APPROXIMATION ET GÉOMÉTRIE DIOPHANTIENNES (GROUPE DE LECTURE À L'ENS LYON 2013)

Huayi Chen

La théorie des nombres transcendants étudie l'algébricité ou la transcendance d'un nombre complexe. Le but de cette théorie est de déterminer si un nombre complexe α vérifie une équation polynomiale (non-triviale) à coefficients dans $\mathbb{Z}$ (un tel nombre est appelé un *nombre algébrique*). Si un nombre complexe n'est pas algébrique, on dit qu'il est *transcendant*. Bien que les nombres transcendants sont "nombreux" (sachant que l'ensemble des nombres algébriques est dénombrable, tandis que le cardinale de $\mathbb{C}$ est égal à celui de $\{0,1\}^{\mathbb{N}}$), il est en général difficile de montre qu'un nombre donné est transcendant. L'approximation diophantienne permet de relier le problème de transcendance à la qualité d'approximation d'un nombre réel par des nombres rationnels. Initiée par le théorème fondateur de Liouville et enrichie par les travaux de de nombreux mathématiciens comme Thue, Siegel, Gel'fond, Roth, Baker etc., cette approche a conduit à une théorie très riche des nombres transcendants avec beaucoup de résultats importants.

Dans la plupart de démonstration diophantienne, on construit des polynômes à coefficients entiers pour aider à mesurer la qualité d'approximation. Ce genre de polynômes sont appelés des polynômes auxiliaires. L'approche initiale de Liouville utilise le polynôme minimal du nombre algébrique que l'on considère. Cependant, pour obtenir de meilleurs résultats, il est nécessaire de construire des polynômes auxiliaires multi-variés. Le point de vue géométrique est particulièrement efficace dans ce contexte. Il permet notamment d'incorporer plusieurs composants (structure de groupe, métrique, algébricité etc.) dans un même cadre. Des recherches (souvent profondes) montrent que les propriétés diophantiennes d'un système d'équations polynomiales à coefficients entiers sont souvent dominées par les propriétés géométriques de la variété définie par

ce système. En outre, la comparaison avec la géométrie algébrique (relativement à une courbe algébrique) donne des idées pertinentes et conduit à la théorie de géométrie arithmétique.

Le but de ce groupe de lecture est de comprendre les idées fondamentales de l'approximation diophantienne via des applications dans le problème de transcendance. Une attention particulière sera faite à l'interprétation géométrique de ces idées. On espère que ce groupe de lecture motivera ses participants à approfondir leurs études en géométrie algébrique et arithmétique.

1. Nombres transcendants et approximation diophantienne

Le but de cette séance est de présenter des définitions de base dans la théorie des nombres transcendants (notamment nombre algébrique, nombre transcendant, polynôme minimal etc.) et quelques résultats fondamentaux. On peut commencer par démontrer que l'ensemble des nombres algébriques est dénombrable, puis établir le théorème de Liouville (1844) comme la suite.

***Théorème 1.1* (Liouville).** — *Soit α un nombre algébrique de degré $d \geqslant 2$, alors il existe une constante explicite $C(\alpha) > 0$ telle que*

$$\left|\frac{p}{q} - \alpha\right| \geqslant \frac{C(\alpha)}{q^d}$$

pour tous entiers p, q tels que $q \neq 0$.

On appelle *nombre de Liouville* tout nombre réel α qui vérifie la condition suivante : il existe deux suites d'entiers $(p_n)_{n\geqslant 0}$ et $(q_n)_{n\geqslant 0}$ telles que $q_n \geqslant 1$ pour tout n, $\lim\limits_{n\to+\infty} q_n = +\infty$ et que

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}$$

pour tout indice $n \geqslant 0$. En utilisant le théorème de Liouville, on peut montrer que tout nombre de Liouville est transcendant. Cela permet de construire explicitement des nombres transcendants comme des séries.

Le théorème de Liouville montre que la qualité d'approximation d'un nombre algébrique irrationnelle ne peut pas être très bonne. Pour mesurer l'irrationalité d'un nombre réel, on introduit la notion suivante.

