Séminaires & Congrès
12, 2005, p. 119–178

INDÉPENDANCE ALGÉBRIQUE DE VALEURS DE SÉRIES D'EISENSTEIN (THÉORÈME DE NESTERENKO)

par

Vincent Bosser

***Résumé.* —** Ce texte est consacré au théorème de Nesterenko sur l'indépendance algébrique de valeurs de séries d'Eisenstein. Après en avoir rappelé l'énoncé et les principaux corollaires, on en présente la preuve, en mettant plus particulièrement l'accent sur le lemme de multiplicité utilisé. La preuve de ce lemme repose sur des résultats d'algèbre commutative (théorie de l'élimination) et de géométrie diophantienne qui sont expliqués en détail. Le texte se termine par un bref aperçu de différentes variantes de la preuve du théorème de Nesterenko, et notamment des méthodes permettant d'obtenir des versions quantitatives du théorème.

***Abstract* (Algebraic independence of values of Eisenstein series). —** This text is devoted to Nesterenko's theorem on the algebraic independence of values of Eisenstein series. After recalling its statement and its main corollaries, we present its proof, stressing particularly the multiplicity estimate used. The proof of this estimate rests on results from commutative algebra (elimination theory) and diophantine geometry which are explained in detail. The text ends with a brief overview of different variants of the proof of Nesterenko's theorem, and especially of the methods providing quantitative versions of the theorem.

Introduction

Soient P, Q et R les fonctions de Ramanujan : ces fonctions sont reliées aux séries d'Eisenstein E_2, E_4, E_6 de poids 2, 4, et 6 par les relations $P(e^{2\pi i\tau}) = E_2(\tau)$, $Q(e^{2\pi i\tau}) = E_4(\tau)$ et $R(e^{2\pi i\tau}) = E_6(\tau)$ (où $\tau \in \mathbb{C}$ est tel que $\Im m\,\tau > 0$). En 1996, Nesterenko a démontré le résultat remarquable suivant : si q est un nombre complexe non nul tel que $|q| < 1$, alors au moins trois nombres parmi q, $P(q)$, $Q(q)$, et $R(q)$ sont algébriquement indépendants sur $\mathbb{Q}$.

Les conséquences de ce théorème sont nombreuses. Par exemple, il implique l'indépendance algébrique sur $\mathbb{Q}$ des nombres π, e^π et $\Gamma(1/4)$, ou bien le théorème stéphanois

***Classification mathématique par sujets* (2000). —** 11J85, 11G, 11G35, 11G50.
***Mots clefs.* —** Indépendance algébrique, séries d'Eisenstein, lemme de multiplicité, lemme de zéro, théorie de l'élimination, géométrie diophantienne, théorème de Bézout.

(anciennement *conjecture de Mahler*), ou bien encore la transcendance des nombres $\sum_{n\geqslant 0} q^{n^2}$ pour q algébrique vérifiant $0<|q|<1$ (nombres qui furent considérés tout d'abord par Liouville avec $q^{-1}\in\mathbb{Z}$, et dont il n'avait pu démontrer que l'irrationalité).

La démonstration de ce résultat suit dans ses grandes lignes le schéma classique d'une preuve de transcendance : construction d'une fonction auxiliaire F à forte multiplicité en zéro à l'aide d'un lemme de Siegel, existence et minoration d'une dérivée non nulle de F au point q d'ordre pas trop grand à l'aide d'une formule d'interpolation, majoration analytique au moyen des inégalités de Cauchy, application d'un lemme de multiplicité, et enfin application d'un critère d'indépendance algébrique.

En fait, l'apport de Nesterenko réside ici dans l'établissement du lemme de multiplicité, qui constitue le point crucial et difficile de la preuve. Ce lemme de multiplicité se démontre à l'aide des techniques de théorie de l'élimination et des outils de géométrie diophantienne qui ont été développés essentiellement par Nesterenko et Philippon au cours de ces 25 dernières années. L'objet de ces notes est d'expliquer comment on peut établir le théorème de Nesterenko, et plus particulièrement le lemme de multiplicité.

