Théorème de Roth

François-Régis André et Thibaut Verron,
sous la direction d'Alena Pirutka.

31 juin 2010

Nous tenons à remercier chaleureusement Alena Pirutka pour sa disponibilité, son aide et ses explications tout au long de ce travail.

Table des matières

1 Introduction

Le but de cet exposé de maîtrise est de démontrer un théorème dû à Roth, traitant des approximations rationnelles de nombres réels. Le premier résultat à ce sujet a été obtenu séparément par Dirichlet et Legendre :

Théorème (Dirichlet, Legendre)**.** *Soit α un nombre réel irrationnel. L'inéquation*

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

a une infinité de solutions rationnelles $\frac{p}{q}$ distinctes.

En 1844, le mathématicien Liouville a formulé un théorème limitant la précision des approximations rationnelles :

Théorème (Liouville)**.** *Soit α un nombre irrationnel, algébrique de degré d. Il existe une constante c telle que pour tout rationnel $\frac{p}{q}$, on ait*

$$\left|\frac{p}{q} - \alpha\right| > \frac{c}{q^d}.$$

La question naturelle que l'on se pose à la lecture de ces théorèmes est « quelle est la précision limite que l'on peut atteindre ? ». Il a fallu attendre 1955 pour que Roth y apporte une réponse :

Théorème (Roth)**.** *Soit $\alpha \in \mathbb{R}$, algébrique et irrationnel. Alors pour tout $\varepsilon > 0$, il n'existe qu'un nombre fini de solutions à l'inéquation*

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

Ce théorème a valu à Roth la médaille Fields en 1958, et fournit un bon critère de transcendance des nombres réels.

La preuve suit un schéma de preuve très analogue à celle du théorème de Liouville. Elle utilise des outils provenant de domaines aussi variés que l'algèbre linéaire, tel le lemme de Siegel, ou la théorie des équations différentielles, en particulier des résultats sur les déterminants wronskiens.

Pour conclure, nous énoncerons un théorème dû à Siegel et portant sur le nombre de points entiers d'une variété algébrique. La démonstration de ce théorème utilise le théorème des sous-espaces de Schmidt, qui généralise le théorème de Roth. Il est à noter qu'il existe également une démonstration utilisant uniquement le lemme de Roth.

2 Le théorème de Liouville

Théorème 1 (Liouville)**.** *Soit $\alpha \in \mathbb{R}$, irrationnel et algébrique de degré d sur $\mathbb{Q}$. Alors il existe une constante $c(\alpha)$ telle que pour tout nombre rationnel $\frac{p}{q}$,*

$$\left|\frac{p}{q} - \alpha\right| > \frac{c(\alpha)}{q^d}.$$

Démonstration. La démonstration se fait en 4 étapes :

1. Choisir un polynôme irréductible $f \in \mathbb{Z}[X]$ qui annule α. Ce polynôme est unique si on impose que ses coefficients soient premiers entre eux et que le coefficient dominant soit positif.
2. Montrer que $f\left(\frac{p}{q}\right) \neq 0$.
3. En déduire que $\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$.
4. Montrer que $\left|f\left(\frac{p}{q}\right)\right| \leq b(\alpha)\left|\frac{p}{q} - \alpha\right|$ si $|p/q - \alpha| \leq 1$.

Étape 1 : immédiate. Notons que f est de degré d.

Étape 2 : si f annule p/q, f est divisible par $X - p/q$, et alors soit f n'est pas irréductible, soit f est de degré 1 et α n'est pas irrationnel.

Étape 3 : le nombre $q^d f\left(\frac{p}{q}\right)$ est entier puisque f est de degré d, et il est non nul d'après ce qui précède. Puisque 1 est le plus petit entier positif, on obtient immédiatement la minoration souhaitée.

Étape 4 : écrivons le développement en série de Taylor de f au voisinage de α :

$$f(X) = f(\alpha) + \sum_{i=1}^{d} a_i (X - \alpha)^i.$$

Or $f(\alpha) = 0$, ce qui permet d'écrire

$$|f(X)| \leq |X - \alpha| \sum_{i=1}^{d} |a_i| \, |X - \alpha|^i.$$

Puisque $|p/q - \alpha| \leq 1$, on a une majoration

$$\left|f\left(\frac{p}{q}\right)\right| \leq \left|\frac{p}{q} - \alpha\right| \sum_{i=1}^{d} |a_i|.$$

On obtient bien la majoration cherchée avec $b(\alpha) = \sum_{i=1}^{d} |a_i|$.

On peut alors conclure :

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{1}{b(\alpha)} f\left(\frac{p}{q}\right) \geq \frac{1}{q^d b(\alpha)} > \frac{1}{q^d \cdot 2b(\alpha)}.$$

On obtient alors la constante $c(\alpha) = \min\left(1, \frac{1}{2b(\alpha)}\right)$. □

3 Le théorème de Roth

Théorème 2 (Roth)**.** *Soit $\alpha \in \mathbb{R}$, algébrique et irrationnel. Alors pour tout $\varepsilon > 0$, il n'existe qu'un nombre fini de solutions à l'inéquation*

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

3.1 Schéma de la démonstration

Les étapes principales de la preuve sont au nombre de quatre, comme pour le théorème de Liouville :

1. Soit $\varepsilon > 0$ et m approximations rationnelles $p_1/q_1, \ldots, p_m/q_m$ telles que pour tout i,
$$\left|\frac{p_i}{q_i} - \alpha\right| < \frac{1}{q_i^{2+\varepsilon}}.$$
On prend $f \in \mathbb{Z}[X_1, \ldots, X_m]$ tel que $f(\alpha, \ldots, \alpha) = 0$, et vérifiant d'autres « bonnes propriétés ».
2. On montre que sous ces conditions, $f(p_1/q_1, \ldots, p_m/q_m) \neq 0$.
3. On en déduit une minoration de $|f(p_1/q_1, \ldots, p_m/q_m)|$.
4. On trouve une majoration de $|f(p_1/q_1, \ldots, p_m/q_m)|$ qui entre en contradiction avec la minoration précédente, pour m assez grand.

Soit $f \in \mathbb{Z}[X_1, \ldots, X_m]$, qui annule $(\alpha, \ldots, \alpha)$. On note $(d_1, \ldots, d_m)$ son multi-degré. On cherche des conditions suffisamment fortes pour que les étapes suivantes de la preuve soient réalisables. En particulier, il faut que le polynôme dépende suffisamment de α pour que la preuve ait un sens. Ainsi, on cherche à éviter des polynômes comme $X_1 - X_2$ ou $4X_1 - 2X_2 - 2X_4$ qui annuleraient tous les m-uplets de la forme $(x, \ldots, x)$. Un moyen simple pour écarter ces problèmes est d'imposer $d_1 \gg d_2 \gg \cdots \gg d_m$.

De plus, pour obtenir une majoration assez efficace, la simple notion de degré ne suffirait pas. Il faut introduire l'indice.

Définition 1 (Indice d'un polynôme)**.** Soit $f \in \mathbb{C}[X_1, \ldots, X_m]$ non nul, de multi-degré $(d_1, \ldots, d_m)$, et $(\alpha_1, \ldots, \alpha_m) \in \mathbb{C}^m$. Écrivons le développement en série de Taylor de f au voisinage de $(\alpha_1, \ldots, \alpha_m)$:

$$f(X_1, \ldots, X_m) = \sum_{I \geq 0} b_I (X_1 - \alpha_1)^{i_1} \cdots (X_m - \alpha_m)^{i_m} \text{ , où } I = (i_1, \ldots, i_m).$$

On pose alors :

$$\operatorname{ind}(f, \alpha_1, \ldots, \alpha_m, d_1, \ldots, d_m) = \min\left\{ \sum_{j=1}^{m} \frac{i_j}{d_j} \mid I \geq 0 \text{ et } b_I \neq 0 \right\},$$

appelé *indice* de f relativement à $(\alpha_1, \ldots, \alpha_m, d_1, \ldots, d_m)$.

Pour obtenir une bonne majoration à l'étape 4, on aura besoin d'un indice t_m de f en $(\alpha, \ldots, \alpha)$ élevé, et d'une relation entre les q_i et d_i. On impose $d_i \simeq \frac{A}{\log(q_i)}$ pour un grand entier A. Soit $q \simeq q_i^{d_i}$.