Définition 1.2. — Soit α un nombre dans $\mathbb{R} \setminus \mathbb{Q}$. On désigne par $\tau(\alpha)$ la borne inférieure de l'ensemble des nombres réels positif ν tels que, pour tout $\varepsilon > 0$, il n'y a qu'un nombre fini de couples d'entiers (p, q) avec $q \neq 0$ et qui vérifient

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\nu+\varepsilon}}.$$

On voit aussitôt de la définition que, si α est un nombre réel algébrique irrationnel, alors $\tau(\alpha)$ est majoré par le degré de α. En outre, il y a un théorème dû à Dirichlet (1842) qui donne la minoration $\tau(\alpha) \geqslant 2$ pour tout $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

***Théorème 1.3* (Dirichlet).** — *Soit α un nombre dans $\mathbb{R} \setminus \mathbb{Q}$. Il y a une infinité de nombres rationnels p/q qui vérifient*

$$\left|\frac{p}{q} - \alpha\right| \leqslant \frac{1}{q^2}.$$

La majoration de la fonction τ fut un sujet important de l'approximation diophantienne. Il fallait plus qu'un siècle après Liouville que Roth a finalement montrer que $\tau(\alpha) = 2$ pour tout nombre $\alpha \in (\mathbb{R} \cap \overline{\mathbb{Q}}) \setminus \mathbb{Q}$. La démonstration du théorème de Roth utilise des idées de la géométrie diophantienne et est le but des dernières séances du groupe de lecture.

Référence. — A. Baker, *Transcendental number theory* (§1.1). Cambridge University Press, London-New York, 1975. x+147 pp.
G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres* (chapitre I.7), Cours Spécialisés **1**, Société Mathématique de France, 1995, xv+457 pp.

2. Irrationalité de $\zeta(2)$ et $\zeta(3)$

Bien que le théorème de Liouville permet de construire une infinité (non-dénombrable) de nombres transcendants, il n'est pas évident de démontrer la transcendance d'un nombre complexe fixé. La plupart de démonstration d'irrationalité / de transcendance consiste à utiliser de façon astucieuse le fait (ou ses variantes en dimension supérieure) qu'un entier non-nul est de valeur absolue $\geqslant 1$. Cet exposé a pour but d'expliquer cette idée par quelques exemples explicites, à savoir l'irrationalité des nombres

$$\zeta(2) = \sum_{n \geqslant 1} \frac{1}{n^2}, \quad \text{et} \quad \zeta(3) = \sum_{n \geqslant 1} \frac{1}{n^3}.$$

C'est un théorème d'Apéry (1978). On ne sait pas encore si $\zeta(3)$ est un nombre transcendant. On présente une approche simplifiée due à Beukers qui consiste à exprimer les restes des séries définissant $\zeta(2)$ et $\zeta(3)$ comme des intégrales doubles :

$$\zeta(2) - \sum_{k=1}^{r} \frac{1}{k^2} = \int_0^1 \int_0^1 \frac{(xy)^r}{1-xy} \, \mathrm{d}x\mathrm{d}y,$$

$$\zeta(3) - \sum_{k=1}^{r} \frac{1}{k^3} = -\frac{1}{2} \int_0^1 \int_0^1 \frac{(xy)^r \log(xy)}{1-xy}.$$

Le point clé de la démonstration d'irrationalité est d'utiliser les polynômes de la forme

$$P_n(x) = \frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}x^n}(x^n(1-x)^n) \in \mathbb{Z}[x]$$

comme noyau d'intégration pour fabriquer des bonnes approximations de $\zeta(2)$ et $\zeta(3)$ par des nombres rationnels.

Référence. — F. Beukers, *A note on the irrationality of* $\zeta(2)$ *and* $\zeta(3)$, Bull. London Math. Soc. **11** (1979), no. 3, 268–272.

3. Transcendance de e et π

La transcendance de e est un théorème de Hermite (1873). Son irrationalité avait été établie précédemment par Euler en 1744. Lindemann (1882) a ensuite montré que le nombre π est transcendant. Sa stratégie est de montrer que l'exponentiel de tout nombre algébrique non-nul (éventuellement non-réel) est nécessairement transcendant. Donc la transcendance de π provient de l'égalité d'Euler $e^{\pi i} = -1$.