Après avoir rappelé, au § 1, l'énoncé et les principales conséquences du théorème, on présentera tout d'abord rapidement (§ 2) la démonstration initiale de Nesterenko, en admettant le lemme de multiplicité. On reviendra ensuite en détail sur la preuve de ce lemme : il s'agit ici d'une majoration de la multiplicité en 0 d'un polynôme non nul en les fonctions z, $P(z)$, $Q(z)$ et $R(z)$. Bien que la preuve proposée s'inspire du travail de Nesterenko, on adoptera ici une présentation différente sur plusieurs points. Tout d'abord, on utilisera le formalisme, les définitions et les résultats de Philippon (formes résultantes, cycles...) plutôt que le point de vue de Nesterenko. Ensuite, de nombreux arguments de la preuve originale ont été modifiés et certains points ont été (me semble-t-il) simplifiés et clarifiés. Cette preuve du lemme de multiplicité fait l'objet du § 4. Comme on l'a dit, elle repose sur des outils d'algèbre commutative et de géométrie diophantienne. Ceux-ci seront présentés au § 3 : théorie de l'élimination, théorie des hauteurs des variétés projectives, distance d'un point à une variété, théorèmes de Bézout arithmétique et métrique... Enfin, dans un dernier paragraphe (§ 5), on donnera un bref aperçu des différentes variantes de la preuve du théorème de Nesterenko, et notamment des méthodes permettant d'obtenir des versions quantitatives du théorème (le plus souvent sans démonstration).

Notations générales. — Dans tout ce texte, on note $\mathbb{N}$ (resp. $\mathbb{N}^*$) l'ensemble des entiers $\geqslant 0$ (resp. $\geqslant 1$). Si F est un polynôme en plusieurs indéterminées $z_1,\dots,z_n$, on note $\deg F$ son degré total, et $\deg_{z_i} F$ son degré partiel par rapport à z_i. De façon analogue, si z^i désigne un groupe d'indéterminées $z_{i_1},\dots,z_{i_k}$, on note $\deg_{z^i} F$ le degré de F par rapport au groupe d'indéterminées z^i. Lorsque $\alpha=(\alpha_1,\dots,\alpha_N)$ est un N-uplet d'éléments de $\mathbb{N}$ (où $N\in\mathbb{N}^*$), on note $|\alpha|=\alpha_1+\cdots+\alpha_N$. Enfin, si K est un corps, on note $\overline{K}$ une clôture algébrique de K.

1. Énoncé du théorème et corollaires

Notons $\mathcal{H} = \{\tau \in \mathbb{C} \mid \Im m\, \tau > 0\}$. Pour tout $k \geqslant 2$, notons E_{2k} la série d'Eisenstein de poids k normalisée par

$$E_{2k}(\tau) = \frac{1}{2\zeta(2k)} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq 0}} \frac{1}{(m\tau+n)^{2k}} \qquad (\tau \in \mathcal{H}).$$

Notons encore E_2 la fonction analytique dans $\mathcal{H}$ définie de façon analogue par

$$E_2(\tau) = \frac{1}{2\zeta(2)} \left[2\sum_{n\geqslant 1} \frac{1}{n^2} + 2\sum_{m\geqslant 1} \sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^2} \right].$$

On sait ([**Sch74**, pages 55 et 63] ou [**Lan76**, Chap. X]), que si $q = e^{2\pi i\tau}$ $(\tau \in \mathcal{H})$, les fonctions E_2, E_4, E_6 admettent le développement en série de Fourier suivant :

$$E_2(\tau) = 1 - 24\sum_{n\geqslant 1} \sigma_1(n) q^n \tag{1}$$

$$E_4(\tau) = 1 + 240\sum_{n\geqslant 1} \sigma_3(n) q^n \tag{2}$$

$$E_6(\tau) = 1 - 504\sum_{n\geqslant 1} \sigma_5(n) q^n \tag{3}$$

où $\sigma_k(n) = \sum_{d|n} d^k$. On notera dans la suite P, Q et R les fonctions définies par $P(q) = E_2(\tau)$, $Q(q) = E_4(\tau)$ et $R(q) = E_6(\tau)$ (notations de Ramanujan). Les fonctions P, Q, R sont définies et analytiques dans le disque ouvert $\{q \in \mathbb{C} \mid |q| < 1\}$. De plus, elles vérifient le système différentiel suivant (voir [**Lan76**], Chap. X, theorem 5.3) :

$$(S_0) \qquad \begin{cases} \mathscr{D}P = \frac{1}{12}(P^2 - Q) \\ \mathscr{D}Q = \frac{1}{3}(PQ - R) \\ \mathscr{D}R = \frac{1}{2}(PR - Q^2) \end{cases}$$

où $\mathscr{D} = q\frac{d}{dq}$.