Dès lors, si on note $M_I = (X_1 - \alpha_1)^{i_1} \cdots (X_m - \alpha_m)^{i_m}$, où $I = (i_1, \ldots, i_m)$, on a

$$\begin{aligned}\left|M_I\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right)\right| &\leq \frac{1}{q_1^{(2+\varepsilon)i_1}} \cdots \frac{1}{q_m^{(2+\varepsilon)i_m}} \\ &\leq \frac{1}{q_1^{(d_1(2+\varepsilon))i_1/d_1}} \cdots \frac{1}{q_m^{(d_m(2+\varepsilon))i_m/d_m}} \\ &\leq \frac{1}{q^{(2+\varepsilon)(i_1/d_1+\cdots+i_m/d_m)}} \\ &\leq \frac{1}{q^{(2+\varepsilon)t_m}}.\end{aligned}$$

Définition 2 (Hauteur d'un polynôme)**.** La décomposition de f en série de Taylor s'écrit

$$f = \sum_{0 \leq I \leq d} b_I M_I.$$

On définit la *hauteur* de f par

$$H(f) = \sup(|b_I|).$$

Soit N le nombre total de monômes M_I avec un coefficient b_I non nul ($N \leq \prod_{i=1}^{d}(d_i + 1)$), on a la majoration

$$\left|f\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right)\right| \leq NH(f)\frac{1}{q^{(2+\varepsilon)t_m}}. \tag{1}$$

D'autre part, si on suppose l'étape 2 réalisée, de même que pour le théorème de Liouville, la minoration obtenue à l'étape 3 sera

$$\left|f\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right)\right| \geq \frac{1}{\prod_{i=1}^{m} q_i^{d^i}} \simeq \frac{1}{q^m}. \tag{2}$$

Pour obtenir une contradiction, on veut donc

$$t_m \geq \frac{m}{2+\varepsilon},$$

et il faudra s'assurer que les valeurs de N et $H(f)$ ne sont pas trop importantes.

On va donc commencer par construire un polynôme f tel que $H(f)$ soit suffisamment petit pour qu'il suffise de fixer l'indice t_m.

3.2 Étape 1 : construction du polynôme

On remarque que pour démontrer le théorème de Roth, on peut se limiter au cas des entiers algébriques. En effet, soit α un nombre algébrique de degré d sur $\mathbb{Q}$. On note $Q = a_0X^d + \cdots + a_d \in \mathbb{Z}[X]$ son polynôme minimal sur $\mathbb{Q}$. On considère alors $\beta = a_0\alpha$. On a $Q(\alpha) = 0$, soit :

$$\begin{aligned} 0 &= a_0^{d-1}Q(\alpha) \\ &= R(\beta) \text{ où } R = X^d + a_1X^{d-1} + a_2a_0X^{d-2} + \cdots + a_da_0^{d-1} \in \mathbb{Z}[X], \text{ unitaire.} \end{aligned}$$

Donc β est un entier algébrique. Si on suppose le théorème de Roth vrai pour les entiers algébriques, on sait qu'il n'existe qu'un nombre fini de solutions à l'inéquation :

$$\left|\frac{p}{q} - \beta\right| \leq \frac{1}{q^{2+\varepsilon}}.$$

Soit un rationnel p/q solution de

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

Le rationnel $a_0^{d-1}p/q$ vérifie

$$\left|\frac{a_0^{d-1}p}{q} - \beta\right| \leq \frac{a_0^{d-1}}{q^{2+\varepsilon}}.$$

Soit $\varepsilon' = \log_q\left(\frac{q^\varepsilon}{a_0^{d-1}}\right)$. On a :

$$\forall q' > q, q'^{\varepsilon-\varepsilon'} > q^{\varepsilon-\varepsilon'} = a_0^{d-1},$$

donc pour tout rationnel p'/q' solution de

$$\left|\frac{p'}{q'} - \alpha\right| \leq \frac{1}{q'^{2+\varepsilon}} \text{ avec } q' > q,$$

le rationnel $a_0^{d-1}p'/q'$ vérifie

$$\left|\frac{a_0^{d-1}p'}{q'} - \beta\right| \leq \frac{a_0^{d-1}}{q'^{2+\varepsilon}} \leq \frac{1}{q'^{2+\varepsilon'}}.$$

Cette équation n'a qu'un nombre fini de solutions par hypothèse, donc il n'existe aussi qu'un nombre fini de solutions rationnelles à

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

On suppose donc dorénavant que α est un entier algébrique, irrationnel donc de degré $d \geq 2$.

3.2.1 Le lemme d'indice

Lemme 3 (Lemme d'indice)**.** *Soient η un réel positif et m un entier tels que*

$$e^{3\eta^2 m/16} > 2d.$$

Soient $(d_1, \ldots, d_m)$ des entiers positifs.
Alors il existe un polynôme $P \in \mathbb{Z}[X_1, \ldots, X_m]$ tel que :

- *Le multi-degré de P est plus petit que $(d_1, \ldots, d_m)$.*
- *L'indice de P en $(\alpha, \ldots, \alpha)$ vérifie*

$$ind(P, \alpha, \ldots, \alpha, d_1, \ldots, d_m) \geq \frac{m}{2}(1 - \eta).$$

- *Il existe une constante B ne dépendant que de α telle que*

$$|P| \leq B^{d_1 + \cdots + d_m}$$

où $|P|$ est le maximum des valeurs absolues des coefficients de P.

3.2.2 Résultats préliminaires

La démonstration utilise le lemme de Siegel, un outil d'algèbre linéaire permettant de borner les solutions d'un système d'équations linéaires.

Lemme 4 (Lemme de Siegel)**.** *Soit un système de M équations à N inconnues ($M < N$) :*

$$\begin{array}{ccccccc} a_{1,1}X_1 & + & \cdots & + & a_{1,N}X_N & = & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ a_{M,1}X_1 & + & \cdots & + & a_{M,N}X_N & = & 0 \end{array}$$

Supposons que $a_{i,j} \in \mathbb{Z}$ et $|a_{i,j}| < A$ pour tous i, j. Alors il existe une solution $(x_1, \ldots, x_N)$ du système telle que pour tout j,

$$|x_i| < 1 + (NA)^{\frac{M}{N-M}}.$$

Démonstration. Pour un $k-$uplet $\mathbf{x} = (x_1, \ldots, x_k)$, on note $|\mathbf{x}| = \sup |x_i|$.

Pour tout nombre réel a, on note $a^+ = \max(a, 0)$ et $a^- = \max(-a, 0)$, de sorte que $a = a^+ - a^-$ et $|a| = a^+ + a^-$.

Soit L_i la forme linéaire définie par

$$L_i(\mathbf{x}) = \sum_{j=1}^{N} a_{i,j} x_j,$$

pour tout $i \in \{1, \ldots, M\}$. On note aussi

$$L_i^+ = \sum_{j=1}^{N} a_{i,j}^+, \; L_i^- = \sum_{j=1}^{N} a_{i,j}^- \text{ et } |L_i| = L_i^+ + L_i^-.$$

On va démontrer le lemme de Siegel à l'aide du théorème des tiroirs. Soit B un entier et $\mathbf{t} \in \mathbb{Z}^N$. Si $0 \leq \mathbf{t} \leq B$ (c'est-à-dire si $\forall\, 1 \leq i \leq M, 0 \leq t_i \leq B$), on a

$$-L_i^- B \leq L_i(\mathbf{t}) \leq L_i^+ B.$$

Le nombre de vecteurs à coordonnées entières dans le pavé $\prod_{i=1}^M \left[-L_i^- B, L_i^+ B\right]$ vaut

$$\prod_{i=1}^{M} (L_j^+ B + L_i^- B + 1) = \prod_{i=1}^{M} (|L_i|\, B + 1),$$

alors que le nombre de vecteurs à coordonnées entières satisfaisant l'hypothèse initiale $0 \leq \mathbf{t} \leq B$ est $(B+1)^N$.

Si on peut trouver B tel que

$$(B+1)^N > \prod_{i=1}^{M} (|L_i|\, B + 1),$$

le principe des tiroirs fournira deux vecteurs distincts $\mathbf{t}_1$ et $\mathbf{t}_2$ tels que pour tout i, $L_i(\mathbf{t}_1) = L_i(\mathbf{t}_2)$, et donc le vecteur $\mathbf{t} = \mathbf{t}_1 - \mathbf{t}_2$ sera une solution du système, avec $|\mathbf{t}| \leq B$.

Il reste à vérifier que la majoration proposée dans l'énoncé du lemme fournit bien un B suffisamment grand pour appliquer le théorème des tiroirs. On pose $B = \left[(NA)^{\frac{M}{N-M}}\right]$. Alors

$$B + 1 > (NA)^{\frac{M}{N-M}},$$

soit

$$(B+1)^N = (B+1)^M (B+1)^{N-M} > (B+1)^M (NA)^M.$$

On a les inégalités $1 \leq NA$ et $|L_i| \leq NA$, soit :

$$(B+1)^N > ((B+1)(NA))^M \geq \prod_{i=1}^{M} (|L_i|\, B + 1).$$

□

On utilisera également le lemme suivant qui permet de borner les coefficients d'une décomposition dans une base.