Le but de cet exposé est de présenter la démonstration de ces résultats, où la méthode de polynôme auxiliaire joue un rôle central. Le point clé pour la démonstration de la transcendance de e est d'introduire l'intégrale

$$I_f(t) = \int_0^t e^{t-s} f(s)\,\mathrm{d}s$$

pour tout polynôme f. Par intégration par partie on peut montrer que

$$I_f(t) = e^t \sum_{j=0}^{d} f^{(j)}(0) - \sum_{j=0}^{d} f^{(j)}(t),$$

où d est le degré de f. Si le nombre e vérifie une équation polynomiale à coefficients entiers

$$a_0 + a_1 e + \cdots + a_n e^n = 0,$$

un choix convenable de f (polynôme auxiliaire) permet d'obtenir des estimés contradictoires pour la quantité

$$J = a_0 I_f(0) + \cdots + a_n I_f(n).$$

La trascendance de π est obtenu de façon similaire, en utilisant l'inégalité d'Euler.

Référence. — A. Baker, *Transcendental number theory* (§§1.2–1.3). Cambridge University Press, London-New York, 1975. x+147 pp.

4. Formes linéaires de logarithmes

Le but de cet exposé est de présenter l'énoncé du théorème de Baker ainsi que ses applications. Le résultat de Baker est une généralisation vaste du théorème de Gel'fond-Schneider (1934) qui affirme que, si $\alpha \neq 1, 0$ est un nombre algébrique et si $\beta \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, alors α^β est un nombre transcendant (on peut choisir une valeur abitraire de α^β dans le cas où $\alpha \in \mathbb{C} \setminus \mathbb{R}_+$). Ce résultat peut être interprété comme une indépendance linéaire de logarithmes. En effet, on peut reformuler le théorème de Gel'fond-Schneider comme la suite :

Théorème 4.1. — *Soient a et b deux nombres algébriques non-nuls. Alors $\log(b)/\log(a)$ est ou bien rationel ou bien transcendant, où on a considéré une valeur non-nulle du logarithme complexe $\log(a)$.*

Le résultat de Baker est une version effective, inhomomgène et multidimensionnelle du théorème de Gel'fond-Schneider.

Théorème 4.2 **(Baker)**. — *Soient $\alpha_1, \dots, \alpha_n$ des nombres algébriques non-nuls. Pour tout $j \in \{1, \dots, n\}$, soit λ_j une valeur logarithmique de α_j. On suppose que les nombres $\lambda_1, \dots, \lambda_n$ sont linéairement indépendants sur $\mathbb{Q}$. Alors, pour tout vecteur non-nul $(\beta_0, \dots, \beta_n) \in \overline{\mathbb{Q}}^{n+1} \setminus \{\mathbf{0}\}$, on a*

$$|\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n| > \Big(\max_{1\leqslant j\leqslant n} H(\beta_j)\Big)^{-C},$$

où C est une constante effective qui ne dépend que de n, $(\lambda_1, \dots, \lambda_n)$, et $\max(d(\beta_0), \dots, d(\beta_n))$.

Dans le cas où β_0 est non-nul, la condition d'indépendance linéaire de $(\lambda_1, \dots, \lambda_n)$ sur $\mathbb{Q}$ n'est pas nécessaire.

Parmi de nombreuses applications du théorème de Baker on peut présenter dans l'exposé comme en déduire le théorème de Gel'fond-Schneider puis la transcendance de e^π. Aussi il est bien d'expliquer l'application du théorème de Baker dans le problème des corps quadratiques imaginaires de nomber de classe un.

Théorème 4.3. — *Soit $\mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire, où d est un entier positif sans facteur carré. Alors le nombre de classe de $\mathbb{Q}(\sqrt{-d})$ est 1 si et seulement si $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.*

Il est souhaitable que l'orateur rappelle quelques notions basiques comme par exemple hauteur naïve de nombre algébrique, corps quadratiques, nombre de classe etc.

