Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Maurice Mignotte

Sur la résolution de systèmes linéaires en nombres entiers

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, n° 2 (1973-1974), exp. n° G16, p. G1-G5

<http://www.numdam.org/item?id=SDPP_1973-1974__15_2_A11_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théorie des nombres)
15e année, 1973/74, n° G16, 5 p.

20 mai 1974

SUR LA RÉSOLUTION DE SYSTÈMES LINÉAIRES EN NOMBRES ENTIERS

par Maurice MIGNOTTE

Introduction.

Les questions abordées tournent autour de lemmes classiques, attribués à C. L. SIEGEL, sur la résolution en nombres entiers de systèmes d'équations ou d'inéquations linéaires.

On montre que la résolution de systèmes d'inéquations permet de résoudre des systèmes d'équations en améliorant même les résultats antérieurs. Ensuite, des techniques probabilistes ou de géométrie des nombres permettent d'obtenir certains raffinements.

Tous ces résultats sont tout particulièrement utiles en théorie des nombres transcendants. On donne, en prime, une forme effective du théorème de l'élément primitif qui, elle aussi, peut servir dans cette théorie.

1. Le résultat classique.

PROPOSITION 1. - *Soient les* m *formes linéaires*

$$L_j(x) = \sum_{i=1}^{n} u_{ij} x_i \ , \quad j = 1, \ldots, m \ , \quad u_{ij} \in \underset{\sim}{R} \ .$$

Soient X *et* ℓ *des nombres entiers positifs tels que* $\ell^m < (X+1)^n$. *Alors il existe des éléments* $x_1, \ldots, x_n$ *entiers, non tous nuls, tels que*

$$\max_{1 \leq i \leq n} |x_i| \leq X$$

et

$$\max_{1 \leq j \leq m} |L_j(x_1, \ldots, x_n)| \leq \frac{nUX}{\ell} \ , \text{ où } \ U = \max_{i,j} |u_{ij}| \ .$$

Démonstration. - Soit E l'ensemble des x de $\underset{\sim}{Z}^n$ avec $0 \leq x_i \leq X$, $i=1,\ldots,n$. L'application $L = (L_1, \ldots, L_m)$ envoie E dans un hypercube C de côté nUX dans $\underset{\sim}{R}^m$. Partageons C en ℓ^m petits cubes égaux. Donc $\ell^m < \text{card } E = (X+1)^m$; on peut appliquer le principe des tiroirs : Deux éléments x' et x'' de E sont envoyés par L dans un même petit cube. Alors $x = x' - x''$ convient.

2. De l'utilité des systèmes d'inégalités.

La proposition 1 permet de démontrer le théorème suivant.

THÉORÈME 1. - *Soit* K *un corps de nombres de degré* δ *sur* $\underset{\sim}{Q}$. *Soient* $a_{i,j}$, $1 \leq i \leq \nu$, $1 \leq j \leq \mu$, *des entiers de* K . *Soit* $A \geq \max_{i,j} |\overline{a_{i,j}}|$, A *entier rationnel. Si on a* $\nu > \mu\delta$, *alors le système*

$$\sum_{i=1}^{\nu} a_{i,j}\, x_i = 0 \ , \quad 1 \leqslant j \leqslant \mu$$

admet une solution $(x_1, \ldots, x_\nu) \in Z^\nu$ non triviale et telle que

$$\max|x_i| \leqslant (2(\nu A)^{\mu\delta})^{1/(\nu-\mu\delta)} \ .$$

Démonstration. - Soient σ_k les plongements de K dans $\underset{\sim}{C}$, $k = 1, \ldots, \delta$. Supposons d'abord σ_1 réel. Les valeurs

$$X = [(\nu A)^{\mu\delta/(\nu-\mu\delta)}] \ , \quad \ell = [(\nu A X)^{\delta}] + 1$$

sont telles qu'on peut appliquer la proposition 1 aux formes $L_j = \sum_{i=1}^{\nu} \sigma_1(a_{ij})\, x_i$. D'où l'existence de $(x_1, \ldots, x_n) \in \underset{\sim}{Z}^n$ non trivial tel que $|x_j| \leqslant X$ et

$$|\sigma_1(\sum_{i=1}^{\nu} a_{ij}\, x_i)| \leqslant \frac{\nu A X}{\ell} < \frac{1}{(\nu A X)^{\delta-1}} \ , \quad j = 1, \ldots, \mu \ .$$