Lemme 5. *Soit α un entier algébrique de degré d sur $\mathbb{Q}$ et soit*

$$Q(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$$

son polynôme minimal. On note

$$|Q| = \sup\{|a_i| \mid 1 \leq i \leq d\},$$

et on rappelle que pour tout $l > 0$, on peut écrire la décomposition de α^l dans la base $(1, \ldots, \alpha^{d-1})$:

$$\alpha^l = \sum_{k=1}^{d} a_k^{(l)} \alpha^{d-k}.$$

On peut choisir les coefficients pour être des entiers vérifiant l'inégalité

$$\left|a_i^{(l)}\right| \leq (|Q| + 1)^l .$$

Démonstration. On raisonne par récurrence sur l. Le résultat est clair pour $0 \leq l < d$. Si le lemme est vrai pour α^l, alors :

$$\begin{aligned}
\alpha^{l+1} &= \alpha \cdot \alpha^l \\
&= \alpha \sum_{k=1}^{d} a_k^{(l)} \alpha^{d-k} \\
&= a_1^{(l)} \alpha^d + \sum_{k=2}^{d} a_k^{(l)} \alpha^{d-k} \\
&= a_1^{(l)} \sum_{k=1}^{d} -a_k \alpha^{d-k} + \sum_{k=2}^{d} a_k^{(l)} \alpha^{d-k} \text{ car } Q(\alpha) = 0 \\
&= \sum_{k=1}^{d} \left(-a_1^{(l)} a_k + a_{k+1}^{(l)}\right) \alpha^{d-k} \text{ avec la convention } a_{d+1}^{(l)} = 0.
\end{aligned}$$

On en déduit

$$a_i^{(l+1)} = -a_1^{(l)} a_i + a_{i+1}^{(l)}.$$

On a alors :

$$\begin{aligned}
\left|a_i^{(l+1)}\right| &\leq \left|a_1^{(l)} a_i\right| + \left|a_{i+1}^{(l)}\right| \leq \max\left\{\left|a_1^{(l)}\right|, \left|a_{i+1}^{(l)}\right|\right\} \cdot (|a_i| + 1) \\
&\leq (|Q| + 1)^l (|Q| + 1) \text{ par hypothèse de récurrence} \\
&\leq (|Q| + 1)^{l+1} .
\end{aligned}$$

□

3.2.3 Démonstration du lemme d'indice

On revient à présent à la preuve du lemme 3. On écrit

$$P(X_1, \ldots, X_m) = \sum_{j_1=0}^{d_1} \cdots \sum_{j_m=0}^{d_m} p_{j_1,\ldots,j_m} X_1^{j_1} \cdots X_m^{j_m},$$

où l'on veut déterminer les coefficients $p_{j_1,\ldots,j_m}$. Le nombre de ces coefficients est

$$N = (d_1 + 1) \cdots (d_m + 1).$$

Pour tout $m-$uplet $(i_1, \ldots, i_m)$, on note

$$P_{i_1,\ldots,i_m} = \frac{1}{i_1! \cdots i_m!} \frac{\partial^{i_1+\cdots+i_m} P}{\partial X_1^{i_1} \cdots \partial X_m^{i_m}}.$$

Explicitement, on a :

$$P_{i_1,\ldots,i_m} = \sum_{j_1=0}^{d_1} \cdots \sum_{j_m=0}^{d_m} p_{j_1,\ldots,j_m} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} X_1^{j_1-i_1} \cdots X_m^{j_m-i_m}.$$

Soit $K = \mathbb{Q}(\alpha)$, on sait que $[K : \mathbb{Q}] = d$. En particulier, pour tout $l > 0$, on peut écrire la décomposition de α^l dans la base $(1, \ldots, \alpha^{d-1})$:

$$\alpha^l = \sum_{k=1}^{d} a_k^{(l)} \alpha^{d-k}. \tag{3}$$

Calculons la valeur de $P_{i_1,\ldots,i_m}$ en $(\alpha, \ldots, \alpha)$:

$$\begin{aligned}
&P_{i_1,\ldots,i_m}(\alpha, \ldots, \alpha) \\
&\quad = \sum_{j_1=0}^{d_1} \cdots \sum_{j_m=0}^{d_m} p_{j_1,\ldots,j_m} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} \alpha^{j_1-i_1+\cdots+j_m-i_m} \\
&\quad = \sum_{j_1=0}^{d_1} \cdots \sum_{j_m=0}^{d_m} p_{j_1,\ldots,j_m} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} \sum_{k=1}^{d} a_k^{(j_1-i_1+\cdots+j_m-i_m)} \alpha^{d-k} \\
&\quad = \sum_{k=1}^{d} \left(\sum_{j_1=0}^{d_1} \cdots \sum_{j_m=0}^{d_m} p_{j_1,\ldots,j_m} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} a_k^{(j_1-i_1+\cdots+j_m-i_m)} \right) \alpha^{d-k}.
\end{aligned}$$

Si on veut $P_{i_1,\ldots,i_m}(\alpha, \ldots, \alpha) = 0$, toutes les parenthèses doivent valoir 0, c'est-à-dire que les $p_{j_1,\ldots,j_m}$ doivent satisfaire les d équations linéaires :

$$\sum_{j_1=0}^{d_1} \cdots \sum_{j_m=0}^{d_m} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} a_k^{(j_1-i_1+\cdots+j_m-i_m)} p_{j_1,\ldots,j_m} = 0. \tag{4}$$

La condition sur l'indice impose que $P_{i_1,\ldots,i_m}(\alpha, \ldots, \alpha) = 0$ pour tous les $m-$uplets $(i_1, \ldots, i_m)$ tels que

$$\frac{i_1}{d_1} + \cdots + \frac{i_m}{d_m} \leq \frac{m}{2}(1 - \eta).$$

Soit I l'ensemble des tels $m-$uplets.

$$\begin{aligned}
\#I &= \sum_{(i_1,\dots,i_m)\in I} 1 \\
&\leq \sum_{(i_1,\dots,i_m)\in I} \underbrace{\exp\underbrace{\left[\frac{\eta}{2}\left(\frac{m}{2}-\frac{\eta m}{2}-\frac{i_1}{d_1}-\cdots-\frac{i_m}{d_m}\right)\right]}_{\geq 0}}_{\geq 1} \\
&\leq \sum_{i_1=0}^{d_1}\cdots\sum_{i_m=0}^{d_m}\exp\left[\frac{\eta}{2}\left(\frac{m}{2}-\frac{\eta m}{2}-\frac{i_1}{d_1}-\cdots-\frac{i_m}{d_m}\right)\right] \\
&= \exp\left(-\frac{\eta^2 m}{4}\right)\sum_{i_1=0}^{d_1}\cdots\sum_{i_m=0}^{d_m}\exp\left[\frac{\eta}{2}\left(\frac{m}{2}-\frac{i_1}{d_1}-\cdots-\frac{i_m}{d_m}\right)\right] \\
&= \exp\left(-\frac{\eta^2 m}{4}\right)\prod_{h=1}^{m}\left(\sum_{i=0}^{d_h}\exp\left(\frac{\eta}{2}\left(\frac{1}{2}-\frac{i}{d_h}\right)\right)\right).
\end{aligned}$$

Pour $|t|\leq 1$, on a $e^t \leq 1+t+t^2$, ce qui permet de majorer les sommes :

$$\begin{aligned}
\sum_{i=0}^{d_h}\exp\left(\frac{\eta}{2}\left(\frac{1}{2}-\frac{i}{d_h}\right)\right) &\leq \sum_{i=0}^{d_h}\left(1+\frac{\eta}{2}\left(\frac{1}{2}-\frac{i}{d_h}\right)+\frac{\eta^2}{4}\left(\frac{1}{2}-\frac{i}{d_h}\right)^2\right) \\
&= \sum_{i=0}^{d_h}\left[\left(1+\frac{\eta}{4}+\frac{\eta^2}{16}\right)-\left(\frac{\eta}{2}+\frac{\eta^2}{4}\right)\frac{i}{d_h}+\frac{\eta^2}{4}\frac{i^2}{d_h^2}\right] \\
&= (d_h+1)\left(1+\frac{\eta}{4}+\frac{\eta^2}{16}\right)-\frac{d_h+1}{2}\left(\frac{\eta}{2}+\frac{\eta^2}{4}\right) \\
&\quad +\frac{(d_h+1)(2d_h+1)}{6d_h}\frac{\eta^2}{4} \\
&= (d_h+1)\left(1+\frac{\eta^2}{48}+\frac{\eta^2}{24d_h}\right) \\
&\leq (d_h+1)\left(1+\frac{\eta^2}{16}\right) \text{ car } d_h\geq 1.
\end{aligned}$$

Si on reprend le premier calcul, on obtient :

$$\begin{aligned}
\#I &\leq \exp\left(-\frac{\eta^2 m}{4}\right)\prod_{h=1}^{m}\left((d_h+1)\left(1+\frac{\eta^2}{16}\right)\right) \\
&\leq \exp\left(-\frac{\eta^2 m}{4}\right)\prod_{h=1}^{m}\left((d_h+1)\exp\left(\frac{\eta^2}{16}\right)\right) \\
&= \underbrace{(d_1+1)\cdots(d_m+1)}_{=N}\exp\left(-\frac{3\eta^2 m}{16}\right).
\end{aligned}$$

Cela signifie que les coefficients $p_{j_1,\dots,j_m}$ doivent satisfaire M équations linéaires, où

$$M \leq dN \exp\left(-\frac{3\eta^2 m}{16}\right) \leq \frac{N}{2} \text{ par hypothèse sur } m. \tag{5}$$

On cherche à présent à majorer les coefficients de ces équations afin d'appliquer le lemme de Siegel.