Référence. — A. Baker, *Transcendental number theory* (§§2.1–2.2, 5.1–5.4). Cambridge University Press, London-New York, 1975. x+147 pp.

5-6. Démonstration du théorème de Baker

Ces deux exposés sont consacrés à la démonstration du théorème de Baker annoncé dans l'exposé précédent. L'orateur peut choisir de commencer par la démonstration de la version qualitative du théorème et expliquer ensuite la minoration de la forme linéaire de logarithme si le temps permet. Plus précisément, on présente la démonstration du résultat suivant.

***Théorème 5.4* (Baker).** — *Soient $\alpha_1, \dots, \alpha_n$ des nombres algébriques non-nuls. Pour tout $j \in \{1, \dots, n\}$, soit λ_j une valeur logarithmique de α_j. Si les nombres $\lambda_1, \dots, \lambda_n$ sont linéairement indépendants sur $\mathbb{Q}$, alors $1, \lambda_1, \dots, \lambda_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.*

La stratégie de la théorème est de raisonner par l'absurde. On suppose qu'il existe des nombres algébriques $\beta_0, \dots, \beta_n$ qui ne sont pas tous nuls tels que

$$\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n = 0.$$

Sans perte de généralité, on peut supposer $\beta_n = -1$. Comme $\lambda_1, \dots, \lambda_n$ sont linéairement indépendants sur $\mathbb{Q}$, les fonctions $z, e^{\lambda_1 z}, \dots, e^{\lambda_n z}$ sont algébriquement indépendants. Le point clé de la démonstration est de construire un polynôme auxiliaire $P \in \mathbb{Z}[X_0, \dots, X_n]$ qui est homomgène de degré N (où N est un paramètre entier $\geqslant 1$) de telle sorte que la fonction

$$F(z) = P(z, e^{\lambda_1 z}, \dots, e^{\lambda_n z})$$

possède beaucoup de zéros dans $\mathbb{Z}$ avec de grandes multiplicités. On conclut par trouver une majoration convenable pour certaine dérivée à ordre supérieure de la fonction F en des entiers.

La construction du polynôme auxiliaire utilise le lemme de Siegel comme la suite.

***Théorème 5.5* (Lemme de Siegel).** — *Soient $N > M$ deux entiers, et $A = (a_{ij})$ une matrice de taille $M \times N$ à coefficients dans $\mathbb{Z}$. Alors l'équation $Ax = 0$ possède une solution non-nulle $(x_1, \dots, x_N) \in \mathbb{Z}^N$ qui vérifie la condition suivante*

$$\max_{1 \leqslant j \leqslant N} |x_j| \leqslant (N\|A\|_{\sup})^{M/(N-M)},$$

où $\|A\|_{\sup} := \sup_{i,j} |a_{ij}|$.

Ce résultat est un outil fondamental dans les démonstrations diophantiennes pour construire des polynômes auxiliaires. Il sera réutilisé dans des exposés à venir pour démontrer le théorème de Roth.

Référence. — A. Baker, *Transcendental number theory* (chapitre 3). Cambridge University Press, London-New York, 1975. x+147 pp.
M. Waldschmidt, *Nombres transcendants* (chapitre 8), Lecture Notes in Mathematics **402** Springer-Verlag, 1974, viii+277 pp.

7. Valeurs absolues sur les corps de nombres

Pour comprendre de façon géométrique l'approximation diophantienne, il est bien de considérer les différentes places d'un corps de nombres d'une faćcon symétrique. Le but de cet exposé est de présenter la notion de valeur absolue pour les corps de nombres. Les contenus de cette séance seront utiles pour la présentation de la théorie des hauteurs dans l'exposé à venir.

Soit K un corps. On appelle valeur absolue sur K toute application $|.| : K \to \mathbb{R}_+$ qui vérifie les conditions suivantes :

(1) $|xy| = |x| \cdot |y|$ pour tous $x, y \in K$,

(2) $|x + y| \leqslant |x| + |y|$ pour tous $x, y \in K$,

(3) $|x| = 0$ si et seulement si $x = 0$.

