i\pi v/\omega)$.

Le lien entre le théorème stéphanois et les différentes versions du problème des quatre exponentielles suggère de transposer le deuxième problème de Schneider :

Problème. – *Démontrer le théorème 2 dans le cas complexe en utilisant les fonctions elliptiques.*

Un raffinement du théorème 2 est conjecturé par Greenberg. Dans le cas complexe, il s'agit de démontrer la transcendance de $J(q)$ pour $q \in \mathbb{C}$, $0 < |q| < 1$, sous la seule hypothèse que $|q|$ est algébrique. Dans le cas p-adique, on prend un élément q de $\mathbb{C}_p$, algébrique sur $\mathbb{Q}_p$, avec $0 < |q|_p < 1$, dont la norme sur $\mathbb{Q}_p$ est algébrique sur $\mathbb{Q}$; on demande encore de montrer que le nombre $J(q)$ est transcendant (le cas important est celui où la norme de q est une puissance de p).

Du théorème 2 on déduit que si q est un élément de $\mathbb{C}_p$ satisfaisant $0 < |q|_p < 1$ tel que le nombre $J(q)$ soit algébrique, alors q n'appartient pas au noyau du logarithme p-adique d'Iwasawa (ce noyau est composé de nombres algébriques, à savoir les nombres ζp^r avec ζ racine de l'unité et $r \in \mathbb{Q}$). Le fait que $\log_p q$ ne soit pas nul a des conséquences intéressantes [8] car il montre, par exemple, que la période multiplicative $q \in \mathbb{C}_p^\times$ d'une courbe elliptique définie sur $\mathbb{Q}$ à réduction multiplicative en p n'est pas une norme universelle pour la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}_p$. À la suite de travaux de Mazur, Manin en déduit : soit E une courbe elliptique définie sur $\mathbb{Q}$ avec réduction multiplicative en p ; soit K l'extension infinie de $\mathbb{Q}$ obtenue en adjoignant toutes les puissances p-ièmes des racines de l'unité, et soit G le groupe de Galois de K sur $\mathbb{Q}$. Désignons par $S(\mathbb{Q})$ et $S(K)$ les groupes de Selmer de E pour les corps $\mathbb{Q}$ et K respectivement. Alors le noyau et le conoyau de l'application $S(\mathbb{Q}) \to S(K)^G$ sont finis. La même conclusion vaut aussi pour le groupe de Selmer associé au carré symétrique du module de Tate pour la courbe E.

Greenberg a aussi déduit du théorème 2 les deux corollaires suivants :

- Si E est une courbe elliptique modulaire sur $\mathbb{Q}$ avec réduction multiplicative en p et si la fonction $L(E, s)$ ne s'annule pas au point $s = 1$, alors la fonction L p-adique de E a un zéro simple en $s = 1$.
- La fonction L p-adique associée au carré symétrique du module de Tate a un zéro simple en $s = 1$ et $s = 2$.

Le premier corollaire utilise un résultat de Greenberg et Stevens sur la dérivée en $s = 1$ de la fonction L p-adique de E, tandis que le second utilise un résultat de Greenberg et Tilouine sur la non-annulation de la dérivée de la fonction L p-adique du carré symétrique d'une courbe elliptique à réduction multiplicative en p. Ce résultat de Greenberg et Tilouine intervient crucialement dans la démonstration, par Hida, Tilouine et Urban [9], de la conjecture principale pour le groupe de Selmer du carré symétrique d'une courbe elliptique à réduction multiplicative en p.

1.3. Mesures de transcendance et approximation simultanée

Une version quantitative du théorème 1 a été donnée par Faisant et Philibert [52]. Pour énoncer cette estimation, on introduit la *hauteur absolue logarithmique* : si γ est un nombre algébrique de degré d et de polynôme minimal sur $\mathbb{Z}$

$$a_0 z^d + a_1 z^{d-1} + \cdots + a_d = a_0(z - \gamma_1) \cdots (z - \gamma_d),$$

avec $a_0 > 0$, on pose

$$\mathrm{h}(\gamma) = \frac{1}{d}\left(\log a_0 + \sum_{i=1}^{d} \log \max\{1, |\gamma_i|\}\right).$$

Voici l'énoncé principal de [52] : *il existe une constante absolue $C > 0$ telle que, si α et β sont des nombres algébriques vérifiant $\alpha \in \mathfrak{H}$ et $j(\alpha) \neq \beta$, alors*

$$|j(\alpha) - \beta| \geq \exp\left\{-CD^3\left(\log D + \mathrm{h}(\alpha) + \mathrm{h}(\beta)\right)^3\right\},$$

où $D = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}]$.

De même, un analogue quantitatif du théorème 2 a été obtenu par Barré [54], [55] : *soit η un nombre réel, $0 < \eta < 1/2$; il existe une constante $C(\eta) > 0$ telle que, si α et β sont des nombres algébriques vérifiant $\eta \leq |\alpha| \leq 1 - \eta$, alors*

$$|J(\alpha) - \beta| \geq \exp\left\{-C(\eta)\mathrm{d}(\alpha)\mathrm{d}(\beta)^3 A^3 B L^3 (\log L)^4\right\},$$

avec

$$\mathrm{d}(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}], \quad \mathrm{d}(\beta) = [\mathbb{Q}(\beta) : \mathbb{Q}],$$

$$A = \max\{\mathrm{d}(\alpha)\mathrm{h}(\alpha), 1\}, \quad B = \max\{\mathrm{d}(\beta)\mathrm{h}(\beta), \mathrm{d}(\beta)\}$$

et

$$L = \max\left\{e, \log \mathrm{d}(\alpha), \log \mathrm{d}(\beta), \log A, \log B\right\}.$$

1.4. Démonstration du théorème 2.

Le premier outil invoqué dans la démonstration de [1] est une estimation, due à Mahler [44], pour la croissance des coefficients de Laurent de puissances de J.

Soit k un entier ≥ 0. On écrit le développement de Taylor à l'origine de la fonction $\left(zJ(z)\right)^k$ sous la forme

$$\left(zJ(z)\right)^k = \sum_{m=0}^{\infty} c_k(m) z^m.$$

Avec les notations du début de la section 1, les coefficients $c(n)$ du développement de Laurent de J à l'origine sont donnés par $c(n) = c_1(n+1)$, $(n \geq 0)$.

Pour tout $m \geq 0$ et tout $k \geq 0$, $c_k(m)$ est un entier rationnel ≥ 0, et l'estimation donnée par Mahler [44] est

$$c_k(n) \leq 1200 e^{4\sqrt{kn}}.$$

Philibert a noté une inexactitude dans la démonstration de [44], mais il l'a corrigée et peut même remplacer 1200 par 1.

Comme l'a suggéré Bertrand [36], nous remplaçons cette estimation par la suivante, dont la démonstration est plus facile :

Lemme 1. – *Pour N et k entiers rationnels vérifiant $0 \leq k \leq N$ et $N \geq 1$, on écrit le développement de Taylor de $\Delta^{2N} J^k$ à l'origine :*

$$\Delta(z)^{2N} J(z)^k = \sum_{m=1}^{\infty} c_{Nk}(m) z^m.$$

Alors, pour tout $m \geq 1$, le nombre $c_{Nk}(m)$ est un entier rationnel de valeur absolue (usuelle) majorée par

$$|c_{Nk}(m)| \leq C^N m^{12N},$$

où $C > 0$ est une constante absolue.

Démonstration.
Si on compose les fonctions Δ^2 et $\Delta^2 J$ avec $\tau \mapsto e^{2i\pi\tau}$, on obtient des formes modulaires paraboliques de poids 24. On déduit ainsi le résultat pour $N = 1$ d'un théorème de Hecke ([74], théorème 5, §4.3, Chap. VII). Le cas général se démontre par les mêmes arguments (cf. [55], lemme 2).

Le deuxième fait important pour la démonstration du théorème 2 est le suivant : *si q est un élément de $\mathcal{C}$ qui vérifie $0 < |q| < 1$ et tel que $J(q)$ soit algébrique, alors pour tout entier $n \geq 1$ le nombre $J(q^n)$ est encore algébrique.* On peut le voir en supposant $\mathcal{C} = \mathbb{C}$ (ce n'est pas restrictif) et en considérant les deux réseaux isogènes $\mathbb{Z} + \mathbb{Z}\tau$ et $\mathbb{Z} + \mathbb{Z}n\tau$. On a aussi besoin d'estimer le degré et la hauteur de ce nombre algébrique $J(q^n)$. On le fait grâce au lemme suivant, concernant le polynôme modulaire, qui fait intervenir la fonction arithmétique

$$\psi(n) = n \prod_{p|n}\left(1 + \frac{1}{p}\right).$$

Quand A est un polynôme à coefficients dans $\mathbb{Z}$, on note $\mathrm{L}(A)$ (*longueur* de A) la somme des valeurs absolues (usuelles) de ses coefficients.

Lemme 2. – *Il existe une constante absolue $c > 0$ ayant la propriété suivante. Soit n un entier positif. Il existe un polynôme non nul $\Phi_n \in \mathbb{Z}[X,Y]$, symétrique en X et Y, de degré $\psi(n)$ en chaque variable, de longueur $\leq n^{c\psi(n)}$, tel que*

$$\Phi_n\left(J(q), J(q^n)\right) = 0.$$

Mahler avait démontré cette estimation, mais avec une borne légèrement moins précise pour la longueur $\mathrm{L}(\Phi_n)$: sa majoration [44] était $e^{cn^{3/2}}$, avec une constante absolue $c > 0$. Quand n est une puisssance de 2, il avait obtenu une meilleure estimation [43] :

$$\mathrm{L}(\Phi_n) \leq 2^{57n} n^{36n} \qquad \text{si } n = 2^m,$$

et il avait précisé qu'une majoration de la forme

$$\mathrm{L}(\Phi_n) \leq 2^{Cn} \qquad \text{si } n = 2^m,$$

avec une constante absolue $C > 0$, lui permettrait de démontrer le théorème 2 (cf. [43], p. 97). La majoration du lemme 2 est due à Cohen [45] qui montre que son estimation est optimale : elle donne en fait un équivalent asymptotique du logarithme de la longueur de Φ_n, dont elle déduit

$$\limsup_{n\to\infty} \frac{1}{n(\log n)(\log\log n)} \log \mathrm{L}(\Phi_n) = 36\pi^{-2}e^{\gamma},$$

où γ est la constante d'Euler, et

$$\lim_{m\to\infty} \frac{1}{m2^m} \log \mathrm{L}(\Phi_{2^m}) = 9\log 2.$$

On peut noter cependant que, pour la démonstration du théorème 2, la borne $e^{cn^{3/2}}$ de Mahler est suffisante.

Démonstration du théorème 2.

On commence par introduire des paramètres pour que les estimations qui vont suivre soient valides. On choisit deux entiers positifs suffisamment grands L et N. Un choix convenable consiste à prendre pour N un entier suffisamment grand, puis à définir $L = [N^2/2]$.