Pour ce faire, on applique le lemme 5 à la décomposition (3) : les coefficients du système (4) sont entiers, et on peut les majorer par

$$\left|\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}a_k^{(j_1-i_1+\cdots+j_m-i_m)}\right| \leq 2^{j_1+\cdots+j_m}\left(|Q|+1\right)^{j_1+\cdots+j_m},$$

car $\binom{a}{b}$ est le cardinal de l'ensemble des parties à b éléments de $\{1,\dots,a\}$, et 2^a est le cardinal de l'ensemble des parties de $\{1,\dots,a\}$, ce qui implique $\binom{a}{b} \leq 2^a$. On en déduit

$$\left|\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}a_k^{(j_1-i_1+\cdots+j_m-i_m)}\right| \leq \left(2\left|Q\right|+2\right)^{d_1+\cdots+d_m}.$$

On peut à présent appliquer le lemme de Siegel au système (4) : d'après l'équation (5), on a $M < N$, et on vient d'obtenir une bonne majoration des coefficients. On obtient un polynôme P vérifiant les deux premières conditions, et dont les coefficients $p_{j_1,\dots,j_m}$ sont majorés par :

$$\begin{aligned}
|P| &\leq \left(N\left(2\left|Q\right|+2\right)^{d_1+\cdots+d_m}\right)^{\frac{M}{N-M}} \\
&\leq N\left(2\left|Q\right|+2\right)^{d_1+\cdots+d_m} \text{ car } M \leq \frac{1}{2}N \\
&= (d_1+1)\cdots(d_m+1)\left(2\left|Q\right|+2\right)^{d_1+\cdots+d_m} \\
&\leq 2^{d_1+\cdots+d_m}\left(2\left|Q\right|+2\right)^{d_1+\cdots+d_m} \text{ car } \forall t \geq 1, 2^t \geq (t+1) \\
&\leq B(\alpha)^{d_1+\cdots+d_m}, \text{ par exemple pour } B(\alpha) = 4\left|Q\right|+4.
\end{aligned}$$

Ceci termine la preuve du lemme 3. □

3.3 Étape 2 : le lemme de Roth

Montrer qu'on peut choisir le polynôme f de manière à ne pas s'annuler en $\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)$ est l'étape centrale de la preuve du théorème de Roth, et c'est aussi le passage le plus difficile. Pour y parvenir, on utilise le lemme de Roth, qui permet sous de bonnes hypothèses de majorer l'indice de f relativement à $\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)$.

3.3.1 Résultats préliminaires sur les wronskiens

Avant d'énoncer et de démontrer le lemme de Roth, rappelons quelques résultats sur les déterminants wronskiens qui seront utiles par la suite.

Définition 3 (Wronskien)**.** Soient $f_1, \ldots, f_k$ des fonctions $k-1$ fois dérivables à valeurs réelles. Le *wronskien* de $f_1, \ldots, f_k$ est la fonction

$$\det\left(f_j^{(i-1)}\right)_{1\leq i,j\leq k}.$$

Un résultat classique de la théorie des équations différentielles affirme que si $f_1, \ldots, f_k$ sont des fractions rationnelles, elles sont linéairement indépendantes sur $\mathbb{R}$ si et seulement si leur wronskien n'est pas identiquement nul. Ce résultat se généralise pour les fonctions de plusieurs variables.

Définition 4 (Wronskien généralisé)**.** Soient $\varphi_1, \ldots, \varphi_k$ des fractions rationnelles en $X_1, \ldots, X_m$. On appelle *wronskien généralisé* des φ_j toute fonction de la forme $\det\left(\Delta_i\left(\varphi_j\right)\right)_{1\leq i,j\leq k}$, où Δ_i est un opérateur différentiel d'ordre inférieur à $i-1$.

Lemme 6. *Soient $\varphi_1, \ldots, \varphi_k$ des fractions rationnelles en $X_1, \ldots, X_m$. Alors $\varphi_1, \ldots, \varphi_k$ sont linéairement indépendantes sur $\mathbb{R}$ si et seulement s'il existe un wronskien généralisé qui ne soit pas identiquement nul.*

Démonstration. Le sens réciproque est immédiat, tout wronskien généralisé d'une famille liée de fractions rationnelles est nul, car on retrouve la relation de liaison dans les colonnes de la matrice qui définit le wronskien.

Pour le sens direct, on procède par récurrence sur k. Si $k=1$, l'opérateur Δ_1 est nécessairement multiple de l'identité, et le wronskien généralisé qui vaut φ_1 n'est pas identiquement nul par hypothèse.

On suppose à présent que pour $k \geq 2$, $\varphi_1, \ldots, \varphi_k$ sont k fractions rationnelles à coefficients réels linéairement indépendantes. Soit Φ une fraction rationnelle à coefficients réels. On pose pour $1 \leq i \leq k$:

$$\varphi_i^* = \Phi \cdot \varphi_i.$$

Les règles usuelles de dérivation montrent que tout wronskien généralisé des φ_i^* est une combinaison linéaire de wronskiens généralisés des φ_i, dont les coefficients s'expriment à l'aide de Φ et de ses dérivées partielles. Pour montrer qu'il existe un wronskien généralisé des φ_i non nul, il suffit donc d'en trouver un pour les φ_i^*. En prenant $\Phi = \varphi_1^{-1}$, on se ramène au cas où $\varphi_1 = 1$. Le sous-espace vectoriel E de $\mathbb{R}\left(X_1, \ldots, X_m\right)$ engendré par $\varphi_1, \ldots, \varphi_k$ est de dimension k. Comme φ_1 et φ_2 sont linéairement indépendantes, φ_2 n'est pas constante, donc quitte à renommer les X_i, on peut supposer que $\frac{\partial \varphi_2}{\partial X_1} \neq 0$. Soit F le sous-espace de E des fractions rationnelles $\varphi = c_1\varphi_1 + \ldots + c_k\varphi_k$ telles que :

$$\frac{\partial \varphi}{\partial X_1} = 0.$$

On pose $t = \dim F$. Comme $\varphi_1 \in F$ et $\varphi_2 \notin F$, on a $1 \leq t \leq k-1$. Soit $\psi_1, \ldots, \psi_k$ une base de E telle que $\psi_1, \ldots, \psi_t$ forment une base de F. Par hypothèse de récurrence, il existe des opérateurs différentiels $\Delta_1^*, \ldots, \Delta_t^*$ d'ordres respectivement inférieurs à $0, \ldots, t-1$ tels que :

$$W_1 = \det\left((\Delta_i^* \psi_j)_{1 \leq i,j \leq t}\right) \neq 0.$$

Par ailleurs, le sous-espace engendré par $\psi_{t+1}, \ldots, \psi_k$ et F ont une intersection nulle. On en déduit donc que pour tous réels $c_{t+1}, \ldots, c_k$ non tous nuls :

$$\frac{\partial}{\partial X_1}\left(c_{t+1}\psi_{t+1} + \ldots + c_k \psi_k\right) \neq 0.$$

Les fractions rationnelles $\frac{\partial \psi_{t+1}}{\partial X_1}, \ldots, \frac{\partial \psi_k}{\partial X_1}$ sont donc linéairement indépendantes. Par hypothèse de récurrence, il existe des opérateurs différentiels $\Delta_{t+1}^*, \ldots, \Delta_k^*$ d'ordres respectivement inférieurs à $0, \ldots, k-t-1$ tels que :

$$W_2 = \det\left(\left(\Delta_i^* \frac{\partial \psi_j}{\partial X_1}\right)_{t < i,j \leq k}\right) \neq 0.$$

On définit les opérateurs Δ_i pour $1 \leq i \leq k$ par :

$$\Delta_i = \begin{cases} \Delta_i^* & \text{si } 1 \leq i \leq t \\ \Delta_i^* \frac{\partial}{\partial X_1} & \text{si } t < i \leq k \end{cases}$$