Comme on l'a dit dans l'introduction, le théorème que nous allons étudier dans ces notes est le suivant [**Nes96**] :

Théorème 1.1. — *Soit $q \in \mathbb{C}$ tel que $0 < |q| < 1$. Alors l'ensemble $\{q, P(q), Q(q), R(q)\}$ contient au moins trois nombres algébriquement indépendants sur $\mathbb{Q}$.*

Ce théorème fournit de nombreux résultats de transcendance ou d'indépendance algébrique. Nous ne donnerons ici à titre d'exemple que cinq corollaires. On pourra consulter [**Nes96**], [**NP01**, chap. 3] et [**Wal97**] pour d'autres résultats.

Selon les notations usuelles, on notera dans ce qui suit j l'invariant modulaire, et J la fonction définie dans le disque épointé $\{q \in \mathbb{C} \mid 0 < |q| < 1\}$ par $J(e^{2\pi i\tau}) = j(\tau)$ ($\tau \in \mathcal{H}$). Le premier corollaire que nous énoncerons est le suivant :

Corollaire 1.2

(i) *Soit $\tau \in \mathcal{H}$ qui ne soit congru ni à i ni à $\rho = e^{2\pi i/3}$ modulo $\mathrm{SL}_2(\mathbb{Z})$, et soit $q = e^{2\pi i\tau}$. Alors on a*

$$\mathrm{degtr}_{\mathbb{Q}}\, \mathbb{Q}(q, J(q), J'(q), J''(q)) \geqslant 3.$$

(ii) *En particulier, pour tout $q \in \mathbb{C}$ algébrique tel que $0 < |q| < 1$, les nombres $J(q)$, $J'(q)$ et $J''(q)$ sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration. — En utilisant la relation bien connue [**Lan76**, chap. 1, § 3]

$$J = 1728\frac{Q^3}{Q^3 - R^2}$$

et le système différentiel (S_0), on vérifie que l'on a les formules :

$$P = 6\frac{\mathscr{D}^2 J}{\mathscr{D}J} - 4\frac{\mathscr{D}J}{J} - 3\frac{\mathscr{D}J}{J - 1728},\ Q = \frac{(\mathscr{D}J)^2}{J(J-1728)},\ R = -\frac{(\mathscr{D}J)^3}{J^2(J-1728)}.$$

Ces formules sont valables lorsque $\mathscr{D}J(q) \neq 0$, $J(q) \neq 0$ et $J(q) \neq 1728$, *i.e.* lorsque τ n'est congru ni à i ni à ρ modulo $\mathrm{SL}_2(\mathbb{Z})$. Il en résulte que dans ce cas les corps $\mathbb{Q}(q, J(q), J'(q), J''(q))$ et $\mathbb{Q}(q, P(q), Q(q), R(q))$ sont égaux. Ceci démontre (i).

Pour démontrer (ii), il suffit de constater que si $q = e^{2\pi i\tau}$ est algébrique, alors τ ne peut pas être algébrique irrationnel d'après le théorème de Gelfond-Schneider (car $2\pi i$ est un logarithme de 1)[(1)]. Donc τ vérifie les hypothèses de (i). □

On remarquera que la partie (ii) du corollaire entraîne en particulier le théorème stéphanois (conjecture de Mahler).

Les deux corollaires suivants concernent les fonctions elliptiques et généralisent des résultats antérieurs de Chudnovsky [**Chu84**].

Corollaire 1.3. — *Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, (ω_1, ω_2) une base du réseau des périodes de $\wp$ telle que $\Im m(\omega_2/\omega_1) > 0$, η_1 la quasi-période correspondant à ω_1, et $\tau = \omega_2/\omega_1$. Alors les nombres $e^{2\pi i\tau}$, ω_1/π et η_1/π sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration. — D'après des formules classiques (voir [**Lan87**], chap. 4, formules (5) et (6) p. 44 et chap. 18, formule (2) p. 249), on a, en notant $q = e^{2\pi i\tau}$:

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

(1) Théorème de Gelfond-Schneider [**Wal00**] : soient $\alpha \in \overline{\mathbb{Q}}$, $\alpha \neq 0$, et $\beta \in \overline{\mathbb{Q}} \smallsetminus \mathbb{Q}$. Alors, pour toute détermination $\ell \neq 0$ du logarithme de α (*i.e.* pour tout $\ell \in \mathbb{C}$, $\ell \neq 0$, tel que $e^{\ell} = \alpha$), le nombre $\alpha^{\beta} := e^{\beta\ell}$ est transcendant.