On montre ensuite l'existence d'un polynôme non nul $A \in \mathbb{Z}[X,Y]$, de degré $\leq N$ par rapport à chaque variable, tel que la fonction analytique $F(z) = \Delta(z)^{2N} A\big(z, J(z)\big)$ ait un zéro à l'origine de multiplicité $\geq L$. L'existence de A est trivialement assurée par la condition $N^2 > L$. Grâce au lemme 1, un lemme de Thue et Siegel (dont la démonstration repose sur le principe des tiroirs) permet, en plus, de majorer la longueur d'un tel polynôme A, grâce à la condition $N^2 \geq 2L$:

$$\mathrm{L}(A) \leq N^{25N}.$$

Les fonctions z et $J(z)$ sont algébriquement indépendantes (cf. [1], lemme 4), donc la fonction F n'est pas identiquement nulle. On désigne par $M = \mathrm{ord}_0 F$ sa multiplicité à l'origine. D'après la construction du polynôme A, on a $M \geq L$.

Soit maintenant $q \in \mathcal{C}$ vérifiant $0 < |q| < 1$. On suppose que N est suffisamment grand par rapport à q. En majorant les coefficients du développement de Taylor à l'origine de la fonction $G(z) = z^{-M}F(z)$, on établit la majoration, pour $|z| \leq |q|$,

$$|F(z)| \leq \begin{cases} |z|^M M^{31N} & \text{si } \mathcal{C} = \mathbb{C}, \\ |z|^M & \text{si } \mathcal{C} = \mathbb{C}_p. \end{cases}$$

Posons $\gamma = 63\big(\log(1/|q|)\big)^{-1}$. On va montrer qu'il existe un entier $S \geq 1$ satisfaisant la majoration $S^2 \leq \gamma N \log M$ tel que $F(q^S) \neq 0$.

Pour cela on désigne par S le plus petit entier tel que $F(q^S) \neq 0$. L'existence de S vient du fait que la fonction F n'est pas identiquement nulle. Afin d'établir la majoration annoncée pour S, on pose $r = (1+|q|)/2$. On définit $|H|_r = \sup_{|z|=r}|H(z)|$ quand $\mathcal{C} = \mathbb{C}$, ou encore quand $\mathcal{C} = \mathbb{C}_p$ et que r est dans le groupe des valeurs. Sinon, $|H|_r$ est la limite de $|H|_\varrho$, pour ϱ dans le groupe des valeurs et tendant vers r. On applique alors le principe du maximum $|H(0)| \leq |H|_r$ à la fonction

$$H(z) = \begin{cases} \dfrac{F(z)}{z^M} \displaystyle\prod_{s=1}^{S-1} \frac{r^2 - z\overline{q}^s}{r(z-q^s)} & \text{si } \mathcal{C} = \mathbb{C}, \\ \dfrac{F(z)}{z^M} \displaystyle\prod_{s=1}^{S-1} \frac{r}{z-q^s} & \text{si } \mathcal{C} = \mathbb{C}_p. \end{cases}$$

D'après ce qui précède, on peut majorer $|H|_r = r^{-M}|F|_r$ par M^{31N} dans le cas complexe, et par 1 dans le cas p-adique. D'un autre côté comme les coefficients de Laurent de J à l'origine sont des entiers rationnels, on a $G(0) = (1/M!)F^{(M)}(0) \in \mathbb{Z}$, donc

$$|H(0)| \geq \begin{cases} r^{S-1}|q|^{-S(S-1)/2} & \text{si } \mathcal{C} = \mathbb{C}, \\ r^{S-1}M^{-25N} & \text{si } \mathcal{C} = \mathbb{C}_p. \end{cases}$$

La majoration annoncée pour S^2 en résulte.

On suppose enfin que notre nombre $q \in \mathcal{C}$, qui satisfait $0 < |q| < 1$, est algébrique, et que $J(q)$ est aussi algébrique. En utilisant le lemme 2, ainsi que des estimations assez fines, on montre l'existence d'une constante $C > 0$, ne dépendant que de q, telle que

$$|F(q^S)| \geq \exp\big\{-CSN(S+\log N)\log\log(3S)\big\}.$$

Mais, grâce à la majoration que nous avons établie pour S, on vérifie que la majoration de $|F(q^S)|$ que nous avons obtenue plus haut, à savoir

$$|F(q^S)| \le \begin{cases} |q|^{MS} M^{31N} & \text{si } \mathcal{C} = \mathbb{C}, \\ |q|^{MS} & \text{si } \mathcal{C} = \mathbb{C}_p \end{cases}$$

n'est pas compatible avec cette minoration. L'hypothèse que q et $J(q)$ sont tous deux algébriques n'est donc pas réalisable.

2. INDÉPENDANCE ALGÉBRIQUE

2.1. Indépendance algébrique de deux nombres

Pour k entier positif on désigne par B_k le k-ième nombre de Bernoulli :

$$\frac{z}{e^z - 1} = 1 - \frac{z}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{z^{2k}}{(2k)!},$$

de sorte que

$$B_1 = 1/6, \quad B_2 = 1/30 \quad \text{et} \quad B_3 = 1/42.$$

On considère la série d'Eisenstein de poids $2k$,

$$E_{2k}(z) = 1 + (-1)^k \frac{4k}{B_k} \sum_{n=1}^{\infty} \frac{n^{2k-1} z^n}{1 - z^n},$$

qui, pour $k > 1$, est le développement de Fourier de la fonction $G_{2k}/\big(2\zeta(2k)\big)$ (voir par exemple [74] Chap. VII, §4). On utilisera aussi les notations de Ramanujan [73] :

$$P(z) = E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \frac{n z^n}{1 - z^n},$$

$$Q(z) = E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 z^n}{1 - z^n},$$

$$R(z) = E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 z^n}{1 - z^n}.$$

Ces fonctions P, Q, R sont reliées aux fonctions J et Δ (introduites plus haut) par

$$\Delta = \frac{1}{1728}\big(Q^3 - R^2\big) \quad \text{et} \quad J = \frac{Q^3}{\Delta}.$$

L'énoncé suivant résulte, dans le cas complexe, des travaux de Chudnovsky [20], [21], [22] sur les périodes de fonctions elliptiques, et, dans le cas ultramétrique, de ceux de Bertrand [32], [33], [34] sur les valeurs de fonctions elliptiques p-adiques de Jacobi-Tate.

Théorème 3. – *Soit q un élément de $\mathcal{C}$ satisfaisant $0 < |q| < 1$. Alors le degré de transcendance sur $\mathbb{Q}$ du corps*

$$\mathbb{Q}\big(P(q), Q(q), R(q)\big)$$

est supérieur ou égal à 2.

Dans le cas complexe, nous allons voir que le théorème 3 s'énonce de manière équivalente sous la forme suivante :

Corollaire 1. – *Soient $\wp$ une fonction elliptique de Weierstraß d'invariants g_2 et g_3, ω une période non nulle de $\wp$ et η la quasi-période correspondante de ζ :*

$$\zeta(z + \omega) = \zeta(z) + \eta.$$

Alors le degré de transcendance sur $\mathbb{Q}$ du corps $\mathbb{Q}(g_2, g_3, \omega/\pi, \eta/\pi)$ est supérieur ou égal à 2.

En particulier, si ω est une période non nulle d'une fonction elliptique d'invariants g_2 et g_3 algébriques attachée à une courbe elliptique de type CM, alors les deux nombres ω et π sont algébriquement indépendants. Comme la période fondamentale réelle de la courbe elliptique $y^2 = 4x^3 - 4x$ est

$$2\int_1^{\infty} \frac{dt}{\sqrt{4t^3 - 4t}} = \frac{1}{2} B(1/4, 1/2) = \frac{\Gamma(1/4)^2}{\sqrt{8\pi}},$$

et que celle de la courbe $y^2 = 4x^3 - 4$ est

$$2\int_1^{\infty} \frac{dt}{\sqrt{4t^3 - 4}} = \frac{1}{3} B(1/6, 1/2) = \frac{\Gamma(1/3)^3}{2^{4/3}\pi},$$

on déduit du corollaire 1 :

Corollaire 2. – *Les deux nombres π et $\Gamma(1/4)$ sont algébriquement indépendants, et il en est de même des deux nombres π et $\Gamma(1/3)$.*

Démonstration du corollaire 1.

Quitte à remplacer la courbe elliptique par une courbe isogène, on peut supposer que le réseau des périodes de $\wp$ est $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ avec $\omega = \omega_1$. En posant $\eta_1 = \eta$, $\tau = \omega_2/\omega_1$ et $q = e^{2i\pi\tau}$, on a (cf. [75], Chap. 4, §2, Prop. 4 et Chap. 18, §3) :

$$P(q) = 3\frac{\omega_1}{\pi} \cdot \frac{\eta_1}{\pi}, \quad Q(q) = \frac{3}{4}\left(\frac{\omega_1}{\pi}\right)^4 g_2, \quad R(q) = \frac{27}{8}\left(\frac{\omega_1}{\pi}\right)^6 g_3.$$

Ces relations montrent que le corollaire 1 équivaut au cas complexe du théorème 3.

Remarque. On a encore

$$\Delta(q) = \left(\frac{\omega_1}{2\pi}\right)^{12} (g_2^3 - 27g_3^2).$$

Les premiers résultats de transcendance de nombres reliés à des intégrales elliptiques sont antérieurs à la solution du septième problème de Hilbert [17]. En 1941, Schneider [18] a obtenu des énoncés généraux sur les périodes de variétés abéliennes dont il déduit des propriétés arithmétiques des valeurs de la fonction Bêta : *pour a et b rationnels non entiers tels que $a+b$ ne soit pas entier, le nombre $B(a,b)$ est transcendant.* Ce résultat se déduit d'un critère de Schneider-Lang en plusieurs variables pour des produits cartésiens [47], Chap. IV.

Une approche entièrement différente a été proposée par André [24], qui utilise les G-fonctions de Siegel pour démontrer l'indépendance algébrique des nombres $\omega_1/2i\pi$ et $\eta_1/2i\pi$, périodes et quasi-périodes attachées à des formes différentielles sur une courbe elliptique $y^2 = (x^2-1)(1-\alpha x^2)$, avec α algébrique, $0 < |\alpha| < 1$. Il écrit ces deux nombres avec des fonctions hypergéométriques sous la forme $iF(1/2, 1/2, 1; \alpha)$ et $iF(-1/2, 1/2, 1; \alpha)$. Ce point de vue vaut aussi bien dans le cas complexe qu'ultramétrique.

Le théorème 3 entraîne que pour $J(q)$ algébrique, les deux nombres $P(q)$ et $\Delta(q)$ sont algébriquement indépendants. Il peut aussi s'exprimer en termes de valeurs des dérivées de la fonction J par rapport à l'opérateur $z(d/dz)$ (voir §2.2).