Chaque Δ_i est d'ordre inférieur à $i-1$. On trouve :

$$\det\left(\Delta_i \psi_j\right) = \begin{pmatrix} \Delta_i^* \psi_j & \Delta_i^* \psi_j \\ 0 & \Delta_i^* \frac{\partial \psi_j}{\partial X_1} \end{pmatrix} = W_1 W_2 \neq 0$$

puis

$$\det\left(\Delta_i \varphi_j\right) = \det P \cdot \det\left(\Delta_i \psi_j\right) \neq 0$$

où P désigne la matrice de passage de la base de E $\psi_1, \ldots, \psi_k$ à la base $\varphi_1, \ldots, \varphi_k$. □

3.3.2 Le lemme de Roth

Lemme 7 (Lemme de Roth)**.** *On suppose que $\delta \leq \frac{1}{12}$, et que m est un entier positif. On pose :*

$$\omega = \omega(m, \delta) = 24 \cdot 2^{-m} \left(\frac{\delta}{12}\right)^{2^{m-1}}.$$

On suppose que $d_1, \ldots, d_m$ vérifient :

$$\forall h \in \{1, \ldots, m-1\}\, \omega d_h \geq d_{h+1}.$$

Soient $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ *des rationnels avec* p_h *et* q_h *premiers entre eux vérifiant les conditions :*

$$\forall h \in \{1, \ldots, m\}\, q_h^{d_h} \geq q_1^{d_1} \text{ et } q_h^{\omega} \geq 2^{3m}.$$

On suppose que $f(X_1, \ldots, X_m)$ *est un polynôme à coefficients entiers de degré inférieur à* d_h *par rapport à* X_h *pour* $1 \leq h \leq m$*, de hauteur :* $|f| \leq q_1^{\omega d_1}$.
(On rappelle que si $f = \sum p_{(i_1,\ldots,i_m)} X^{i_1} \cdots X^{i_m}$*, on définit* $|f| = \sup |p_{(i_1,\ldots,i_m)}|$*.)*
Sous ces hypothèses, l'indice de f *en* $(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m})$ *est inférieur à* δ*.*

3.3.3 Démonstration du lemme de Roth

On raisonne par récurrence sur m. Si $m = 1$:
f se met sous la forme :

$$f(X) = \left(X - \frac{p_1}{q_1}\right)^l M(X) = (q_1 X - p_1)^l R(X)$$

où M et R sont des polynômes à coefficients rationnels. Comme f et $(q_1 X - p_1)$ sont à coefficients entiers, R est aussi à coefficients entiers par le lemme de Gauss. Le coefficient dominant de f est donc divisible par q_1^l, donc :

$$q_1^l \leq |f| \leq q_1^{\omega d_1} = q_1^{\delta d_1}.$$

On en déduit que $\frac{l}{d_1} \leq \delta$, et comme l'indice de f relativement à $\left(\frac{p_1}{q_1}; d_1\right)$ est $\frac{l}{d_1}$, on obtient le résultat pour $m = 1$.

On suppose à présent le résultat vrai pour les polynômes à $m-1$ variables.
On décompose f sous la forme :

$$f(X_1, \ldots, X_m) = \sum_{j=1}^{k} \varphi_j(X_1, \ldots, X_{m-1})\, \psi_j(X_m)$$

où les $\varphi_1, \ldots, \varphi_k$ et $\psi_1, \ldots, \psi_k$ sont des polynômes à coefficients rationnels. On prend une telle décomposition avec k minimal. On a donc : $k \leq d_m + 1$. Les polynômes $\varphi_1, \ldots, \varphi_k$ sont alors linéairement indépendants sur $\mathbb{Q}$, donc sur $\mathbb{R}$ car ils sont à coefficients rationnels. On pose pour $1 \leq i, j \leq k$:

$$U(X_m) = \det\left(\frac{1}{(i-1)!} \frac{\partial^{i-1}}{\partial X_m^{i-1}} \psi_j(X_m)\right)_{1 \leq i,j \leq k}$$

Comme les ψ_j sont linéairement indépendants, U n'est pas identiquement nulle. De plus, d'après le lemme 6, pour tout $1 \leq i \leq k$, il existe un opérateur différentiel

$$\Delta_i' = \frac{1}{i_1! \ldots i_{m-1}!} \frac{\partial^{i_1 + \ldots + i_{m-1}}}{\partial X_1^{i_1} \ldots \partial X_{m-1}^{i_{m-1}}}$$

d'ordre

$$i_1 + \ldots + i_{m-1} \leq i - 1 \leq k - 1 \leq d_m,$$

tel que

$$V(X_1, \ldots, X_{m-1}) := \det\left(\Delta_i^{'} \varphi_j\right)_{1 \leq i,j \leq k} \neq 0.$$

On pose :

$$\begin{aligned} W(X_1, \ldots, X_m) &= \det\left(\frac{1}{(j-1)!} \frac{\partial^{j-1}}{\partial X_m^{j-1}} \Delta_i^{'} f\right)_{1 \leq i,j \leq k} \\ &= \det\left(\sum_{r=1}^{k} \left(\Delta_i^{'} \varphi_r\right) \left(\frac{1}{(j-1)!} \frac{\partial^{j-1}}{\partial X_m^{j-1}} \psi_r\right)\right)_{1 \leq i,j \leq k} \\ &= V(X_1, \ldots, X_{m-1})\, U(X_m) \neq 0. \end{aligned}$$

Les coefficients de la matrice sont de la forme $f_{i_1,\ldots,i_{m-1},j-1}$, qui sont des polynômes à coefficients entiers. W est donc un polynôme à coefficients entiers. La preuve consiste alors à majorer l'indice de W grâce au lemme suivant, puis en l'exprimant en fonction de l'indice de f, à déduire la majoration cherchée de l'indice de f.

Lemme 8. *L'indice Θ de W relativement à $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; d_1, \ldots, d_m\right)$ vérifie :*

$$\Theta \leq \frac{k\delta^2}{6}.$$

Démonstration. Les polynômes U et V ne sont pas nécessairement à coefficients entiers, mais il existe une factorisation :

$$W(X_1, \ldots, X_m) = V^*(X_1, \ldots, X_{m-1})\, U^*(X_m)$$

avec U^* et V^* à coefficients entiers. On estime alors les hauteurs de U^* et V^*. On a déjà montré lors de la preuve du lemme 3 que :

$$|f_{i_1,\ldots,i_{m-1},j-1}| \leq 2^{d_1+\ldots+d_m} |f| \leq 2^{d_1+\ldots+d_m} q_1^{\omega d_1}.$$

Le nombre de termes dans $f_{i_1 \ldots i_{m-1}(j-1)}$ est inférieur à $2^{d_1+\ldots+d_m}$, et le nombre de termes du développement du déterminant de W est

$$k! \leq k^{k-1} \leq k^{d_m} \leq 2^{kd_m}.$$

On en déduit que :

$$|W| \leq 2^{kd_m} \left(2^{d_1+\ldots+d_m} 2^{d_1+\ldots+d_m} q_1^{\omega d_1}\right)^k \leq \left(2^{3md_1} q_1^{\omega d_1}\right)^k$$

car $d_1 \geq \ldots \geq d_m$. Par hypothèse, $q_1^{\omega} \geq 2^{3m}$, donc $|W| \leq q_1^{2\omega d_1 k}$.
On obtient :

$$|U^*| \leq q_1^{2\omega d_1 k} \leq q_m^{2\omega d_m k} \text{ et } |V^*| \leq q_1^{2\omega d_1 k}.$$

On applique alors l'hypothèse de récurrence du lemme de Roth au polynôme $V(X_1, \ldots, X_{m-1})$ à $m-1$ variables, de degré kd_h au plus en X_h avec $\frac{\delta^2}{12}$ à la place de δ. Le calcul précédent montre que V^* vérifie bien

$$|V^*| \leq q_1^{\omega\left(m-1, \frac{\delta^2}{12}\right)kd_1} \text{ car } \omega\left(m-1, \frac{\delta^2}{12}\right) = 2\omega(m, \delta).$$

L'indice de V^* relativement à $\left(\frac{p_1}{q_1}, \ldots, \frac{p_{m-1}}{q_{m-1}}; kd_1, \ldots, kd_{m-1}\right)$ est donc inférieur à $\frac{k\delta^2}{12}$. L'indice de V^* vu comme un polynôme en $X_1, \ldots, X_m$, relativement à $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; kd_1, \ldots, kd_m\right)$ est aussi inférieur à $\frac{k\delta^2}{12}$. De même, en appliquant cette fois-ci le cas $m = 1$ du lemme de Roth à U^* de degré inférieur à kd_m avec $\frac{\delta^2}{12}$ à la place de δ, et $\omega\left(1, \frac{\delta^2}{12}\right) \geq 2\omega(m, \delta)$, l'indice de U^*, vu comme polynôme en $X_1, \ldots, X_m$, relativement à $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; d_1, \ldots, d_m\right)$ est inférieur à $\frac{\delta^2}{12}$.