Les entiers algébriques $\eta_j = \sum_{i=1}^{\nu} a_{ij}\, x_i$ vérifient alors

$$|\mathrm{Norm}_{K/\underset{\sim}{Q}}(\eta_j)| < \frac{1}{(\nu A X)^{\delta-1}} \prod_{k=2}^{\delta} |\sigma_k(\eta_j)| \leqslant 1 \ ,$$

on a donc $\eta_1 = \ldots = \eta_\mu = 0$.

Dans le cas où K n'admet pas de plongement réel, on considère les composantes réelles et imaginaires des $\sigma_1(\eta_j)$, d'où la présence du facteur 2.

On a montré qu'on peut remplacer la constante 2 par 1 lorsque K n'est pas totalement imaginaire.

Il est intéressant de comparer le théorème 1 au résultat classique analogue dans lequel la majoration précédente des x_i est

$$\max|x_i| \leqslant (C_K\, \nu A)^{\mu\delta/(\nu-\mu\delta)} \ ,$$

où C_K est une constante, non calculée, qui dépend de K (voir [4], Appendice). Dans la démonstration classique, on choisit une base d'entiers de K, puis on résoud un système à coefficients entiers de $\mu\delta$ équations.

Le résultat donné ici améliore légèrement un résultat publié en [5] (lemme 1.3.1).

3. Retour sur la proposition 1.

Nous donnerons deux démonstrations de résultats essentiellement équivalents, dans l'ordre chronologique où nous les avons rencontrées. Les notations sont celles de la proposition 1 et de sa démonstration.

3.1. Principe des tiroirs et considérations probabilistes.

Afin d'expliquer l'idée de ce qui suit, considérons le cas $m = 1$. Pour $n = 1$, l'ensemble $L_1(E)$ est constitué par des points équidistribués sur un intervalle fini. Par contre, si $n \geqslant 2$, les points de $L_1(E)$ sont distribués de manière irrégulière, une forte proportion d'entre eux étant concentrés autour d'une valeur moyenne. De manière plus précise, leur distribution s'approche, pour n tendant vers l'infini, de celle de la loi de Gauss (théorème central-limite). On n'appli-

quera donc pas le principe des tiroirs à $L_i(E)$ tout entier, mais à une partie de $L(E)$ où les points sont suffisamment denses. La démonstration qui suit est extraite de [2].

PROPOSITION 2. - *Les notations sont celles de la proposition 1. Pour tout* X *entier tel que* $(X+1)^{n/m} > 2$, *il existe* $x = (x_1, \dots, x_n) \in \underset{\sim}{Z}^n$ *non nul tel que* $\max|x_i| \leq X$ *et* $\max|L_j(x)| < (\log(18m))^{1/2}(\sqrt{n}\,U(X+1))/((X+1)^{n/m} - 2)$.

Démonstration. - Posons

$N = \text{card } E = (X+1)^n$; $\lambda = (\log(18m)/5)^{1/2}$;

$F_j = \{x \in E ; \ |\sum_{i=1}^n u_{ij}(x_i - \frac{X}{2})| \leq \lambda\sqrt{n}\,U(X+1)\}$; $F = \bigcap_{j=1}^m F_j$;

$F'_j = \complement_E F_j$, $N' = \text{card } F$; $N'_j = \text{card } F'_j$.