Selon une conjecture de Lang ([35], p. 652) quand $j'(\tau)$ n'est pas nul, les deux nombres $j(\tau)$ et $j'(\tau)$ ne sont pas simultanément algébriques. L'équation différentielle satisfaite par la fonction j :

$$j'(\tau) = \frac{18}{2i\pi} \cdot \frac{g_3(\tau)}{g_2(\tau)} \cdot j(\tau),$$

(où $g_2(\tau)$, $g_3(\tau)$ désignent les invariants de la fonction de Weierstraß de réseau $\mathbb{Z}+\mathbb{Z}\tau$), ramène cette question à celle de la transcendance de ω^2/π, quand ω est une période non nulle d'une fonction elliptique $\wp$ de Weierstraß d'invariants g_2 et g_3 algébriques. Le théorème de Chudnovsky résout donc le cas de multiplication complexe. Plus précisément [32], pour $\tau \in \mathfrak{H}$ avec $j(\tau)$ algébrique distinct de 0 et 1728, les deux nombres

$$\frac{1}{(2i\pi)^2} j''(\tau) \qquad \text{et} \qquad \frac{1}{2i\pi} j'(\tau)$$

sont algébriquement indépendants. De plus, si τ est quadratique, les deux nombres π et $j'(\tau)$ sont algébriquement indépendants.

Nous utiliserons plus loin une version quantitative du théorème 3, due à Philibert [53]. Un raffinement séparant degré et hauteur a été donné ensuite dans [70]. Une mesure d'indépendance algébrique légèrement plus précise (quand la hauteur est grande comparée au degré) avait été annoncée par Chudnovsky ; la démonstration, esquissée dans [22] Chap. 8, n'est pas convaincante, mais le résultat annoncé a été très récemment démontré par Philippon.

Pour un polynôme A à coefficients complexes, on définit $t(A)$ comme la somme du degré total de A et du logarithme de sa longueur. Voici donc l'énoncé de Philibert :

Proposition 1. – *Sous les hypothèses du théorème 3, si $J(q)$ est algébrique, pour tout $\epsilon > 0$ il existe une constante $C(\epsilon) > 0$ vérifiant la propriété suivante : si $A \in \mathbb{Z}[X,Y]$ est un polynôme non nul, on a*

$$\big|A\big(P(q), \Delta(q)\big)\big| > \exp\{-C(\epsilon)t(A)^{3+\epsilon}\}.$$

Enfin le problème de la transcendance de $\Gamma(1/5)$ n'est toujours pas résolu. À la suite de la conjecture de Rohrlich, selon laquelle $(2\pi)^{-1/2}\Gamma(z)$ *est la distribution impaire universelle à valeurs dans des groupes où la multiplication par 2 est inversible,* Lang (voir [26], Chap. 2, p. 66) pose la question d'indépendance algébrique : il n'y aurait pas de relation de dépendance entre les valeurs de la fonction Γ en des arguments rationnels, autre que celles qui résultent des relations fonctionnelles connues.

2.2. Indépendance algébrique de trois nombres

Voici le résultat principal de [2] et [3] :

Théorème 4. – *Soit q un élément de $\mathcal{C}$ satisfaisant $0 < |q| < 1$. Alors le degré de transcendance sur $\mathbb{Q}$ du corps*

$$\mathbb{Q}\big(q, P(q), Q(q), R(q)\big)$$

est supérieur ou égal à 3.

Mahler a montré dans [41] que les trois fonctions P, Q, R sont algébriquement indépendantes sur le corps $\mathbb{C}(z)$. Elles vérifient d'autre part le système d'équations différentielles [73], [76] :

$$12\frac{DP}{P} = P - \frac{Q}{P}, \qquad 3\frac{DQ}{Q} = P - \frac{R}{Q}, \qquad 2\frac{DR}{R} = P - \frac{Q^2}{R},$$

avec $D = z(d/dz)$. Ainsi la dérivation D laisse stable l'anneau $\mathbb{Q}[P,Q,R]$. On reconnaît là les hypothèses principales du critère de Schneider-Lang, et Serre m'avait suggéré dès 1972 qu'il serait intéressant de développer cette remarque.

On déduit de ces relations

$$\frac{DJ}{J} = -\frac{R}{Q}, \qquad \frac{DJ}{J-1728} = -\frac{Q^2}{R},$$

et

$$6\frac{D^2 J}{DJ} = P - \frac{4R}{Q} - \frac{3Q^2}{R}.$$

Le théorème 4 résout donc une conjecture de Bertrand [32] : *si q est un nombre algébrique vérifiant $0 < |q| < 1$, alors les trois nombres $J(q)$, $DJ(q)$, $D^2J(q)$ sont algébriquement indépendants.* Plus généralement, *si $q \in \mathcal{C}$ vérifie $0 < |q| < 1$, $J(q) \neq 0$ et $J(q) \neq 1728$, alors trois au moins des quatre nombres q, $J(q)$, $DJ(q)$, $D^2J(q)$ sont algébriquement indépendants.*

Du théorème 4 on déduit aussi le corollaire suivant :

Corollaire 1. – *Soit q un nombre complexe vérifiant $0 < |q| < 1$ et tel que $J(q)$ soit algébrique. Alors les trois nombres q, $P(q)$, $\Delta(q)$, sont algébriquement indépendants.*

Le théorème 4 a de nombreuses conséquences : en voici quatre. Les deux premières (qui résultent du corollaire 1) concernent les périodes d'intégrales elliptiques [2], la suivante les fonctions thêta [36], [37], la dernière les suites de Lucas [37].

Corollaire 2. – *Soient $\wp$ une fonction elliptique de Weierstraß d'invariants g_2 et g_3 algébriques, ω une période non nulle de $\wp$, η la quasi-période correspondante de la fonction ζ de Weierstraß attachée à $\wp$ et $\tau \in \mathfrak{H}$ le quotient de deux périodes fondamentales de $\wp$. Alors les trois nombres*

$$e^{2i\pi\tau}, \quad \omega/\pi \quad \text{et} \quad \eta/\pi$$

sont algébriquement indépendants.

Dans le cas CM, en utilisant le fait que les trois nombres ω/π, η/π et $1/\omega$ sont linéairement dépendants sur le corps des nombres algébriques (voir [19], lemme 3.1 et appendice 1), on obtient l'indépendance algébrique des trois nombres

$$e^{2i\pi\tau}, \quad \omega \quad \text{et} \quad \pi.$$

Pour $q = e^{-2\pi}$, on a $J(q) = j(i) = 1728$, tandis que le choix $q = -e^{-\pi\sqrt{3}}$ donne $J(q) = j(\varrho) = 0$ (où ϱ est une racine primitive cubique de l'unité). On déduit du corollaire 2 :

Corollaire 3. – *Les trois nombres*

$$\pi,\ e^{\pi},\ \Gamma(1/4) \qquad \bigl(\textit{resp.}\quad \pi,\ e^{\pi\sqrt{3}},\ \Gamma(1/3)\bigr)$$

sont algébriquement indépendants. En particulier les deux nombres π et e^{π} sont algébriquement indépendants.

L'indépendance algébrique des deux nombres π et e^{π} n'était pas connue. On obtient plus généralement, quand D est un entier rationnel > 0, l'indépendance algébrique des trois nombres π, $e^{\pi\sqrt{D}}$ et ω, où ω est une période non nulle d'une courbe elliptique, définie sur le corps des nombres algébriques, dont l'anneau des endomorphismes est un ordre du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-D})$.

On déduit du corollaire 3 que le produit canonique de Weierstraß associé au réseau $\mathbb{Z} + \mathbb{Z}i$,

$$\sigma(z) = z \prod_{\substack{\omega \in \mathbb{Z}+\mathbb{Z}i \\ \omega \neq 0}} (1 - z/\omega) e^{(z/\omega)+(z^2/2\omega^2)},$$

prend des valeurs transcendantes aux points de $\mathbb{Q} + \mathbb{Q}i$ qui ne sont pas dans $\mathbb{Z} + \mathbb{Z}i$; par exemple le nombre

$$\sigma(1/2) = 2^{5/4}\pi^{1/2}e^{\pi/8}\Gamma(1/4)^{-2}$$

est transcendant.

L'indépendance algébrique de π et e^{π} montre aussi que le nombre

$$\sum_{n=2}^{\infty}(n^4-1)^{-1} = \frac{7}{8} - \frac{\pi}{4}\coth\pi$$

est transcendant [40].

Le corollaire suivant fait intervenir les séries thêta de Jacobi (voir par exemple [77], Chap. V, §6, Th.6) :

$$\theta_2(z) = 2z^{1/4}\sum_{n\geq 0} z^{n(n+1)} = 2z^{1/4}\prod_{n=1}^{\infty}(1-z^{4n})(1+z^{2n}),$$

$$\theta_3(z) = \sum_{n\in\mathbb{Z}} z^{n^2} = \prod_{n=1}^{\infty}(1-z^{2n})(1+z^{2n-1})^2,$$

$$\theta_4(z) = \theta_3(-z) = \sum_{n\in\mathbb{Z}}(-1)^n z^{n^2} = \prod_{n=1}^{\infty}(1-z^{2n})(1-z^{2n-1})^2.$$

On peut formuler le théorème 4 de la façon suivante :

Corollaire 4. – *Soient i, j et k trois indices $\in \{2,3,4\}$ avec $i \neq j$. Soit q un nombre complexe, $0 < |q| < 1$. Alors chacun des deux corps*

$$\mathbb{Q}\big(q, \theta_i(q), \theta_j(q), D\theta_k(q)\big) \quad et \quad \mathbb{Q}\big(q, \theta_k(q), D\theta_k(q), D^2\theta_k(q)\big)$$

a un degré de transcendance ≥ 3 sur $\mathbb{Q}$.

Ainsi, pour $q \in \mathbb{C}$ algébrique, $0 < |q| < 1$, le nombre $\theta_3(q)$ est transcendant. Le problème de la transcendance du nombre $\sum_{n\geq 0} \ell^{-n^2}$, quand ℓ est un entier rationnel > 1, était ouvert depuis que Liouville ([38] p. 140) avait remarqué que, pour ces nombres, l'argument lui ayant permis d'expliciter les premiers exemples de nombres transcendants donnait seulement un résultat d'irrationalité.