Comme $W = U^*V^*$, on en déduit que :

$$\Theta \leq \frac{k\delta^2}{6}.$$

Ceci conclut donc la preuve du lemme 8. □

On note θ l'indice de f relativement à $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; d_1, \ldots, d_m\right)$. On remarque que :

$$\begin{aligned}
\text{ind}(f_{i_1 \ldots i_{m-1}}(j-1)) &\geq \theta - \frac{i_1}{d_1} - \ldots - \frac{i_{m-1}}{d_{m-1}} - \frac{j-1}{d_m} \\
&\geq \theta - \frac{i_1 + \ldots + i_{m-1}}{d_{m-1}} - \frac{j-1}{d_m} \\
&\geq \theta - \frac{d_m}{d_{m-1}} - \frac{j-1}{d_m} \\
&\geq \theta - \omega - \frac{j-1}{d_m} \\
&\geq \theta - \frac{\delta^2}{24} - \frac{j-1}{d_m}.
\end{aligned}$$

Chaque composante de la colonne j du déterminant qui définit W est de la forme $f_{i_1 \ldots i_{m-1}(j-1)}$. Le développement de ce déterminant est une somme de produits de k éléments, un de chaque colonne. On en déduit que

$$\begin{aligned}
\Theta = \text{ind}(W) &\geq \sum_{j=1}^{k} \max\left(\theta - \frac{\delta^2}{24} - \frac{j-1}{d_m}, 0\right) \\
&\geq -\frac{k\delta^2}{24} + \sum_{i=0}^{k-1} \max\left(\theta - \frac{i}{d_m}, 0\right).
\end{aligned}$$

D'où :

$$\sum_{i=0}^{k-1} max\left(\theta - \frac{i}{d_m}, 0\right) \leq \Theta + \frac{k\delta^2}{24} \leq \frac{k\delta^2}{6} + \frac{k\delta^2}{24} < \frac{k\delta^2}{4}.$$

Il y a alors deux cas possibles :

1. Si $\theta > \frac{k-1}{d_m}$, l'inégalité ci-dessus devient :

$$\frac{1}{2}k\left(\theta + \theta - \frac{k-1}{d_m}\right) < k\frac{\delta^2}{4},$$

soit

$$\theta + \left(\theta - \frac{k-1}{d_m}\right) < \frac{\delta^2}{2}.$$

Or

$$\theta - \frac{k-1}{d_m} > 0,$$

donc

$$\theta < \frac{\delta^2}{2} < \delta.$$

2. Si $\theta \leq \frac{k-1}{d_m}$, l'inégalité devient alors :

$$\sum_{i=0}^{[\theta d_m]} \left(\theta - \frac{i}{d_m}\right) < \frac{k\delta^2}{4}$$

d'où :

$$\frac{1}{2}\theta\left([\theta d_m] + 1\right) < \frac{k\delta^2}{4}$$

et

$$\frac{1}{2}\theta^2 d_m < \frac{k\delta^2}{4}.$$

Or

$$k \leq d_m + 1 \leq 2d_m,$$

donc

$$\frac{1}{2}\theta^2 d_m < \frac{1}{2}\delta^2 d_m,$$

d'où

$$\theta < \delta.$$

Dans les deux cas, l'indice θ de f relativement à $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; d_1, \ldots, d_m\right)$ est inférieur à δ. Ceci conclut donc la preuve du lemme de Roth. □

3.4 Conclusion

On rappelle que α est un entier algébrique irrationnel de degré d. Soit η un réel positif. Soit m un entier assez grand pour que

$$e^{3(\eta/2)^2 m/16} > 2d$$

et

$$\delta < \min\left(\frac{1}{12}, \frac{m\eta}{16}\right).$$

Soient $p_1/q_1, \ldots, p_m/q_m$ m approximations rationnelles distinctes de α, soit A un grand entier et pour tout i, $d_i \simeq \frac{A}{log(q_i)}$.

Soit

$$q = e^A \simeq q_i^{d_i} \text{ pour tout } i.$$

Le lemme 3 appliqué à $\eta/2$ et $(d_1, \ldots, d_m)$ fournit un polynôme f annulant $(\alpha, \ldots, \alpha)$, de multidegré inférieur à $(d_1, \ldots, d_m)$ et vérifiant

$$\text{ind}\,(f, \alpha, \ldots, \alpha, d_1, \ldots, d_m) \geq \frac{m(1-\eta/2)}{2}$$

et

$$|f| \leq B^{d_1+\cdots+d_m}$$

pour un B réel, ne dépendant que de α.

Le calcul des polynômes dérivés effectué lors de la démonstration du lemme d'indice montre que

$$H(f) \leq CNB^{d_1+\cdots+d_m}\,|f|\,,$$

où C est une constante ne dépendant que de α.

On choisit A assez grand pour que les hypothèses du lemme de Roth (lemme 7) soient vérifiées, cela prouve que l'indice de f en $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right)$ est inférieur à δ. Par définition de l'indice, il existe m entiers $(i_1, \ldots, i_m)$ vérifiant

$$\sum_{j=1}^{m} \frac{i_j}{d_j} \leq \delta,$$

tels que si on pose

$$D = \frac{1}{i_1! \cdots i_m!} \frac{\partial^{i_1+\cdots+i_m} P}{\partial X_1^{i_1} \cdots \partial X_m^{i_m}},$$

Df sera un polynôme à coefficients entiers vérifiant

$$Df\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) \neq 0.$$

L'opérateur D réduit l'indice de f en $(\alpha,\dots,\alpha)$ d'une constante $c_2 \leq \delta$, et il augmente les coefficients de f d'un facteur c_1. Soit $(d'_1,\dots,d'_m)$ le multidegré de Df. On a donc

$$H(Df) \leq CNc_1 B^{2(d_1+\cdots+d_m)}$$

et

$$\operatorname{ind}(Df,\alpha,\dots,\alpha,d'_1,\dots,d'_m) \geq \frac{m(1-\eta/2)}{2} - \delta.$$

On rappelle les résultats montrés en introduction

$$\left| f\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right| \leq NH(f)\frac{1}{q^{(2+\varepsilon)t_m}}.$$

et

$$\left| f\left(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\right)\right| \geq \frac{1}{\prod_{i=1}^m q_i^{d_i}} \simeq \frac{1}{q^m}.$$

On en déduit

$$\begin{aligned} 1 \leq NH(Df)\frac{q^m}{q^{(2+\varepsilon)t_m}} &\leq CN^2c_1B^{2(d_1+\cdots+d_m)}\frac{q^m}{q^{(2+\varepsilon)\left(\frac{m}{2}\left(1-\frac{\eta}{2}\right)-\delta\right)}} \\ &\leq CN^2c_1B^{2(d_1+\cdots+d_m)}q^{\frac{m\eta}{2}+\frac{m\eta\varepsilon}{4}-\frac{m\varepsilon}{2}+(2+\varepsilon)\delta} \\ &\leq CN^2c_1B^{2(d_1+\cdots+d_m)}q^{\frac{5m\eta}{8}+\frac{5m\eta\varepsilon}{16}-\frac{m\varepsilon}{2}}. \end{aligned}$$

Le même raisonnement que lors de la preuve du lemme 3 montre qu'on a

$$c_1 \leq 2^{d_1+\cdots+d_m}.$$

Quitte à choisir A assez grand, on peut supposer que

$$B^{d_1+\cdots+d_m} \leq q^{m\eta/16},$$

et

$$2^{d_1+\cdots+d_m} \leq q^{m\eta/16},$$

soit

$$c_1 \leq q^{m\eta/16},$$

ainsi que

$$N = \prod_{i=1}^m (d_i+1) \leq q^{m\eta/16},$$

et

$$C \leq q^{m\eta/16}.$$

On a donc

$$\begin{aligned} 1 &\leq q^{\frac{m\eta}{16}+2\cdot\frac{m\eta}{16}+\frac{m\eta}{16}+2\cdot\frac{m\eta}{16}+\frac{5m\eta}{8}-\frac{m\varepsilon}{2}+\frac{5}{16}m\eta\varepsilon} \\ &\leq q^{m\eta-\frac{m\varepsilon}{2}+\frac{5}{16}m\eta\varepsilon} \\ &\leq q^{m\eta-\frac{m\varepsilon}{2}+\frac{m\eta\varepsilon}{2}}. \end{aligned}$$

On obtient la contradiction voulue pourvu que η soit choisi tel que

$$\eta < \frac{\varepsilon}{2+\varepsilon}.$$

Cela conclut la preuve du théorème de Roth.