Majorons d'abord N'_j, et pour cela considérons l'expression

$$S_j = \sum_{x\in E} \exp\Big(\frac{12\lambda}{\sqrt{n}\,U} \sum_{i=1}^n u_{ij}\,\Big(\frac{x_i - X/2}{X+1}\Big)\Big) .$$

On a d'une part

$$N'_j \exp(12\lambda^2) \leq 2S_j$$

et, d'autre part,

$$S_j = \prod_{i=1}^n \frac{\operatorname{sh}(6\lambda u_{ij}/(\sqrt{n}\,U))}{\operatorname{sh}(6\lambda u_{ij}/((X+1)\sqrt{n}\,U))} \leq N \prod_{i=1}^n \operatorname{sh}(6\lambda u_{ij}/(\sqrt{n}\,U))/(6\lambda u_{ij}/(\sqrt{n}\,U))$$

$$\leq N \exp((6\lambda^2 \textstyle\sum u_{ij}^2)/(nU^2)) \leq N \exp(6\lambda^2) ,$$

en utilisant l'inégalité $\frac{\operatorname{sh} t}{t} \leq \exp(t^2/6)$, dont la démonstration est laissée au lecteur. D'où $N'_j \leq 2N \exp(-6\lambda^2)$, et ainsi

$$N' \geq N - N'_1 - \dots - N'_m \geq N(1 - 2m\exp(-6\lambda^2)) .$$

Par construction, l'image de F par L est contenue dans un cube C' de côté $2\lambda\sqrt{n}\,U(X+1)$. Soit alors h le plus grand entier tel que $h^m < N'$. Découpons maintenant C' en h^m petits cubes, et appliquons le principe des tiroirs. Ceci montre l'existence de $(x_1, \dots, x_n) \in \underset{\sim}{Z}^n$, non nul, tel que $\max|x_i| \leq X$ et

$$|L_j(x_1, \dots, x_n)| \leq \frac{2\lambda\sqrt{n}\,U(X+1)}{h} .$$

Un calcul immédiat achève la démonstration.

3.2. Géométrie des nombres et formes quadratiques.

La méthode employée ci-dessous est due à K. MAHLER (voir [1], chap. 1), mais les détails diffèrent quelque peu.

LEMME 1. - *Soit* $F(x_1, \dots, x_n)$ *une forme quadratique définie positive de discriminant* D. *Alors il existe* $x \in \underset{\sim}{Z}^n$, *non nul, tel que*

$$F(x) \leq \frac{4}{\pi}(\Gamma(1+\tfrac{n}{2})^2 D)^{1/n} \leq nD^{1/n} .$$

Démonstration. - Soit t un nombre positif. Alors, l'ellipsoïde $F(x) \leq t$ a

pour volume $V(t) = t^{n/2} D^{-1/2} \pi^{n/2} \Gamma(1 + \frac{n}{2})^{-1}$. D'après le théorème de Minkowski, cet ellipsoïde contient un élément non nul de $\underset{\sim}{Z}^n$ si t vérifie $V(t) = 2^n$. D'où le résultat.

On applique ce résultat à la forme quadratique $F(x)^2 = s^2 \sum_{j=1}^{m} L_j^2(x) + \|x\|^2$, où $\|x\|^2 = x_1^2 + \ldots + x_n^2$, $s \geqslant U^{-1}$.

Par souci de simplicité, bornons-nous au cas $m = 1$, le cas général est traité en [1]. Le discriminant D de F vérifie

$$D = 1 + s^2 \sum_{i=1}^{n} u_{i1}^2 \leqslant 1 + s^2 U^2 \leqslant (n + 1)s^2 U^2 .$$

Le lemme 1 assure l'existence de $x \in \underset{\sim}{Z}^n$ non nul, tel que

$$s^2 L_1^2(x) + \|x\|^2 \leqslant n(n + 1)^{1/n} (s^2 U^2)^{1/n} .$$

D'où

$$\|x\|^2 \leqslant \sqrt{n}\ (n + 1)^{1/2n} (s^2 U^2)^{1/n} = t ,$$

$$|L_1(x)| \leqslant ts^{-1} = Un^{n/2} \sqrt{n + 1}\ t^{-(n-1)} .$$

On a obtenu le résultat suivant.