A part des valeurs absolues usuelle, les valeurs absolues sur $\mathbb{Q}$ contiennent aussi les valeurs absolues p-adique $|.|_p$, qui envoie p en p^{-1}. Avec le langage des valeurs absolues, le simple fait $n \in \mathbb{Z} \setminus \{0\} \Rightarrow |n| \geqslant 1$ se traduit comme la formule de produit

Proposition 7.1. — *Si a est un nombre rationnel non-nul, alors*

$$|a| \cdot \prod_p |a|_p = 1.$$

Non-seulement cette égalité marche par tout nombre rationnel non-nul (on n'a donc pas besoin de passer aux entiers), mais encore la formule de produit se généralise naturellement au cas d'un corps de nombres quelconque. Pour cela, il est bien de discuter les prolongement d'une valeur absolue dans une extension finie. Plus précisément, on introduira la notion de *place* pour un corps de nombres K : une place de K est par définition une classe d'équivalence de valeurs absolues non-triviales sur K par rapport à la relation d'équivalence suivante :

$$|.| \sim |.|' \iff |.| \text{ et } |.|' \text{ définissent la même topologie sur } K.$$

On désigne par M_K l'ensemble des places de K. Pour toute place $v \in M_K$, il existe une unique valeur absolue $|.|_v$ dans la classe v, qui prolonge ou bien la valeur absolue usuelle sur $\mathbb{Q}$ ou bien une des valeurs absolues p-adique. Le théorème suivant est la formule de produit pour le corps de nombres K.

Proposition 7.2. — *Pour tout nombre $\alpha \in K^\times$, il n'existe qu'un nombre fini de places $v \in M_K$ telles que $|\alpha|_v \neq 1$. En outre, on a*

$$\prod_{v \in M_K} |\alpha|_v^{[K_v:\mathbb{Q}_v]} = 1,$$

où K_v et $\mathbb{Q}_v$ sont respectivement les complétés de K et $\mathbb{Q}$ par rapport à la valeur absolue $|.|_v$.

Référence. — J. Neukirch, Algebraic number theory (II.1-6), Grundlehren der Mathematischen Wissenschaften **322.** Springer-Verlag, Berlin, 1999, xviii+571 pp.

8. Hauteur

La notion de hauteur est un outil pour mesurer la complexité d'un nombre algébrique ou un vecteur de nombres algébriques. La formule de produit permet de définir une fonction de hauteur sur les points algébrique dans un espace projectif. On peut ainsi se servir des outils de la géométrie algébrique à étudier les problèmes diophantien. Il est sans doute pas possible de présenter la théorie des schémas dans ce groupe de lecture. On se contente de considérer les points de l'espace projectif à valeurs dans un corps. Soit $n \geqslant 1$ un entier. Pour tout corps k, on désigne par $\mathbb{P}^n(k)$ l'espace $k^{n+1} \setminus \{\mathbf{0}\}$ modulo l'action de $k^\times$. Si $(x_0, \ldots, x_n)$ est un point dans $k^{n+1} \setminus \{\mathbf{0}\}$, on désigne par $(x_0 : \cdots : x_n)$ sa classe dans $\mathbb{P}^n(k)$. Si k'/k est une extension de corps, alors l'inclusion $k^{n+1} \to k'^{n+1}$ induit naturellement une application injective $\mathbb{P}^n(k) \to \mathbb{P}^n(k')$.

Si K est un corps nombres et si $x = (x_0 : \cdots : x_n)$ est un point dans $\mathbb{P}^n(K)$, on désigne par $H_K(x)$ le nombre

$$H_K(x) := \prod_{v \in M_K} \max(\|x_0\|_v, \ldots, \|x_n\|_v).$$

Dans le cas où $K = \mathbb{Q}$, on peut toujours écrire un point $x \in \mathbb{P}^n(\mathbb{Q})$ sous la forme $(x_0 : \cdots : x_n)$, où $x_0, \ldots, x_n$ sont des entiers premiers entre eux. On a