4 Le théorème de Siegel

On donne maintenant une application de ce résultat à l'étude des points entiers d'une courbe algébrique. La preuve se base sur le théorème des sous-espaces de Schmidt, sous une forme due à Schlikewei et qui généralise le théorème de Roth.

4.1 Le théorème des sous-espaces

Théorème 9 (Schmidt)**.** *Soient $L_1, \ldots, L_m$ m formes linéaires à m variables à coefficients réels algébriques, linéairement indépendantes. Alors pour tout $\varepsilon \geq 0$, les points $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ qui vérifient l'inégalité*

$$|L_1(\mathbf{x}), \ldots, L_m(\mathbf{x})| \leq ||\mathbf{x}||^{-\varepsilon} \tag{6}$$

sont contenus dans un nombre fini de sous-espaces vectoriels propres de $\mathbb{Q}^m$.

On retrouve le théorème de Roth en prenant $m = 2$, $L_1(x, y) = x$ et $L_2(x, y) = \alpha x - y$.

Pour montrer le théorème de Siegel, on a besoin d'une reformulation plus générale de ce théorème. On introduit pour cela la notion de valeurs absolues $\mathfrak{p}$-adique, où $\mathfrak{p}$ est un idéal premier d'une extension algébrique K de $\mathbb{Q}$.

Définition 5 (Valeur absolue)**.** Soit K un corps, une *valeur absolue* sur K est une application $v : K \to \mathbb{R}^+$ vérifiant pour tous $x, y \in K$:

- $v(x) = 0 \Leftrightarrow x = 0$,
- $v(x + y) \leq v(x) + v(y)$,
- $v(x \cdot y) = v(x)v(y)$.

Définition 6 (Valeur absolue p-adique)**.** Soit p un nombre premier. On définit la valuation p-adique $v_p(r)$ d'un rationnel r par l'unique écriture de r sous la forme

$$r = p^{v_p(r)} \frac{s}{q}. \tag{7}$$

où p, q et s sont des entiers premiers entre eux et $q > 0$. On définit sur $\mathbb{Q}$ la *valeur absolue p-adique* $|\cdot|_p$ par

$$|r|_p = p^{-v_p(r)}. \tag{8}$$

en utilisant les mêmes notations que ci-dessus.

On se place à présent dans une extension finie K de $\mathbb{Q}$. On note $\mathcal{O}_K$ l'anneau des entiers algébriques dans K. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On admet que l'on peut définir de manière analogue une valeur absolue $\mathfrak{p}$-adique sur K, et qu'une telle valeur absolue $\mathfrak{p}$-adique sur K prolonge une valeur absolue p-adique sur $\mathbb{Q}$. On définit également les valeurs absolues infinies sur K qui sont les valeurs absolues induites de la norme usuelle sur $\mathbb{C}$ par les morphismes de corps : $K \to \mathbb{C}$.

On rappelle la définition du complété d'un espace métrique :

Définition 7 (Complété d'un espace métrique)**.** Soit X un espace métrique, il existe un espace métrique $\tilde{X}$ complet et une injection $i : X \to \tilde{X}$ isométrique d'image dense. L'espace $\tilde{X}$ est unique à isométrie près et est appelé *complété* de X.

On normalise les valeurs absolues sur K ainsi :

Définition 8 (Valeur absolue normalisée)**.** Soit v une valeur absolue $\mathfrak{p}$-adique sur K. On note p le nombre premier tel que v induise sur $\mathbb{Q}$ la valeur absolue p-adique. On note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la topologie induite par la valeur absolue p-adique et K_v le complété de K pour la topologie induite par v. On pose alors $d = [K : \mathbb{Q}]$ et $d_v = [K_v : \mathbb{Q}_p]$. On définit la *valeur absolue v' normalisée de v* par $|x|_{v'} = |x|_v^{-d_v/d}$.

Si v est une valeur absolue infinie, on normalise v de même, en posant $d_v = 1$ si v est induite par un morphisme à image réelle, et $d_v = 2$ sinon.

On ne considère par la suite que des valeurs absolues normalisées, également désignées de façon générale par v. On note M_K l'ensemble des valeurs absolues sur K.

On a alors la formule dite du produit :

$$\forall x \in K^*, \prod_{v \in M_K} |x|_v = 1.$$

Définition 9 (Hauteur d'un point)**.** Soit $x = (x_1, \ldots, x_m) \in K^m$. On pose

$$H(x) = \prod_{v \in M_K} \|x\|_v$$

où $\|x\|_v = \max |x_1|_v, \ldots, |x_m|_v$.

Définition 10 (Anneau des entiers)**.** Soit S un ensemble fini de valeurs absolues sur K contenant les valeurs absolues infinies. On définit l'*anneau $\mathcal{O}_S$ des S-entiers* de K, c'est-à-dire l'ensemble des éléments $\alpha \in K$ tels que $|\alpha|_v \leq 1$ pour toute valeur absolue $v \notin S$.

On peut à présent formuler le théorème des sous-espaces de Schlickewei :

Théorème 10 (Schlickewei)**.** *Pour tout $v \in S$, soient $L_{1,v}, \ldots, L_{m,v}$ m formes linéaires à m variables à coefficients algébriques linéairement indépendantes. Alors pour tout $\varepsilon > 0$, les points $\mathbf{x} = (x_1, \ldots, x_m) \in \mathcal{O}_S^m$ vérifiant l'inégalité :*

$$\prod_{v \in S} \prod_{i=1}^{m} |L_{i,v}(\mathbf{x})|_v \leq H(\mathbf{x})^{-\varepsilon}. \tag{9}$$

sont contenus dans un nombre fini de sous-espaces vectoriels propres de K^m.

4.2 Le théorème de Siegel

On donne quelques définitions et propriétés sur les variétés algébriques qui sont nécessaires pour énoncer le théorème de Siegel et donner sa démonstration. L'existence des objets ainsi que les propriétés sont admises.

Définition 11 (Variété algébrique affine)**.** Soit K un corps. Une *variété algébrique affine* sur K est définie par un idéal de $K[X_1, \ldots, X_n]$.

Dans la suite, on ne considère que le cas où $n = 2$ et où l'idéal est engendré par un polynôme non constant. On parle alors de *courbe algébrique plane*.

On considère une courbe C définie par un polynôme $P(x, y)$ à coefficients rationnels irréductible sur $\mathbb{Q}$. Si L est une extension algébrique de $\mathbb{Q}$, on note $C(L)$ l'ensemble des points (x, y) de $\mathbb{A}^2(L)$ tels que $P(x, y) = 0$.

Définition 12 (Fonctions et fractions régulières)**.** On désigne par

$$K[C] = K[x, y]/(P)$$

l'anneau des *fonctions régulières* sur C et $K(C)$ son corps des fractions.

Définition 13 (Courbe projective)**.** On note $\bar{C}$ la *courbe projective* définie par le polynôme homogène $\tilde{P}$ associé à P. Si L est une extension algébrique de $\mathbb{Q}$, on note $\bar{C}(L)$ les points de $\mathbb{P}^2(L)$ de coordonnées homogènes $[x : y : z]$ tels que $\tilde{P}(x, y, z) = 0$.

L'espace affine $\mathbb{A}^2\left(\bar{\mathbb{Q}}\right)$ s'injecte dans l'espace projectif via l'application $(x, y) \mapsto [x : y : 1]$, ce qui permet de voir $C(\bar{\mathbb{Q}})$ comme une partie de $\bar{C}(\bar{\mathbb{Q}})$.

Dans la suite, on suppose également que la courbe C est lisse :

Définition 14 (Lissité)**.** La courbe algébrique projective $\bar{C}$, définie par le polynôme $\tilde{P}(x, y, z)$ est dite *lisse* si et seulement si en tout point de $\bar{C}(\bar{\mathbb{Q}})$, l'un des polynômes $\frac{\partial P}{\partial x}$, $\frac{\partial P}{\partial y}$ ou $\frac{\partial P}{\partial z}$ est non nul.

On introduit à présent des notions nécessaires pour énoncer le théorème de Riemann-Roch, qui joue un rôle déterminant dans la preuve du théorème de Siegel.

Définition 15 (Ordre d'une fraction régulière en un point)**.** Soit $y \in K(C)$ une fraction régulière et Q un point de $\bar{C}\left(\bar{\mathbb{Q}}\right)$. On définit l'*ordre* $\mathrm{ord}_Q\, y$ de y en Q de sorte que si Q est zéro de y, sa multiplicité est $\mathrm{ord}_Q\, y$, si Q est pôle de y, son ordre comme pôle est $-\mathrm{ord}_Q\, y$ ($\mathrm{ord}_Q\, y$ est alors négatif), et sinon, $\mathrm{ord}_Q\, y$ est nul.