On en déduit $\mathbb{Q}(q, P(q), Q(q), R(q)) \subset \mathbb{Q}(q, g_2, g_3, \omega_1/\pi, \eta_1/\pi) \subset \overline{\mathbb{Q}}(q, \omega_1/\pi, \eta_1/\pi)$, d'où le corollaire. □

Corollaire 1.4

(i) *Soit $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, correspondant à une courbe elliptique à multiplications complexes par le corps quadratique K. Alors, si ω est une période non nulle de $\wp$ et $\tau \in K$ est tel que $\Im m\, \tau \neq 0$, les trois nombres π, ω et $e^{2\pi i\tau}$ sont algébriquement indépendants sur $\mathbb{Q}$.*

(ii) *En particulier, les nombres π, e^{π} et $\Gamma(1/4)$ (resp. π, $e^{\pi\sqrt{3}}$ et $\Gamma(1/3)$) sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration

(i) Il n'y a pas de restriction à supposer la période $\omega = \omega_1$ primitive (*i.e.* multiple d'aucune autre période). Soit alors ω_2 telle que (ω_1, ω_2) soit une base du réseau des périodes de $\wp$ et telle que $\omega_2/\omega_1 \in \mathcal{H}$. Notons η_1, η_2 les quasi-périodes correspondant à ω_1 et ω_2. On peut supposer sans perte de généralité que $\tau = \omega_2/\omega_1$ (car ω_2/ω_1 est dans $K = \mathbb{Q}(\tau)$, donc de la forme $a + b\tau$, $a, b \in \mathbb{Q}$, $b \neq 0$). Maintenant, d'après [**Mas75**, Chap. 3, Lemma 3.1], il existe $\kappa \in \overline{\mathbb{Q}}$ et des entiers A, B, C avec $C \neq 0$ tels que

$$A + B\tau + C\tau^2 = 0 \qquad \text{et} \qquad A\eta_1 - C\tau\eta_2 = \kappa\tau\omega_1. \tag{4}$$

D'autre part, on dispose de la relation de Legendre :

$$\tau\omega_1\eta_1 - \omega_1\eta_2 = 2\pi i. \tag{5}$$

On déduit aisément de (4) et (5) que $\eta_1 \in \overline{\mathbb{Q}}(\pi, \omega_1)$, d'où $\overline{\mathbb{Q}}(e^{2\pi i\tau}, \omega_1/\pi, \eta_1/\pi) \subset \overline{\mathbb{Q}}(e^{2\pi i\tau}, \pi, \omega_1)$. Le corollaire 1.3 donne alors immédiatement le résultat.

(ii) On applique (i) à la courbe elliptique d'équation $y^2 = 4x^3 - 4x$, pour laquelle on a $K = \mathbb{Q}(i)$. On prend alors $\tau = i$ et pour ω la période fondamentale réelle $\omega = 2\int_1^\infty \frac{dt}{\sqrt{4t^3-4t}} = \frac{1}{2}B(1/4, 1/2) = \frac{\Gamma(1/4)^2}{\sqrt{8\pi}}$, où B désigne la fonction bêta d'Euler. On procède de façon analogue pour les nombres π, $e^{\pi\sqrt{3}}$ et $\Gamma(1/3)$ avec la courbe elliptique d'équation $y^2 = 4x^3 - 4$. Voir [**Nes96**, Corollary 5] pour les détails. □

Une conséquence remarquable du corollaire 1.4 est la suivante.

Corollaire 1.5. — *Pour tout entier $d \geqslant 1$, les nombres π et $e^{\pi\sqrt{d}}$ sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration. — Pour tout corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-d})$, il existe une fonction $\wp$ de Weierstrass d'invariants g_2, g_3 algébriques et définissant une courbe elliptique CM dont le corps des multiplications complexes est K. Il suffit alors d'appliquer le corollaire 1.4 (i) avec $\tau = i\sqrt{d}$. □