Démonstration du corollaire 4.
Les relations suivantes (cf. [36])

$$\begin{aligned}\theta_3^4 &= \theta_2^4 + \theta_4^4,\\ Q(z^2) &= 2^{-1}\big(\theta_2(z)^8 + \theta_3(z)^8 + \theta_4(z)^8\big),\\ \Delta(z^2) &= 2^{-8}\big(\theta_2(z)\theta_3(z)\theta_4(z)\big)^8\end{aligned}$$

et

$$\begin{aligned}\theta_2^4 &= 4(D\theta_3/\theta_3 - D\theta_4/\theta_4),\\ \theta_4^4 &= 4(D\theta_2/\theta_2 - D\theta_3/\theta_3),\\ P(z^2) &= 4\big(D\theta_2/\theta_2 + D\theta_3/\theta_3 + D\theta_4/\theta_4)(z),\end{aligned}$$

montrent que les deux corps

$$\mathbb{Q}\big(q^2, P(q^2), Q(q^2), R(q^2)\big) \quad \text{et} \quad \mathbb{Q}\big(q, \theta_i(q), \theta_j(q), D\theta_k(q)\big)$$

ont la même clôture algébrique. Ceci démontre la première partie du corollaire 4, tandis que la seconde, disons dans le cas $k = 3$, se déduit de la relation (cf. [36])

$$D^2\theta_3/\theta_3 - 3(D\theta_3/\theta_3)^2 = 2^{-3}\theta_2^4\theta_4^4.$$

Dans le cas particulier où q est algébrique, une démonstration différente de l'indépendance algébrique des trois nombres $y(q), Dy(q), D^2y(q)$ (où y est l'une des trois fonctions thêta) est proposée dans [37] ; elle repose sur un argument de spécialisation de Weil, combiné avec le fait que les trois fonctions y, Dy, D^2y sont algébriquement indépendantes [42].

Le dernier corollaire concerne les suites de Lucas.

Corollaire 5. – *Soit α un nombre complexe algébrique vérifiant $0 < |\alpha| < 1$. Soit $\beta = \pm 1/\alpha$. On pose, pour $n \geq 1$,*

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Alors le nombre

$$\sum_{n=1}^{\infty} \frac{1}{U_n^2}$$

est transcendant.

En choisissant $\alpha = (1-\sqrt{5})/2$ et $\beta = -1/\alpha$, la suite $(U_n)_{n\geq 0}$ ainsi obtenue est la suite de Fibonacci :

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad (n \geq 2),$$

et on obtient la transcendance de la somme de la série

$$\sum_{n=1}^{\infty} \frac{1}{F_n^2}.$$

Il est intéressant de noter (cf. [37]) que certaines séries analogues ont pour sommes des nombres algébriques, quelquefois même rationnels :

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{F_nF_{n+1}} = \frac{1-\sqrt{5}}{2}, \qquad \sum_{n=1}^{\infty} \frac{1}{F_nF_{n+2}} = 1.$$

Démonstration du corollaire 5.
On se contente de traiter le cas $\beta = 1/\alpha$. La dérivée logarithmique de la fonction Δ pour l'opérateur $D = z(d/dz)$ est

$$\frac{D\Delta(z)}{\Delta(z)} = 1 - 24\sum_{n=1}^{\infty} \frac{nz^n}{1-z^n} = 1 - 24\sum_{n=1}^{\infty} \frac{z^n}{(1-z^n)^2}.$$

En posant $z = \alpha^2$, on trouve

$$\frac{D\Delta(\alpha^2)}{\Delta(\alpha^2)} = 1 - \frac{24}{(\beta-\alpha)^2}\sum_{n=1}^{\infty} \frac{1}{U_n^2}.$$

2.3. Mesures d'indépendance algébrique

Nesterenko [2], [3] et Philippon [56] ont établi des raffinements quantitatifs du théorème 4. Dans l'exemple qui suit, tiré de [56], on utilise la même notation $t(A)$ que dans la proposition 1 (pour désigner la somme $\deg A + \log \mathrm{L}(A)$ du degré total de A et du logarithme de la longueur de A) ; mais on pourrait aussi séparer degré et hauteur.

Soit $q \in \mathcal{C}$ satisfaisant $0 < |q| < 1$, tel que le corps

$$\mathbb{Q}\big(q, P(q), Q(q), R(q)\big)$$

ait un degré de transcendance égal à 3 sur $\mathbb{Q}$. Choisissons une base de transcendance $(\theta_1, \theta_2, \theta_3)$. Il existe alors une constante $\gamma > 0$, dépendant de q, $\theta_1, \theta_2, \theta_3$ (et de p quand $\mathcal{C} = \mathbb{C}_p$), telle que, pour tout polynôme non nul $A \in \mathbb{Z}[X_1, X_2, X_3]$ on ait

$$|A(\theta_1, \theta_2, \theta_3)| > \exp\{-\gamma T^4 (\log T)^{16}\},$$

avec $T = \max\{e, t(A)\}$.

Cette estimation s'applique en particulier aux triplets

$$\big(\pi, e^{\pi}, \Gamma(1/4)\big) \qquad \text{et} \qquad \big(\pi, e^{\pi\sqrt{3}}, \Gamma(1/3)\big),$$

fournissant ainsi des mesures d'indépendance algébriques très précises (l'exposant 4 pour T est optimal).

Les résultats quantitatifs de [56] sont plus généraux : ils concernent des idéaux de polynômes de différentes codimensions. Par exemple Philippon donne aussi des mesures d'approximations simultanées des nombres q, $P(q)$, $Q(q)$ et $R(q)$ par des nombres algébriques.

Malgré ces progrès on ne sait pas encore montrer que le nombre e^{π} n'est pas un nombre de Liouville.

2.4. Démonstration directe du corollaire 1 du théorème 4.

La démonstration que nous allons donner du corollaire 1 est inspirée par le travail de Philippon [56]. Elle est nettement plus simple que celle de [2], et utilise la mesure d'indépendance algébrique due à Philibert (proposition 1 ci-dessus - voir [53]).

Le but de l'argument transcendant est d'établir le résultat suivant :

Proposition 2. – *Soit $q \in \mathcal{C}$, $0 < |q| < 1$. Il existe deux constantes positives c et κ, (dépendant de $|q|$), ayant la propriété suivante : pour tout entier N suffisamment*

grand, il existe un entier $M \geq N^4$ et un polynôme non nul $A_N \in \mathbb{Z}[z, X_1, X_2, X_3]$ tel que

$$\deg A_N \leq cN \log M, \qquad \log H(A_N) \leq cN(\log M)^2,$$

et

$$0 < \big|A_N\big(q, P(q), Q(q), R(q)\big)\big| \leq e^{-\kappa M}.$$

Démonstration.

On désigne par N un entier suffisamment grand, et on pose $L = [N^4/2]$. Il existe un polynôme non nul $A \in \mathbb{Z}[z, X_1, X_2, X_3]$, de degré $\leq N$ par rapport à chacune des quatre variables, tel que la fonction $F(z) = A\big(z, P(z), Q(z), R(z)\big)$ ait, à l'origine, un zéro de multiplicité $\geq L$. Le lemme de Thue-Siegel montre l'existence d'un tel polynôme dont la longueur est majorée par :

$$\mathrm{L}(A) \leq N^{85N}.$$

Soit $M = \mathrm{ord}_0 F$ l'ordre de F en $z = 0$. La construction de A donne $M \geq L$. Un point essentiel de la démonstration de Nesterenko consiste à établir l'inégalité $M \leq C_0 L$, où C_0 est une constante absolue. Cette majoration ("lemme de multiplicités" ou "lemme de zéros") est décrite dans la section suivante (théorème 5). Dans cette démonstration, nous ne l'utiliserons pas.

On pose $r = \min\{(1 + |q|)/2, 2|q|\}$ et on suppose N suffisamment grand par rapport à q. La fonction F a un zéro de multiplicité M à l'origine. En majorant les coefficients de Taylor de la fonction $G(z) = z^{-M} F(z)$ à l'origine, on obtient, pour $|z| \leq r$ (cf. [2] lemme 2.2)

$$|F(z)| \leq \begin{cases} |z|^M M^{48N} & \text{si } \mathcal{C} = \mathbb{C}, \\ |z|^M & \text{si } \mathcal{C} = \mathbb{C}_p. \end{cases}$$

L'étape suivante consiste à montrer que le nombre $T = \mathrm{ord}_q F$ est majoré par $T \leq \gamma N \log M$, avec $\gamma = 48\big(\log(r/|q|)\big)^{-1}$. Pour cela on applique le principe du maximum $|H(0)| \leq |H|_r$ à la fonction

$$H(z) = \begin{cases} \dfrac{F(z)}{z^M} \cdot \left(\dfrac{r^2 - \overline{q}z}{r(z-q)}\right)^T & \text{si } \mathcal{C} = \mathbb{C}, \\[2ex] \dfrac{F(z)}{z^M} \cdot \left(\dfrac{r}{z-q}\right)^T & \text{si } \mathcal{C} = \mathbb{C}_p. \end{cases}$$

Le nombre $G(0) = (1/M!)F^{(M)}(0)$ est entier et n'est pas nul. On minore sa valeur absolue par 1 dans le cas complexe, et on minore sa valeur absolue p-adique en majorant sa valeur absolue ordinaire quand $\mathcal{C} = \mathbb{C}_p$. On trouve

$$|H(0)| \geq \begin{cases} (r/|q|)^T & \text{si } \mathcal{C} = \mathbb{C}, \\ M^{-17N}(r/|q|)^T & \text{si } \mathcal{C} = \mathbb{C}_p. \end{cases}$$

La majoration de $|H|_r = r^{-M}|F|_r$ par M^{48N} dans le cas complexe et par 1 dans le cas p-adique fournit l'estimation annoncée pour T.

On introduit l'opérateur de dérivation

$$D = z\frac{d}{dz} + \frac{1}{12}(X_1^2 - X_2)\frac{\partial}{\partial X_1} + \frac{1}{3}(X_1X_2 - X_3)\frac{\partial}{\partial X_2} + \frac{1}{2}(X_1X_3 - X_2^2)\frac{\partial}{\partial X_3}$$

sur l'anneau $\mathcal{C}[z, X_1, X_2, X_3]$, de telle sorte que

$$z\frac{d}{dz}F(z) = (DA)\big(z, P(z), Q(z), R(z)\big).$$

On pose

$$A_N(z, X_1, X_2, X_3) = (12z)^T(z^{-1}D)^T A(z, X_1, X_2, X_3).$$

On vérifie

$$\deg A_N \leq 4N + T \leq (\gamma+1)N\log M,$$

$$\mathrm{L}(A_N) \leq N^{85N}5^{4N}(48N + 24T)^T \leq \exp\{2\gamma N(\log M)^2\},$$

et

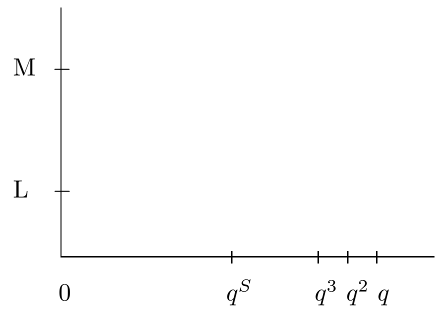
$$|A_N\big(q, P(q), Q(q), R(q)\big)| \leq 12^T T!(r - |q|)^{-T} r^M M^{48N} \leq e^{-\kappa M}.$$

Ceci termine la démonstration de la proposition 2.