Définition 16 (Diviseur à l'infini et diviseur asssocié à une fraction)**.** On pose

$$\bar{C}\left(\bar{\mathbb{Q}}\right) \setminus C\left(\bar{\mathbb{Q}}\right) = \{Q_1, \ldots, Q_r\}$$

l'ensemble des zéros de $\tilde{P}$ à l'infini comptés avec multiplicité. Quitte à remplacer K par une extension, on peut supposer que les points $Q_1, \ldots, Q_r$ sont à coordonnées dans K. On définit alors le *diviseur à l'infini*

$$D = Q_1 + \ldots + Q_r.$$

Pour tout élément y de $K(C)$, on définit le *diviseur* (y) *de* y comme la somme des zéros et des pôles de y comptés avec leur ordre.

Définition 17 (Paramètre local)**.** Soit Q un zéro de $\tilde{P}$, vu comme point de l'espace projectif. Un *paramètre local* pour C (courbe algébrique lisse) au voisinage de Q est une fraction régulière dont Q est un zéro d'ordre 1.

Soit n un entier naturel. On définit le sous-espace vectoriel de $K(C)$

$$\mathcal{L} = \mathcal{L}(nD) = \{y \in K(C) \,|\, (y) + nD \geq 0\},$$

où $(y) + nD \geq 0$ signifie que tous les termes apparaissant dans la somme formelle sont affectés d'un coefficient positif.

On peut à présent énoncer le théorème de Riemann-Roch :

Théorème 11 (Riemann-Roch)**.** *Pour de grandes valeurs de n, la dimension l de $\mathcal{L}(nD)$ est $l = nr - O(1) \sim nr$.*

On peut à présent énoncer le théorème de Siegel.

Théorème 12 (Siegel)**.** *On suppose que $r = |\bar{C}\left(\bar{\mathbb{Q}}\right) \setminus C\left(\bar{\mathbb{Q}}\right)| \geq 3$. Alors C n'a qu'un nombre fini de points dans $\mathbb{A}^2(\mathcal{O}_S)$.*

4.3 Démonstration du théorème de Siegel

On suit la preuve de Corvaja et Zannier.

On considère un entier naturel n. D'après le théorème de Riemann-Roch, $\mathcal{L}$ est de dimension finie $l \sim nr$. Soit $y_1, \ldots, y_l$ une base de $\mathcal{L}$. Chaque y_j est le quotient de deux fonctions régulières premières entre elles. La fonction du dénominateur n'a alors aucun zéro dans C, elle est donc constante. Les y_j sont donc des fonctions régulières que l'on peut supposer à coefficients dans

$\mathcal{O}_S$ quitte à les multiplier par une constante. On obtient donc que pour tout point M S-entier de $C(K)$, $y_j(M) \in \mathcal{O}_S$.

On suppose à présent par l'absurde qu'il existe une suite infinie $P_1, P_2, \ldots$ de points S-entiers distincts. Comme $\bar{C}$ est une courbe projective, l'ensemble $\bar{C}(K_v)$ est un fermé de l'espace projectif, donc il est compact pour la topologie v-adique pour tout v. Quitte à extraire, on peut donc supposer que la suite $(P_i)_i$ converge pour la topologie v-adique pour tout v dans S et on note Q_v la limite correspondante. On désigne alors par S' l'ensemble des valeurs absolues v dans S telles que $Q_v \in \bar{C}\left(\bar{\mathbb{Q}}\right) \setminus C\left(\bar{\mathbb{Q}}\right)$ et S'' l'ensemble des v telles que $Q_v \in C\left(\bar{\mathbb{Q}}\right)$, de sorte que $S = S' \cup S''$.

On estime $|y_j(P_i)|$ pour v dans S et $i = 1, 2, \ldots$ Pour v dans S'', comme la suite $(P_i)_i$ reste dans un compact de C pour la topologie v-adique, $(|y_j(P_i)|)_i$ est bornée. Pour v dans S', on fixe un paramètre local t_v de l'espace projectif au voisinage de Q_v. Lorsque i tend vers l'infini, on obtient donc que

$$|y_j(P_i)|_v \ll |t_v(P_i)|_v^{ord_{Q_v} y_j}.$$

Ainsi, en posant $y = (y_1, \ldots, y_l)$, on trouve :

$$\|y(P_i)\|_v \ll \begin{cases} |t_v(P_i)|_v^{ord_{Q_v} y_j} & \text{si } v \in S' \\ 1 & \text{si } v \in S'' \end{cases}$$

Comme les $y_j(P_i)$ sont dans $\mathcal{O}_S$, on obtient

$$H(y(P_i)) = \prod_{v \in S} \|y(P_i)\|_v \ll \prod_{v \in S'} |t_v(P_i)|_v^{ord_{Q_v} y_j}. \tag{10}$$

Une fois ces calculs préliminaires achevés, on peut attaquer le cœur de la preuve de Corvaja-Zannier. Soit $v \in S'$. Pour tout $k \geq 1$, on considère le sous-espace vectoriel W_k de $\mathcal{L}$ défini par

$$W_k = \{\varphi \in \mathcal{L} \mid \mathrm{ord}_{Q_v} \varphi \geq k - n - 1\}.$$

On a $V = W_1 \supset W_2 \supset \cdots$ et $\dim(W_k/W_{k+1}) \leq 1$ car chaque augmentation de l'ordre d'annulation impose au plus une condition linéaire supplémentaire. Donc en particulier, pour tout k, $\dim W_k \geq l - k + 1$. On a $W_d \neq \{0\}$, on en choisit une base que l'on complète successivement en des bases de $W_{d-1}, \ldots, W_1$. On note $w_l, \ldots, w_1$ la famille obtenue. Par construction, on a pour tout $k \geq 1, w_k \in W_k$, soit :

$$\mathrm{ord}_{Q_v} w_k \geq k - n - 1,$$

d'où

$$\sum_{k=1}^{l} \mathrm{ord}_{Q_v} w_k \geq \sum_{k=1}^{l} k - n - 1 = \frac{l(l - 2n - 1)}{2}.$$

Puisque pour n grand, $l \sim rn$ et $r \geq 3$, on peut choisir n assez grand pour que

$$A := \frac{l(l-2n-1)}{2} > 0.$$

En exprimant les vecteurs w_k comme combinaison linéaire des y_i, on obtient l formes linéaires indépendantes $L_{l,v}, \ldots, L_{1,v}$ en $\mathbf{y}$ sur k. Pour $v \in S''$, on pose pour tout $1 \leq k \leq l$, $L_{k,v} = y_k$.

On cherche à présent à borner $|L_{k,v}(\mathbf{y}(P_i))|_v$ pour tout k et v. Pour $v \in S''$, on a

$$|L_{k,v}(\mathbf{y}(P_i))|_v = |y_k(P_i)|_v \ll 1,$$

et pour $v \in S'$, on a

$$|L_{k,v}(\mathbf{y}(P_i))|_v = |w_k(P_i)|_v \ll |t_v(P_i)|_v^{\operatorname{ord}_{Q_v} w_k}.$$

On obtient donc

$$\prod_{v \in S} \prod_{k=1}^{l} |L_{k,v}(\mathbf{y}(P_i))|_v \ll \prod_{v \in S'} |t_v(P_i)|_v^{\sum_{k=1}^{l} \operatorname{ord}_{Q_v} w_k} \leq \prod_{v \in S'} |t_v(P_i)|_v^{A}.$$

D'après l'équation (10), on a

$$\prod_{v \in S} \prod_{k=1}^{l} |L_{k,v}(\mathbf{y}(P_i))|_v \ll H(\mathbf{y}(P_i))^{-\frac{A}{n}}.$$

En posant $\varepsilon = -\frac{A}{n}$, on peut appliquer le théorème de sous-espace à nos formes linéaires $L_{k,v}$. On obtient qu'il existe un nombre fini de fonctions non nulles $u_1, \ldots, u_l$ dans $\mathcal{L}$ telles que chaque P_i soit zéro d'un u_j. On en déduit qu'il n'existe qu'un nombre fini de P_i distincts, ce qui contredit l'hypothèse. □

Références

[1] M. Nakamaye, **Roth's Theorem : an introduction to diophantine approximation**, Notes pour l'école doctorale « Géométrie diophantienne, Rennes, 2009.

[2] M. Hindry and J. H. Silvermann, **Diophantine geometry.** An introduction. Graduate Texts in Mathematics, 201. *Springer-Verlag, New York,* 2000.

[3] W. M. Schmidt, **Diophantine approximation.** Lecture Notes in Mathematics, 785. *Springer, Berlin,* 1980.

[4] P. Corvaja and U. Zannier, **A subspace theorem approach to integral points on curves.**

[5] Y. Bilu, **The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...].** Séminaire Bourbaki. Vol. 2006/2007.