$$H_{\mathbb{Q}}(x) = \max(|x_0|, \ldots, |x_n|).$$

Si x est un point dans $\mathbb{P}^n(K)$ et si K' est une extension finie de K, on peut considérer x comme un point dans $\mathbb{P}^n(K')$. On a la relation $H_{K'}(x) = H_K(x)^{[K':K]}$. Cela nous permet de définir la version absolue de la fonction de hateur en mettant $H(x) = H_K(x)^{1/[K:\mathbb{Q}]}$. La hauteur absolue ne dépend pas du choix du corps de nombres K tel que x soit dans $\mathbb{P}^n(K)$. Ainsi on obtient une fonction de hauteur de $\mathbb{P}^n(\overline{\mathbb{Q}})$ vers $\mathbb{R}_+$.

Le théorème de finitude de Northcott est un résultat important dans la théorie de hauteur.

Théorème 8.1. — *Soient $n \geqslant 1$ et $D \geqslant 1$ deux entiers, et $B > 0$ un nombre réel. Le ensemble*

$$\{x \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid [\mathbb{Q}(x) : \mathbb{Q}] \leqslant D,\ H(x) \leqslant B\}$$

est fini.

La hauteur des polynômes fait partie aussi du but de l'exposé. La relation entre la hauteur naïve et la hauteur de Mahler est particulièrement intéressante.

Référence. — M. Hindry, J. Silverman, Diophantine geometry, An introduction (B.1-3, B.7). Graduate Texts in Mathematics **201.** Springer-Verlag, New York, 2000, xiv+558 pp.

9. Introduction au théorème de Roth

Le but de cet exposé est de présenter l'énoncé du théorème de Roth et quelques outils préparatoire pour la démonstration de ce théorème. Le théorème de Roth affirme que l'exposant d'approximation de tout nombre réel algébrique irrationnel est exactement 2.

Théorème 9.1 **(Roth)**. — *Si α est un nombre algébrique irrationnel, alors pour tout $\varepsilon > 0$ il n'y a qu'un nombre fini de couples d'entiers (p, q) tels que $q \neq 0$ et que*

$$\left|\frac{p}{q} - \alpha\right| \leqslant \frac{1}{q^{2+\varepsilon}}$$

À l'aide des places introduites dans l'exposé **7.**, on peut énoncer une version généralisée du théorème de Roth, qui a une forme plus symétrique.

Théorème 9.2. — *Soient K un corps de nombres et S une famille finie de places de K. Pour chaque place $v \in S$, on choisit un prolongement de $|.|_v$ sur $\overline{\mathbb{Q}}$. Pour toute corps de nombres $K' \supset K$, tout $\alpha \in K'$ et tout $\varepsilon > 0$, il n'y a qu'un nombre fini d'éléments $\beta \in K$ tels que*

$$\prod_{v \in S} \min\{|\beta - \alpha|_v^{[K'_v : \mathbb{Q}_v]}, 1\} \leqslant \frac{1}{H_K(\beta)^{2+\varepsilon}}$$

Le passage à la forme initiale du théorème de Roth provient d'une idée de Mahler et devrait être expliqué dans l'exposé.

Tout comme dans la démonstration du théorème de Baker, il faut construire des polynôme auxiliaires multi-variés qui s'annulent à un grand ordre en $(\alpha, \ldots, \alpha)$. Mais ici il faut adopter un traitement biaisé pour les différentes variables des polynômes auxiliares. Pour cela on introduit dans cet exposé la notion d'indice pour les polynômes à plusieurs variables.

Soient $m \geqslant 1$ un entier et $\boldsymbol{r} = (r_1, \ldots, r_m)$ un vecteur dans $]0, +\infty[^m$. Pour tout élément $\boldsymbol{j} = (j_1, \ldots, j_m) \in \mathbb{N}^m$, on désigne par $\mathrm{ind}_{\boldsymbol{r}}(\boldsymbol{j})$ le nombre

$$\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m},$$

appelé l'indice de $\boldsymbol{j}$ par rapport à $\boldsymbol{r}$. Si k est un corps et si P est un polynôme dans $k[X_1, \ldots, X_m]$ est un polynôme, pour tout $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in k^m$, on désigne par $\mathrm{ind}_{\boldsymbol{r},\boldsymbol{\alpha}}(P)$ le plus petit indice (par rapport à $\boldsymbol{r}$) de vecteurs $\boldsymbol{j} = (j_1, \ldots, j_m) \in \mathbb{N}^m$ tels que $\partial_{\boldsymbol{j}} P(\boldsymbol{\alpha}) \neq 0$, où

$$\partial_{\boldsymbol{j}} P := \frac{1}{j_1! \cdots j_m!} \frac{\partial^{j_1 + \cdots + j_m} P}{\partial X_1^{j_1} \cdots \partial X_m^{j_m}}.$$