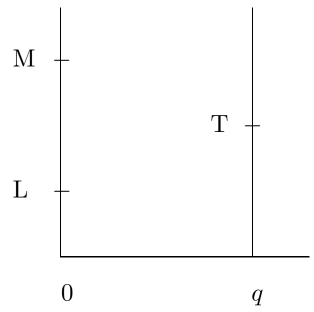
Pour déduire le corollaire 1 des propositions 1 et 2, on suppose $q \in \mathbb{C}$, $0 < |q| < 1$, $J(q)$ algébrique, et les trois nombres q, $P(q)$, $\Delta(q)$ algébriquement dépendants. Alors chacun des quatre nombres q, $P(q)$, $Q(q)$, $R(q)$ est racine d'un polynôme $f_i(X_i, \omega/\pi, \eta/\pi)$, $(i = 0, 1, 2, 3)$, avec $f_i \in \mathbb{Z}[X_i, Y_1, Y_2]$. On élimine, dans l'anneau de polynômes en 6 variables $\mathbb{Z}[X_0, X_1, X_2, X_3, Y_1, Y_2]$, les 4 variables X_0, X_1, X_2, X_3 entre les 5 polynômes A, f_0, f_1, f_2, f_3. On voit ainsi que les estimations données par les propositions 1 et 2 ne sont pas compatibles.

Les deux démonstrations que nous venons de présenter (théorème 2 et proposition 2) sont schématisées par les deux diagrammes suivants : on construit à chaque fois une

fonction auxiliaire ayant un zéro de multiplicité au moins L en l'origine, on désigne par M cette multiplicité, et on considère soit une valeur non nulle $F(q^S)$ de F en un point (q^S figure sur l'axe horizontal), soit une dérivée $F^{(T)}(q) \neq 0$ de F au point q (l'ordre de dérivation T est porté sur un axe vertical).



Théorème 2



Proposition 2

Les structures de démonstrations sont donc semblables ; les Stéphanois ne pouvaient pas utiliser les dérivées de la fonction auxiliaire au point q car l'équation différentielle satisfaite par la fonction J est d'ordre 3.

Ce type de démonstration (avec construction d'une fonction auxiliaire, recherche d'une valeur non nulle, majoration et minoration) est essentiellement la seule méthode dont on dispose actuellement. C'est Hermite en 1873 qui a introduit le premier ce type d'argument pour démontrer la transcendance de e, suivi par Siegel en 1929 (qui introduit les E- et G-fonctions), puis Mahler en 1930 [10], suivi de Gel'fond et Schneider qui résolvent le septième problème de Hilbert en 1934. L'utilisation du principe des tiroirs pour la construction de la fonction auxiliaire, qui était une des caractéristiques de toutes ces méthodes, peut être évitée, comme l'a montré Laurent ; une démonstration des théorèmes 2 et 4 à l'aide de déterminants d'interpolation de Laurent se trouve dans [57].

L'utilisation d'une mesure de transcendance pour établir un résultat d'indépendance algébrique avait été suggérée par Lang ([47], Chap. VI, historical note), comme premier pas d'un processus inductif. La “rigidité absolument fantastique” dont il est question dans cette note historique n'est plus ce qu'elle était.

2.5. Démonstration du théorème 4.

La démonstration de Nesterenko diffère de la précédente, car elle utilise, comme nous l'avons dit, une majoration de M/L. Une autre différence apparaît dans le choix de T : au lieu de définir T comme l'ordre en q de la fonction F, il montre dans [2] qu'il existe un entier T dans l'intervalle $0 \le T \le \gamma N \log N$ tel que

$$|D^T F(q)| \ge \left(\frac{1}{2}|q|\right)^{2M}.$$

L'existence de cet entier T repose sur une formule d'interpolation (c'est ce que Philippon appelle un "lemme de Schwarz approché" ; cf.[57]) que nous énonçons dans le cas complexe.

Lemme 3. – *Soient M et T deux entiers ≥ 0, r un nombre réel et q un nombre complexe vérifiant $0 < |q| \le r$. Soit F une fonction analytique dans un ouvert contenant le disque $|z| \le r$ du plan complexe, ayant un zéro de multiplicité $\ge M$ à l'origine. Alors*

$$\frac{r^M}{M!}|F^{(M)}(0)| \le \left(\frac{r}{|q|}\right)^{-T}|F|_r + 2^{M+T}\left(\frac{r}{|q|}\right)^M \cdot \sum_{t=0}^{T-1}\left(\frac{|q|}{2}\right)^t \frac{1}{t!}|F^{(t)}(q)|.$$

On obtient ainsi l'énoncé suivant, plus précis que la proposition 2 :

Proposition 3. – *Soit $q \in \mathcal{C}$, $0 < |q| < 1$. Il existe des constantes c, κ_1 et κ_2 positives (dépendant de $|q|$) et il existe une suite $(A_N)_{N\ge 2}$ de polynômes non nuls de l'anneau $\mathbb{Z}[z, X_1, X_2, X_3]$, vérifiant, pour tout $N \ge 2$,*

$$\deg A_N \le cN \log N, \qquad \log H(A_N) \le cN(\log N)^2,$$

et

$$\exp\{-\kappa_2 N^4\} \le \left|A_N\big(q, P(q), Q(q), R(q)\big)\right| \le \exp\{-\kappa_1 N^4\}.$$

Le lemme 2.4 de [2] explicite les constantes c, κ_1 et κ_2 en fonction de $|q|$ dans le cas $\mathcal{C} = \mathbb{C}$: en gardant la notation $r = \min\{(1+|q|)/2, 2|q|\}$, on peut prendre

$$c = 380\big(\log(r/|q|)\big)^{-1}, \quad \kappa_1 = (1/4)\log(1/r), \quad \kappa_2 = 6 \cdot 10^{45}\log(2/|q|).$$

Enfin, pour déduire le théorème 4 de la proposition 3, il ne reste plus qu'à utiliser le critère d'indépendance algébrique de Philippon [69] :

Proposition 4. – *Soient $\theta_1, \ldots, \theta_n$ des éléments de $\mathcal{C}$, t un entier ≥ 0, σ, λ, R des fonctions croisssantes de $\mathbb{N}$ dans $\mathbb{R}$, non bornées, telles que λ/σ^t soit croissante et*

$$\liminf_{N\to\infty} \lambda(N)/R(N+1) > 0, \qquad \liminf_{N\to\infty} \lambda(N)/\sigma(N+1)^t = \infty.$$

On suppose qu'il existe une suite $(A_N)_{N\ge 0}$ de polynômes non nuls de $\mathbb{Z}[X_1, \ldots, X_n]$ vérifiant, pour tout N suffisamment grand,

$$\deg A_N \le \sigma(N), \qquad \log H(A_N) \le \sigma(N),$$

et

$$|A_N(\theta_1, \ldots, \theta_n)| \le e^{-\lambda(N)}.$$

On suppose de plus que A_N ne s'annule pas dans la boule $\max_{1\le i\le n}|z_i - \theta_i| \le e^{-R(N)}$ de $\mathcal{C}^n$. Alors le corps $\mathbb{Q}(\theta_1, \ldots, \theta_n)$ a un degré de transcendance $\ge t$ sur $\mathbb{Q}$.

Dans la situation de la proposition 3, on applique ce critère avec $n = 4$, $t = 1$, $\lambda(N) = \kappa_1 N^4$, $R(N) = 2\kappa_2 N^4$, $\sigma(N) = cN(\log N)^2$. La minoration de $|A_N(\theta_1, \ldots, \theta_n)|$ garantit que A_N ne s'annule pas dans un voisinage convenable du point $(\theta_1, \ldots, \theta_n)$.

Remarque. Les démonstrations des estimations diophantiennes de Nesterenko raffinant le théorème 4 de façon quantitative reposent encore sur la proposition 3, mais la proposition 4 est remplacée par le critère d'Ably [71]. Les estimations de [56] demandent un peu plus de travail car degré et hauteur sont séparés (Philippon utilise les critères de Jabbouri [70] et Jadot [72]).

3. LEMMES DE ZÉROS

3.1. Énoncés

Un des points importants de la démonstration de Nesterenko était la majoration de la multiplicité en l'origine de la fonction auxiliaire F. Il établit pour cela le résultat suivant [2], Théorème 3 :

Théorème 5. – *Soient L_0 et L des entiers positifs, $A \in \mathcal{C}[z, X_1, X_2, X_3]$ un polynôme non nul, de degré $\le L_0$ en z et $\le L$ en chacune des trois autres variables X_1, X_2, X_3. Alors la multiplicité du zéro à l'origine de la fonction analytique*

$$A\big(z, P(z), Q(z), R(z)\big)$$

est majorée par cL_0L^3, avec $c = 2 \cdot 10^{45}$.

Ce théorème 5 est un exemple de *lemmes de zéros* que Nesterenko a établis pendant ces 20 dernières années [59], [60], [65], [66], [67].

La démonstration, qui repose sur des arguments d'algèbre commutative, se fait par récurrence sur le rang d'un idéal. Pour cela il est nécessaire d'établir un énoncé plus général : on ne se contente pas de majorer la multiplicité en l'origine d'une fonction $A\big(z,P(z),Q(z),R(z)\big)$, mais on considère un idéal homogène $\mathfrak{I}$ de l'anneau de polynômes $\mathcal{R}[X_0,X_1,X_2,X_3]$, où $\mathcal{R}=\mathcal{C}[z]$. Pour un tel idéal on va définir, à l'aide des formes de Chow, des quantités $B(\mathfrak{I})$, $N(\mathfrak{I})$ et $\mathrm{ord}\mathfrak{I}(\overline{f})$, qui satisferont la condition suivante : si $\mathfrak{I}$ est l'idéal principal engendré par un polynôme homogène ${}^hA(X_0,X_1,X_2,X_3)=X_0^{\deg A}A(X_1/X_0,X_2/X_0,X_3/X_0)$, alors

$$B(\mathfrak{I})=\deg_z A,\quad N(\mathfrak{I})=\deg A\quad \text{et}\quad \mathrm{ord}\mathfrak{I}(\overline{f})\geq \mathrm{ord}_0 A\big(z,P(z),Q(z),R(z)\big).$$

L'énoncé suivant contiendra donc le théorème 5 (qui correspond au cas particulier $r=3$).

Théorème 6. – *Soit $\mathfrak{I}$ un idéal homogène dans l'anneau $\mathcal{R}[X_0,X_1,X_2,X_3]$, pur de rang $4-r$ avec $r\in\{1,2,3\}$. Alors*

$$\mathrm{ord}\mathfrak{I}(\overline{f})\leq \varrho^{2r-1}\big(B(\mathfrak{I})N(\mathfrak{I})^{r/(4-r)}+N(\mathfrak{I})^{3/(4-r)}\big),$$

avec $\varrho=10^9$.

3.2. Formes de Chow

Voici la définition de $B(\mathfrak{I})$, $N(\mathfrak{I})$ et $\mathrm{ord}\mathfrak{I}(\overline{f})$.