PROPOSITION 3. - Soit n un entier positif. Soit

$$L(x) = \sum_{i=1}^{n} u_i x_i , \quad u_i \in \underset{\sim}{R} , \quad \max|u_i| = U .$$

Alors, pour $t \geqslant \sqrt{n}\ (n + 1)^{1/2n}$, il existe $x \in \underset{\sim}{Z}^n$ tel que $0 < \|x\| < t$, et $|L(x)| \leqslant n^{n/2} \sqrt{n + 1}\ Ut^{-(n-1)}$.

Complément : une forme effective du théorème de l'élément primitif.

PROPOSITION 4. - Soit $K = \underset{\sim}{Q}(\alpha_1 , \ldots , \alpha_k)$ un corps de nombres de degré d . Alors il existe des entiers $a_2 , \ldots , a_k$, avec $0 \leqslant a_i \leqslant (d(d - 1))/2$ pour $i = 1 , \ldots , k$, tel que le nombre $\alpha = \alpha_1 + a_2 \alpha_2 + \ldots + a_k \alpha_k$ engendre K (i. e. $K = \underset{\sim}{Q}(\alpha)$).

Démonstration. - Il suffit de considérer le cas $k = 2$. Le corps K admet d plongements distincts dans $\underset{\sim}{C}$: $\sigma_1 , \ldots , \sigma_d$. Un élément $\eta \in K$ engendre K si les $\sigma_j(\eta)$ sont distincts. Considérons les éléments $\beta_n = \alpha_1 + n\alpha_2$ pour $0 \leqslant n \leqslant (d(d - 1))/2$. Nous allons montrer que l'un des β_n est tel que

$$\sigma_i(\beta_n) \neq \sigma_j(\beta_n) \quad \text{si} \quad i \neq j .$$

Remarquons d'abord que, pour $i \neq j$, on a $\sigma_i \neq \sigma_j$ et donc $\sigma_i(\alpha_1) \neq \sigma_j(\alpha_1)$ ou $\sigma_i(\alpha_2) \neq \sigma_j(\alpha_2)$. Considérons le polynôme

$$P(X) = \prod_{i<j} (\sigma_i(\alpha_1 + X\alpha_2) - \sigma_j(\alpha_1 + X\alpha_2)) .$$

D'après ce qui précède, P n'est pas nul ; il admet donc au plus $(d(d - 1))/2$ racines. D'où l'existence de n tel que $0 \leqslant n \leqslant (d(d - 1))/2$ et $P(n) \neq 0$. L'élément $\alpha = \beta_n$ est un générateur de K .

Ce résultat s'avère en particulier utile pour l'étude de l'approximation simultanée de nombres transcendants par des nombres algébriques (voir [3]).

BIBLIOGRAPHIE

[1] MAHLER (Kurt). - Lectures on transcendental numbers (manuscrit).

[2] MIGNOTTE (Maurice). - Sur les multiples des polynômes irréductibles (manuscrit).

[3] MIGNOTTE (Maurice) et WALDSCHMIDT (Michel). - Approximation des valeurs de fonctions transcendantes, II (en préparation).

[4] SCHNEIDER (Theodor). - Einführung in die transzendenten Zahlen. - Berlin, Springer-Verlag, 1957 (Grundlehren der matematischen Wissenschaften, 81) et [en français] Introduction aux nombres transcendants. - Paris, Gauthier-Villars, 1959.

[5] WALDSCHMIDT (Michel). - Un premier cours sur les nombres transcendants. - Berlin, Springer-Verlag (Lecture Notes in Mathematics) (à paraître).

(Texte reçu le 20 mai 1974)

Maurice MIGNOTTE
158 boulevard Galliéni
92390 VILLENEUVE LA GARENNE