Plusieurs propriétés de la fonction d'indice seront expliquées dans cet exposé, notamment une estimation du comptage de vecteur à indices bornés.

Lemme 9.3. — *Soit $\boldsymbol{r} = (r_1, \ldots, r_m)$ un vecteur dans $]0, +\infty[^m$ et $\varepsilon \in]0, 1/2[$, alors le nombre des vecteurs $\boldsymbol{j} = (j_1, \ldots, j_m) \in \mathbb{N}^m$ qui vérifient*

$$0 \leqslant j_1 \leqslant r_1, \ \ldots, \ 0 \leqslant j_m \leqslant r_m, \ \mathrm{ind}_{\boldsymbol{r}}(\boldsymbol{j}) \leqslant \Big(\frac{1}{2} - \varepsilon\Big) m$$

est majoré par $(r_1 + 1) \cdots (r_m + 1) e^{-\varepsilon^2 m/4}$.

Référence. — M. Hindry, J. Silverman, Diophantine geometry, An introduction (D.2-3). Graduate Texts in Mathematics **201.** Springer-Verlag, New York, 2000, xiv+558 pp.

10-11. Démonstration du théorème de Roth

Le but de ces deux exposés est de présenter la démonstration du théorème de Roth. Prenons les notations du théorème 9.2. Le point clé est de construire un polynôme auxiliaire qui possède un grand indice en $(\alpha, \ldots, \alpha)$ et dont la hauteur est contrôlée en fonction de α. On raisonne toujours par l'absurde en supposant qu'il existe une infinité de β qui donnent des approximations assez précises de α comme demandée. D'après le théorème de Northcott, on peut construire une suite $(\beta_j)_{j \geqslant 1}$ qui donnent des bonnes approximations et telle que la hauteur de β_j est beaucoup plus grande que celle de β_{j-1}. À l'aide du lemme de Siegel, on peut construire un polynôme auxiliaire $P \in \mathbb{Z}[X_1, \ldots, X_m]$ (dont la hauteur est contrôlée) qui s'annule à un grand ordre en $(\alpha, \ldots, \alpha)$, et donc prend une valeur petite en $(\beta_1, \ldots, \beta_m)$, et donc s'annule à un ordre assez grand en $(\beta_1, \ldots, \beta_m)$. On conclure par le lemme de Roth comme la suite.

Lemme 9.4. — *Soient $m \geqslant 1$ un entier, $\eta > 0$ et $\boldsymbol{r} = (r_j)_{j=1}^m$ une famille d'entiers tels que $r_{j+1}/r_j \leqslant \eta^{2^{m-1}}$ pour tout j. Si $P \in \overline{\mathbb{Q}}[X_1, \ldots, X_m]$ est un polynôme tel que $\deg_{X_j}(P) \leqslant r_j$ et que*

$$\eta^{2^{m-1}} \min_{1 \leqslant j \leqslant m} \{r_j \log H(\beta_j)\} \geqslant \log H(P) + 2mr_1,$$

alors $\mathrm{ind}_{\boldsymbol{r},\boldsymbol{\beta}}(P) \leqslant 2m\eta$.

Référence. — M. Hindry, J. Silverman, Diophantine geometry, An introduction (D.4-7). Graduate Texts in Mathematics **201.** Springer-Verlag, New York, 2000, xiv+558 pp.

---

15 janvier 2013

Huayi Chen, • *E-mail :* huayi.chen@ujf-grenoble.fr
Url : http://www-fourier.ujf-grenoble.fr/~huayi