On désigne toujours par $\mathcal{R}$ l'anneau $\mathcal{C}[z]$. Soient m un entier positif et $\mathfrak{I}$ un idéal homogène de $\mathcal{R}[X_0,\dots,X_m]$, pur de rang $m+1-r\geq 1$. On introduit r formes linéaires “génériques” $L_i(X)=\sum_{j=0}^m U_{ij}X_j$, $(1\leq i\leq r)$, ce qui signifie que U_{ij}, $(1\leq i\leq r$, $1\leq j\leq m)$ sont des variables indépendantes. L'*idéal U-éliminant* $\overline{\mathfrak{I}}$ de $\mathfrak{I}$ est l'idéal de l'anneau des polynômes à coefficients dans $\mathcal{R}$ en les $r(m+1)$ variables U_{ij} formé des G pour lesquels il existe un entier $M\geq 1$ vérifiant

$$GX_i^M\in(\mathfrak{I},L_1,\dots,L_r)\quad \text{pour } 0\leq i\leq m.$$

Grâce au choix de r, l'idéal $\overline{\mathfrak{I}}$ est principal et non nul. Une *forme de Chow* de $\mathfrak{I}$ est un générateur $F_{\mathfrak{I}}$ de $\overline{\mathfrak{I}}$. Si on pose $\underline{U}_i=(U_{0i},\dots,U_{mi})$, ce polynôme $F_{\mathfrak{I}}$ est symétrique en $\underline{U}_1,\dots,\underline{U}_r$, et son degré en $\underline{U}_1$ est noté $N(\mathfrak{I})$. Le degré de $F_{\mathfrak{I}}$ en z est noté $B(\mathfrak{I})$.

Soient $f_0,\dots,f_m$ des séries formelles en z à coefficients complexes vérifiant $\min_{0\leq i\leq m}\mathrm{ord}_0 f_i=0$. On note $\overline{f}\in\big(\mathcal{C}[[z]]\big)^{m+1}$ le vecteur colonne de composantes $(f_0,\dots,f_m)$. Pour définir $\mathrm{ord}\mathfrak{I}(\overline{f})$, on introduit encore r matrices antisymétriques “génériques” $S^{(1)},\dots,$ $S^{(r)}$, avec $S^{(i)}=\big(S^{(i)}_{kj}\big)_{0\leq k,j\leq m}$, ce qui veut dire que $S^{(i)}_{kj}$,

$(1\leq i\leq r,\ 0\leq k,j\leq m)$ sont de nouvelles variables, liées par les seules relations $S^{(i)}_{kj}+S^{(i)}_{jk}=0$. Quand $F_{\mathfrak{I}}$ est une forme de Chow de $\mathfrak{I}$, on définit une série formelle

$$\mathfrak{S}(F_{\mathfrak{I}})=F_{\mathfrak{I}}\big(S^{(1)}\overline{f},\dots,S^{(r)}\overline{f}\big),$$

et on pose

$$\mathrm{ord}\mathfrak{I}(\overline{f})=\mathrm{ord}_0\mathfrak{S}(F_{\mathfrak{I}}).$$

Dans la suite, on utilisera ces définitions avec $m=3$ et $\overline{f}=\big(1,P,Q,R\big)$.

Quand $\mathfrak{p}$ est un idéal premier homogène de $\mathcal{R}[X_0,\dots,X_m]$ de rang $m+1-r$ tel que $\mathfrak{p}\cap\mathcal{R}=\{0\}$, on montre qu'il existe un polynôme homogène non nul dans $\mathfrak{p}$, de degré (en les variables $X_0,\dots,X_m$) majoré par $1+c(m)N(\mathfrak{p})^{1/(m-r+1)}$, et de degré en z majoré par $c(m)B(\mathfrak{p})N(\mathfrak{p})^{-(m-r)/(m-r+1)}$ (avec une constante explicite $c(m)>0$ ne dépendant que de m). Si, de plus, $X_0\notin\mathfrak{p}$, et si $Q\in\mathcal{R}[X_0,\dots,X_m]$ est un polynôme homogène qui n'appartient pas à $\mathfrak{p}$, alors l'idéal $\mathfrak{I}=(\mathfrak{p},Q)$ vérifie

$$B(\mathfrak{I})\leq B(\mathfrak{p})\deg_X Q+N(\mathfrak{p})\deg_z Q,\qquad N(\mathfrak{I})\leq N(\mathfrak{p})\deg_X Q.$$

De plus on peut aussi minorer $\mathrm{ord}\mathfrak{I}(\overline{f})$ en fonction de $\mathrm{ord}\mathfrak{p}(\overline{f})$, $B(\mathfrak{p})$, $N(\mathfrak{p})$, $\deg_X Q$ et $\deg_z Q$.

L'opérateur D introduit plus haut doit être rendu homogène. Comme l'a remarqué Gaudron, il convient de poser

$$\mathfrak{D}=zX_0\frac{d}{dz}+\frac{1}{12}(X_1^2-X_0X_2)\frac{\partial}{\partial X_1}+\frac{1}{3}(X_1X_2-X_0X_3)\frac{\partial}{\partial X_2}+\frac{1}{2}(X_1X_3-X_2^2)\frac{\partial}{\partial X_3}.$$

3.3. Indications sur la démonstration du théorème 6.

Il n'y a pas de restriction à supposer $\mathfrak{I}\cap\mathcal{R}=\{0\}$. On procède par récurrence sur r. On commence par se ramener au cas où l'idéal $\mathfrak{I}$ est premier de la façon suivante : on considère une décomposition primaire réduite $\mathfrak{I}=\mathfrak{Q}_1\cap\dots\cap\mathfrak{Q}_t$ de $\mathfrak{I}$, où $\mathfrak{Q}_1,\dots,\mathfrak{Q}_t$ sont ordonnés de telle sorte que

$$\mathfrak{Q}_i\cap\mathcal{R}=\{0\},\quad (1\leq i\leq s),\qquad \mathfrak{Q}_{s+1}\cap\dots\cap\mathfrak{Q}_t\cap\mathcal{R}=(\gamma),$$

avec $\gamma\in\mathcal{R}$, $\gamma\neq 0$. Soient $\mathfrak{P}_1,\dots,\mathfrak{P}_t$ les idéaux premiers associés à $\mathfrak{I}$ et $e_1,\dots,e_t$

leurs exposants. On a (cf. [65] ou [66])

$$B(\mathfrak{I}) = \deg_z \gamma + \sum_{i=1}^{s} e_i B(\mathfrak{P}_i),$$

$$N(\mathfrak{I}) = \sum_{i=1}^{s} e_i N(\mathfrak{P}_i),$$

$$\mathrm{ord}\mathfrak{I}(\overline{f}) = \mathrm{ord}_0\gamma + \sum_{i=1}^{s} e_i \mathrm{ord}\mathfrak{P}_i(\overline{f}).$$

On part d'un idéal premier homogène $\mathfrak{P}$. Si on peut construire un idéal de la forme $(\mathfrak{P}, Q)$, avec $Q = \mathfrak{D}P$, $P \in \mathfrak{P}$ et $Q \notin \mathfrak{P}$, dont le rang est strictement inférieur au rang de $\mathfrak{P}$, alors on peut utiliser l'hypothèse de récurrence. Sinon, on montre qu'il existe un idéal premier $\mathfrak{p}$, contenu dans $\mathfrak{P}$, qui est stable par $\mathfrak{D}$. Le point essentiel de la démonstration consiste à déterminer ces idéaux stables. C'est le “lemme de stabilité” suivant :

Lemme 4. — *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{C}[z, X_0, X_1, X_2, X_3]$, homogène dans $\mathcal{R}[X_0, X_1, X_2, X_3]$, qui s'annule en $(0, 1, 1, 1, 1)$, et tel que $\mathfrak{D}\mathfrak{p} \subset \mathfrak{p}$. Alors $z(X_2^3 - X_0X_3^2) \in \mathfrak{p}$.*

La relation $D\Delta = \Delta P$ montre que l'idéal principal engendré par $X_2^3 - X_0X_3^2$ est stable sous $\mathfrak{D}$.

Pour terminer la démonstration du théorème 5, on utilise le fait que, pour un tel idéal premier $\mathfrak{p}$ contenant $X_2^3 - X_0X_3^2$, on a

$$\mathrm{ord}\mathfrak{p}(\overline{f}) \leq 3N(\mathfrak{p}) + B(\mathfrak{p}).$$

La démonstration du lemme 4 distingue plusieurs cas suivant la dimension de l'idéal $\mathfrak{p} \cap \mathcal{R}[X_0, X_1, X_2, X_3]$. Si cette dimension est nulle, on applique le théorème des zéros de Hilbert. Si elle vaut 1, on paramètre (Puiseux) une courbe algébrique contenue dans la variété des zéros de $\mathfrak{p} \cap \mathcal{R}[X_0, X_1, X_2, X_3]$ par $\big(1 : x : f(x) : g(x)\big)$. On montre qu'il existe des polynômes non nuls $A \in \mathfrak{p} \cap \mathcal{R}[X_0, X_1, X_2]$ et $B \in \mathfrak{p} \cap \mathcal{R}[X_0, X_1, X_3]$. En dérivant $A\big(1, x, f(x), g(x)\big)$ et $B\big(1, x, f(x), g(x)\big)$, on obtient un système différentiel satisfait par f et g, dont on montre que la seule solution est $(f, g) = (x^2, x^3)$.

Si $\mathfrak{p} \cap \mathcal{R}[X_0, X_1, X_2, X_3]$ est de dimension 2, cet idéal est principal. On en choisit un générateur A, et on écrit $\mathfrak{D}A \in \mathfrak{p}$. On montre ainsi que $u(z) = A\big(z, 1, P(z), Q(z), R(z)\big)$ satisfait une équation différentielle $zu'(z) = \big(aP(z)+b\big)u(z)$,

avec deux nombres a et b complexes. On vérifie ensuite que a et b sont des entiers rationnels, et on en conclut $A = cz^b(X_2^3 - X_3^2X_0)^a$.

Enfin le cas où $\mathfrak{p} \cap \mathcal{R}[X_0, X_1, X_2, X_3]$ est de dimension 3 est facile : on a $\mathfrak{p} \cap \mathcal{R} \neq \{0\}$, donc $z \in \mathfrak{p}$.

Il est intéressant de comparer le théorème 5 avec le lemme de zéros obtenu par Philibert [68] :

Soient $L_1 \geq 0$ et $L_2 \geq 1$ deux entiers et $P \in \mathcal{C}[X, Y]$ un polynôme non nul vérifiant $\deg_X P \leq L_1$ et $\deg_Y P \leq L_2$. Alors

$$\mathrm{ord}_0 P\big(z, J(z)\big) \leq 9L_1L_2 + \frac{3}{2}L_2 - \frac{1}{2}.$$

Cet énoncé permet de majorer M par $37L$ dans la démonstration du théorème 2. Il joue un rôle crucial dans les travaux de Barré [54] et [55].

Un énoncé conjectural, contenant à la fois ce résultat de Philibert et le théorème 5, a été proposé par Bertrand [36]. On peut être encore plus ambitieux en proposant le problème suivant : *pour tout polynôme non nul $A \in \mathcal{C}[z, X_1, X_2, X_3]$, de degré $\leq L_0$ en z et $\leq L_i$ en X_i, avec $L_i \geq 1$, $(0 \leq i \leq 3)$, et pour toute base de transcendance $\{f, g, h\}$ du corps $K = \mathbb{Q}(P, Q, R)$, montrer que la multiplicité du zéro à l'origine de la fonction analytique*

$$A\big(z, f(z), g(z), h(z)\big)$$

est majorée par $cL_0L_1L_2L_3$, avec une constante $c > 0$ ne dépendant que de f, g, h.

S'il reste encore des erreurs dans ce texte, je m'en excuse auprès de tous ceux qui en ont corrigé une version préliminaire.

BIBLIOGRAPHIE COMMENTÉE

Les deux principaux articles à la base de cet exposé sont les suivants :

[1] K. BARRÉ-SIRIEIX, G. DIAZ, F. GRAMAIN, G. PHILIBERT - *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), 1–9.

[2] Yu.V. NESTERENKO - *Modular functions and transcendence questions*, Mat. Sb., **187** N° 9 (1996), 65–96. Engl. Transl., Sbornik Math., **187** N° 9 (1996), 1319–1348.

Les résultats de ce second article ont été annoncés dans une note aux Comptes Rendus :

[3] Yu.V. NESTERENKO - *Modular functions and transcendence problems - Un théorème de transcendance sur les fonctions modulaires*, C. R. Acad. Sc. Paris, Sér. 1 **322** (1996), 909–914.

Le théorème de Schneider sur la transcendance de $j(\tau)$ date de 1937 :

[4] Th. SCHNEIDER - *Arithmetische Untersuchungen elliptischer Integrale*, Math. Ann. **113** (1937), 1–13.

La démonstration se trouve aussi dans son livre :

[5] Th. SCHNEIDER - *Einführung in die transzendenten Zahlen*, Springer-Verlag 1957 (en allemand) ; trad. franç. : *Introduction aux nombres transcendants*, Gauthier-Villars 1959.

Le théorème stéphanois répond à une question posée par Mahler dans le cas complexe et par Manin dans le cas général :

[6] K. MAHLER - *Remarks on a paper by W. Schwarz*, J. Number Theory **1** (1969), 512–521.

[7] Yu. MANIN - *Cyclotomic fields and modular curves*, Usp. Mat. Nauk **26** N°6 (1971), 7–71 (en russe) ; trad. angl. : Russian Math. Surveys **26** (1971), 7–78.

Voir aussi, pour le cas p-adique,

[8] B. MAZUR, J. TATE and J. TEITELBAUM - *On p-adic analogs of the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[9] H. HIDA, J. TILOUINE, E. URBAN - *Adjoint modular Galois representations and their Selmer groups*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), 4249-4252.

Dans [6], Mahler développe la méthode de transcendance qu'il avait élaborée une quarantaine d'années plus tôt.

[10] K. MAHLER - *Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen*, Math. Z. **32** (1930), 545–585.

Après la parution de [6], de nombreux auteurs ont développé la méthode de Mahler, notamment J. Loxton, A.J. van der Poorten, K.K. Kubota, Kumiko Nishioka, P.G. Becker, T. Töpfer :

[11] K. NISHIOKA - *Mahler's functions and transcendence*, Lecture Notes in Math. **1631** Springer-Verlag (1996).

La méthode de Gel'fond-Schneider a aussi été appliquée par plusieurs auteurs à l'étude de fonctions analytiques dans un disque. En plus de la conjecture de Mahler-Manin, une des motivations de ces recherches est le deuxième problème de Schneider [5].

[12] P. BUNDSCHUH - *Quelques résultats arithmétiques sur les fonctions thêta de Jacobi*, Groupe d'Etude sur les Problèmes Diophantiens, 1983-84, fasc. 1, Publ. Univ. P. et M. Curie **64** (1984), n°1, 15 pp.

[13] F. GRAMAIN, M. MIGNOTTE et M. WALDSCHMIDT - *Valeurs algébriques de fonctions analytiques*, Acta Arith. **47** (1986), 97–121.

[14] I. WAKABAYASHI - *Algebraic values of functions on the unit disk*, Proc. Prospects of Math. Sci., World Sci. Pub. (1988), 235–266.

[15] P. BUNDSCHUH et M. WALDSCHMIDT - *Irrationality results for theta functions by Gel'fond–Schneider's method*, Acta Arith. **53** (1989), 73-91 et **78** (1996), 99.

Le critère de Schneider-Lang, qui permet de démontrer la transcendance de valeurs de fonctions satisfaisant des équations différentielles, peut être étendu en un énoncé donnant des résultats d'indépendance algébrique :

[16] G. WÜSTHOLZ - *Algebraische Unabhängigkeit von Werten von Funktionen, die gewissen Differentialgleichungen genügen*, J. reine angew. Math. **317** (1980), 102–119.

Les premiers résultats de transcendance concernant les fonctions elliptiques ou abéliennes ont été obtenus par Siegel et Schneider :

[17] C.L. SIEGEL - *Über die Perioden elliptischer Funktionen*, J. reine angew. Math. **167** (1932), 62–69.

[18] Th. SCHNEIDER - *Zur Theorie der Abelschen Funktionen und Integrale*, J. reine angew. Math. **183** (1941), 110–128.

Quand g_2 et g_3 sont algébriques, l'espace vectoriel engendré sur le corps des nombres algébriques par $1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$ a pour dimension 4 dans le cas CM, et 6 sinon.

[19] D.W. MASSER - *Elliptic functions and transcendence*, Springer-Verlag, Lecture Notes in Math. **437** (1975).

La transcendance de $\Gamma(1/4)$ a été démontrée il y a vingt ans :

[20] G.V. CHUDNOVSKIJ - *Algebraic independence of constants connected with exponential and elliptical functions*, Dokl. Ukr. SSR Ser. A **8** (1976), 698–701 (en russe) ; résumé angl. p. 767.

[21] G.V. CHUDNOVSKY - *Algebraic independence of values of exponential and elliptic functions*, Proc. Intern. Cong. Math. Helsinki **1** (1978), 339–350.

[22] G.V. CHUDNOVSKY - *Contributions to the theory of transcendental numbers*, Math. Surveys and Monographs N°19, Amer. Math. Soc., 1984, 450 pp.

[23] M. WALDSCHMIDT - *Les travaux de G.V. Čudnovskiĭ sur les nombres transcendants*, Sém. Bourbaki 28ème année (1975/76), N° 488 ; Springer-Verlag, Lecture

Notes in Math. **567** (1977), 274–292.

Un analogue p-adique du théorème de Chudnovsky sur l'indépendance algébrique de périodes et quasi-périodes attachées à des formes différentielles elliptiques a été établi par André, en utilisant une approche entièrement différente de celle de [20] :

[24] Y. ANDRÉ - *G-fonctions et transcendance*, J. reine angew. Math. **476** (1996), 95–125.

Les nombres rationnels dans l'intervalle $]0,1[$, où on sait montrer que la fonction Γ prend des valeurs transcendantes, sont $\{1/6, 1/4, 1/3, 1/2, 2/3, 3/4, 5/6\}$. Ce sont précisément ces valeurs pour lesquelles un algorithme de calcul rapide est connu, utilisant la moyenne arithmético-géométrique :

[25] J.M. BORWEIN and I.J. ZUCKER - *Fast evaluation of the gamma function for small rational fractions using complete elliptic integrals of the first kind*, IMA Journal of Numerical Analysis **12** (1992), 519–526.

Les auteurs de [25] qualifient de "surprenante" la formule

$$\frac{\Gamma(1/24)\Gamma(11/24)}{\Gamma(5/24)\Gamma(7/24)} = \sqrt{3}\sqrt{2+\sqrt{3}}.$$

La conjecture de Rohrlich donne un algorithme (conjectural) pour trouver toutes les relations de ce type :

[26] S. LANG - *Cyclotomic Fields*, Graduate Texts in Math. **59** Springer-Verlag 1978.

Pour étudier la transcendance de nombres tels que $\Gamma(1/5)$, on est amené à considérer des formes différentielles sur des courbes de genre ≥ 2, et à utiliser la formule de Chowla et Selberg :

[27] S. CHOWLA and A. SELBERG - *On Epstein's zeta function*, J. reine angew. Math. **227** (1966), 97–110.

[28] B. GROSS - *On the periods of abelian integrals and a formula of Chowla and Selberg*, Invent. Math. **45** (1978), 193–208.

[29] N. KOBLITZ and D.E. ROHRLICH - *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. **30** (1978), 1183–1205.

[30] N. KOBLITZ - *Gamma function identities and elliptic differentials on Fermat curves*, Duke Math. J. **45** (1978), 87–99.

Les premiers résultats de transcendance concernant les valeurs de fonctions modulaires ont été déduits par Bertrand, d'abord des énoncés de Schneider :

[31] D. BERTRAND - *Séries d'Eisenstein et transcendance*, Bull. Soc. Math. France **104** (1976), 309–321.

puis de ceux de Chudnovsky :

[32] D. BERTRAND - *Fonctions modulaires, courbes de Tate et indépendance algébrique*, Sém. Delange-Pisot-Poitou (Théorie des Nombres) 19ème année (1977/78), n°36, 11 pp.

[33] D. BERTRAND - *Modular functions and algebraic independence*, Proc. Conf. p-adic analysis, Nijmegen 1978, Kath. Univ. Report n°7806.

[34] D. BERTRAND - *Fonctions modulaires et indépendance algébrique II*, Journées Arithmétiques Luminy, Soc. Math. France, Astérisque **61** (1979), 29–34.

Ces travaux de Bertrand fournissent aussi des analogues ultramétriques des résultats de Schneider et de Chudnovsky.

La conjecture sur la transcendance de $j'(\tau)$, quand $j(\tau)$ est algébrique différent de 0 et 1728, est discutée dans le §4 de :

[35] S. LANG - *Transcendental numbers and diophantine approximations*, Bull. Amer. Math. Soc. **77** (1971), 635–677.

Plusieurs conséquences du théorème de Nesterenko ont été obtenues récemment :

[36] D. BERTRAND - *Theta functions and transcendence*, Madras Number Theory Symposium 1996, The Ramanujan J., **1** (1997), 339–350.

[37] D. DUVERNEY, K. NISHIOKA, K. NISHIOKA and I. SHIOKAWA - *Transcendence of Jacobi's theta series*, Proc. Japan. Acad. Sc., **72**, Sér. A (1996), 202–203 ; *Transcendence of Jacobi's theta series and related results*, in "Number Theory – Diophantine, Computational and Algebraic Aspects", K.Győry, A.Pethő and V.T.Sòs, eds., Proc. Conf. Number Theory Eger 1996, W. de Gruyter, à paraître ; *Transcendence of Roger-Ramanujan continued fraction and reciprocal sums of Fibonacci numbers*, Proc. Japan. Acad. Sc., à paraître.

Les nombres $\sum_{n\geq 1} \ell^{-n^2}$ ($\ell > 1$ entier), considérés par Liouville en 1851 :

[38] J. LIOUVILLE - *Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques*, J. Math. Pures App. **16** (1851), 133–142

ne sont pas des "nombres de Liouville" (!) ; cela a été montré par Bundschuh en 1970, utilisant les fonctions de Tschakaloff $\sum_{n=0}^{\infty} z^n q^{-n(n-1)/2}$:

[39] P. BUNDSCHUH - *Ein Satz über ganze Funktionen und Irrationalitätsausagen*, Invent. Math. **9** (1970), 175–184.

La fonction de Golomb est $\gamma(n) = \mathrm{Card}\{(a,b) \in \mathbb{N}^2 \, ; \, a^b = n\}$. Sa série de Dirichlet génératrice est $\sum_{n=2}^{\infty} \gamma(n) n^{-s} = \sum_{n=2}^{\infty} (n^s - 1)^{-1}$ qui converge pour $\Re e(s) > 1$:

[40] P. BUNDSCHUH - *Zwei Bemerkungen über transzendente Zahlen*, Mh. Math. **88** (1979), 293–304.

L'indépendance algébrique des fonctions z, $P(z)$, $Q(z)$ et $R(z)$ est établie dans :

[41] K. MAHLER - *On algebraic differential equations satisfied by automorphic functions*, J. Austral. Math. Soc. **10** (1969), 445–450.

Dans cet article, Mahler donne des résultats plus généraux d'indépendance algébrique de fonctions, et pose un problème qui a été résolu par Keiji Nishioka ; par exemple les fonctions thêta de Jacobi ne satisfont pas d'équation différentielle d'ordre inférieur à 3 sur $\mathbb{C}(q)$:

[42] K. NISHIOKA - *A conjecture of Mahler on automorphic functions*, Arch. Math. **53** (1989), 46–51.

C'est encore Mahler qui, le premier, a étudié la croissance de la longueur des polynômes modulaires :

[43] K. MAHLER - *On the coefficients of the 2^n-th transformation polynomial for $j(\omega)$*, Acta Arith. **21** (1972), 89–97.

[44] K. MAHLER - *On the coefficients of transformation polynomials for the modular function*, Bull. Austral. Math. Soc. **10** (1974), 197–218.

[45] P. COHEN - *On the coefficients of the transformation polynomials for the elliptic modular function*, Math. Proc. Camb. Phil. Soc. **95** (1984), 389–402.

Le problème des quatre exponentielles est posé dans [5], ainsi que dans :

[46] S. LANG - *Nombres transcendants*, Sém. Bourbaki 18ème année (1965/66), N° 305.

[47] S. LANG - *Introduction to transcendental numbers*, Addison-Wesley series in Math., Addison-Wesley 1966.

[48] K. RAMACHANDRA - *Contributions to the theory of transcendental numbers (I)*, Acta Arith. **14** (1968), 65–72 ; *(II)*, id., 73–88.

[49] J-P. SERRE - *Dépendance d'exponentielles p-adiques*, Sém. Delange-Pisot-Poitou (Théorie des Nombres) 7ème année (1965/66), n°15.

[50] D. BERTRAND - *Valeurs de fonctions thêta et hauteurs p-adiques*, Sém. Th. Nombres, Paris 1980–81, (Séminaire Delange–Pisot–Poitou), Progress in Math. **22**, Birkhäuser Verlag (1982), 1–11.

[51] G. DIAZ - *La conjecture des quatre exponentielles et les conjectures de D. Bertrand sur la fonction modulaire*, J. Th. Nombres Bordeaux, **9** (1997), 229–245.

Des énoncés d'approximation (mesures d'approximation, de transcendance, d'indépendance algébrique) apportent des raffinements quantitatifs aux théorèmes de transcendance :

[52] A. FAISANT et G. PHILIBERT - *Quelques résultats de transcendance liés à l'invariant modulaire j*, J. Number Theory **25** (1987), 184–200.

[53] G. PHILIBERT - *Une mesure d'indépendance algébrique*, Ann. Inst. Fourier (Grenoble) **38** (1988), 85–103.

[54] K. BARRÉ - *Mesures de transcendance pour l'invariant modulaire*, C. R. Acad. Sc. Paris, Sér. 1 **323** (1996), 447–452.

[55] K. BARRÉ - *Mesure d'approximation simultanée de q et $J(q)$*, J. Number Theory, à paraître.

Comme le note Bertrand [36], en transcendance, une hiérarchie des fonctions est donnée par la croissance de la hauteur des coefficients de leur série de Taylor à l'origine : pour les G-fonctions, la croissance est c^n ; pour les fonctions modulaires, l'estimation de Mahler sur les coefficients de J, qui donne $O\big(\exp(4\sqrt{n})\big)$, est un exemple typique ; pour les formes modulaires de poids k, la croissance est n^k ; enfin, pour les E-fonctions, la valeur absolue des coefficients de Taylor croît comme $c^n/n!$, mais leur hauteur comme $c^n n!$. Cela peut être formalisé :

[56] P. PHILIPPON - *Indépendance algébrique et K-fonctions*, J. reine angew. Math., à paraître.

[57] P. PHILIPPON - *Une approche méthodique pour la transcendance et l'indépendance algébrique de valeurs de fonctions analytiques*, J. Number Theory, **64** (1997), 291-338.

Un rapport sur les progrès récents concernant l'indépendance algébrique (incluant des travaux de D. Roy, G. Diaz, M. Laurent, P. Philippon et d'autres) vient d'être rédigé :

[58] M. LAURENT - *New methods in algebraic independence*, Proc. Conf. Number Theory Eger 1996, à paraître.

Voici maintenant quelques références concernant les lemmes de zéros :

[59] Yu.V. NESTERENKO - *Estimates of the orders of zeros of analytic functions of a certain class and their application to the theory of transcendental numbers*, Dokl. Akad. Nauk SSSR **205** (1972) ; trad. angl. Soviet Math. Dokl. **13** (1972), 938–942.

[60] Yu.V. NESTERENKO - *Estimates for the orders of zeros of functions of a certain class and application in the theory of transcendental numbers*, Izv. Akad. Nauk SSSR **41** (1977) ; trad. angl. Math. USSR Izv. **11** (1977), 239–270.

[61] D.W. MASSER - *A vanishing theorem for power series*, Invent. Math. **67** (1982), 275–296.

[62] D.W. MASSER - *Zero estimates on group varieties*, Proc. Intern. Cong. Math. Warszawa (1983), 493–502.

[63] P. PHILIPPON - *Lemme de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France **114** (1986), 355–383, et **115** (1987), 397–398.

[64] D. BERTRAND - *Lemmes de zéros et nombres transcendants*, Sém. Bourbaki, 38ème Année 1985–86, N° 652 ; Soc. Math. France, Astérisque, **145–146** (1987), 21–44.

[65] Yu.V. NESTERENKO - *Estimates for the number of zeros of certain functions*, in *New Advances in Transcendence Theory*, Proc. Conf. Durham 1986, ed. A. Baker, Cambridge Univ. Press (1988), 263–269.

[66] Yu.V. NESTERENKO - *Bounds for the number of zeroes of functions of a certain class*, Acta Arith. **53** (1989), 29–46 (en russe).

[67] Yu.V. NESTERENKO - *Algebraic independence of values of analytic functions*, Proc. Intern. Cong. Math. Kyoto (1990), 447–457.

[68] G. PHILIBERT - *Un lemme de zéros pour l'invariant modulaire*, J. Number Theory, à paraître.

Le critère d'indépendance algébrique de Philippon :

[69] P. PHILIPPON - *Critères pour l'indépendance algébrique*, Inst. Hautes Et. Sci. Publ. Math. **64** (1986), 5–52.

a été raffiné pour obtenir des résultats d'approximation diophantienne, par Jabbouri (qui sépare degré et hauteur), par Ably (qui obtient ainsi des mesures d'indépendance algébrique dans des groupes algébriques), et plus récemment par Jadot :

[70] E.M. JABBOURI - *Sur un critère pour l'indépendance algébrique de P. Philippon*, Approximations diophantiennes et nombres transcendants, Luminy 1990, éd. P. Philippon, W. De Gruyter, 1992, 285–307.

[71] M. ABLY - *Résultats quantitatifs d'indépendance algébrique pour les groupes algébriques*, J. Number Theory **42** (1992), 194–231.

[72] C. JADOT. - *Critères pour l'indépendance algébrique et linéaire*, Thèse, Univ. P. et M. Curie (Paris VI), 1996.

On trouvera des informations sur les fonctions modulaires, elliptiques et thêta dans les références suivantes :

[73] S. RAMANUJAN - *On certain arithmetical functions*, Trans. Camb. Phil. Soc. **22** (1916), 159–184 ; Collected Papers of Srinivasa Ramanujan, Chelsea Publ., N.Y. 1927, N°18, 136–162.

[74] J-P. SERRE - *Cours d'arithmétique*, Coll. SUP, Presses Univ. France, 1970 ; trad. angl. : *A course in arithmetic*, Graduate Texts in Math. **7** Springer-Verlag 1973.

[75] S. LANG - *Elliptic functions*, Springer-Verlag 1973.

[76] S. LANG - *Introduction to modular forms*, Springer-Verlag 1976.

[77] K. CHANDRASEKHARAN - *Elliptic functions*, Grund. der math. Wiss. **281** Springer-Verlag 1985.

Une formule donnant les valeurs des coefficients $c(n)$ (dans le développement de Laurent de J à l'origine) en termes de valeurs en des points CM (sans faire intervenir de sommes infinies comme chez Petersson et Rademacher) a été déduite par Kaneko d'un travail de Zagier :

[78] M. KANEKO - *The Fourier coefficients and the singular moduli of the elliptic modular function* $j(\tau)$, Mem. Fac. Engin. Design Kyoto Inst. Tech. **44** (1996), 1–5.

Une extension du théorème 1 en dimension supérieure a fait l'objet de plusieurs travaux

[79] Y. MORITA - *On transcendency of special values of arithmetic automorphic functions*, J. Math. Soc. Japan **24** (1972), 268–274.

[80] H. SHIGA et J. WOLFART - *Criteria for complex multiplication and transcendence properties of automorphic functions*, J. reine angew. Math. **463** (1995), 1–25.

[81] P. BEAZLEY COHEN - *Humbert surfaces and transcendence properties of automorphic functions*, Rocky Mountain J. Math. **26** (1996), 987–1002.

L'analogue en caractéristique finie du théorème stéphanois a été démontré juste avant le cas classique (complexe ou p-adique) :

[82] D. THAKUR - *Automata style proof of Voloch's result on transcendence*, J. Number Theory **58** (1996), 60–63.

[83] J.F. VOLOCH - *Transcendence of elliptic modular functions in characteristic p*, J. Number Theory **58** (1996), 55–59.

Michel WALDSCHMIDT
Institut de Mathématiques de Jussieu
UMR 9994 du CNRS
Problèmes Diophantiens
Case 247
4, place Jussieu
F–75252 PARIS CEDEX 05
miw@math.jussieu.fr