

Une remarque sur le théorème de Kronecker

K. Mahler

Le théorème de Kronecker sur les approximations simultanées inhomogènes peut s'obtenir de nombreuses manières différentes. La démonstration la plus simple repose probablement sur la géométrie des nombres, comme je vais le montrer dans cette note.

Les faits fondamentaux de la géométrie des nombres se trouvent dans l'ouvrage *An Introduction to the Geometry of Numbers* de J. W. S. Cassels, Berlin 1959. Nous suivons la notation de ce livre ; les références à celui-ci porteront les lettres IGN suivies du numéro de page.

1. L'espace à n dimensions de tous les points

$$x = (x_1, \dots, x_n), \quad y = (y_1, \dots, y_n), \quad 0 = (0, \dots, 0)$$

à coordonnées réelles est noté $\mathbb{R}^n$. Les points de $\mathbb{R}^n$ sont également considérés comme des vecteurs. La somme de deux points x et y est alors définie par

$$x + y = (x_1 + y_1, \dots, x_n + y_n),$$

le produit du point x par le nombre réel t par

$$tx = (tx_1, \dots, tx_n),$$

et le produit scalaire des points x et y par

$$xy = x_1y_1 + \dots + x_ny_n.$$

La fonction à valeurs réelles $F(x)$ de x dans $\mathbb{R}^n$ est appelée une fonction de distance convexe si

$$F(0) = 0; \quad F(x) > 0 \text{ si } x \neq 0, \tag{1}$$

$$F(tx) = |t|F(x), \tag{2}$$

$$F(x + y) \leq F(x) + F(y). \tag{3}$$

Lorsque $F(x)$ est une telle fonction de distance convexe, l'ensemble de points K défini par

$$K : F(x) \leq 1$$

est convexe, borné, fermé, symétrique par rapport à 0, et contient 0 comme point intérieur. Le volume de K défini par

$$V = \int \dots \int_K dx_1 \dots dx_n$$

est un nombre positif (IGN 108 f.).

Référence : L'enseignement mathématique, 2ème série, Tome XII, Fascicule 3, juillet-septembre 1966.

On peut montrer qu'à chaque fonction de distance convexe $F(x)$ est associée une seconde fonction de distance convexe

$$F^*(y) = \sup_{x \neq 0} \frac{xy}{F(x)} = \sup_{F(x)=1} xy,$$

et réciproquement,

$$F(x) = \sup_{y \neq 0} \frac{xy}{F^*(y)} = \sup_{F^*(y)=1} xy.$$

Les deux corps convexes

$$K : F(x) \leq 1 \quad \text{et} \quad K^* : F^*(y) \leq 1$$

sont polaires réciproques par rapport à la sphère unité

$$E : xx = 1$$

en ce sens que chaque point y de la frontière de K^* a pour hyperplan polaire par rapport à E l'hyperplan tangent (ou plus exactement, l'hyperplan d'appui)

$$xy = F^*(y)$$

de K . La relation analogue vaut lorsque l'on permute K et K^* , et par conséquent aussi $F(x)$ et $F^*(y)$ (IGN 112 f.).

2. Un point réticulaire (ou point d'un réseau) dans $\mathbb{R}^n$ est un point à coordonnées entières rationnelles. À l'aide de ces points du réseau, les n minima successifs du corps convexe K sont définis comme suit.

Le premier minimum $m^{(1)}$ est la plus petite valeur de $F(x)$ pour tout point du réseau $x \neq 0$; désignons par $x^{(1)} \neq 0$ un point du réseau satisfaisant à

$$F(x^{(1)}) = m^{(1)}.$$

Soit ensuite $2 \leq k \leq n$, et supposons que les $k-1$ premiers minima successifs $m^{(1)}, \dots, m^{(k-1)}$ et les $k-1$ points du réseau indépendants correspondants $x^{(1)}, \dots, x^{(k-1)}$ satisfaisant à

$$F(x^{(h)}) = m^{(h)} \quad (h = 1, 2, \dots, k-1)$$

aient déjà été définis. Le k -ième minimum $m^{(k)}$ est alors la plus petite valeur de $F(x)$ pour tout point du réseau x qui est linéairement indépendant de $x^{(1)}, \dots, x^{(k-1)}$, et nous désignons par $x^{(k)}$ un tel point du réseau pour lequel

$$F(x^{(k)}) = m^{(k)}.$$

On peut démontrer que les n minima successifs $m^{(1)}, \dots, m^{(n)}$ sont uniques. Ils satisfont aux inégalités

$$0 < m^{(1)} \leq m^{(2)} \leq \dots \leq m^{(n)}; \quad \frac{2^n}{n!} \leq V m^{(1)} m^{(2)} \dots m^{(n)} \leq 2^n. \quad (4)$$

Les n points du réseau correspondants $x^{(1)}, \dots, x^{(n)}$ ne sont pas uniques. Ils sont linéairement indépendants et forment ainsi une base de $\mathbb{R}^n$, mais ils ne constituent pas nécessairement une base

de l'ensemble de tous les points du réseau (IGN, 215 f.).

Il existe également de manière naturelle n minima successifs $m^{*(1)}, \dots, m^{*(n)}$ du corps convexe polaire réciproque K^* et un ensemble de n points du réseau linéairement indépendants $y^{(1)}, \dots, y^{(n)}$ tels que

$$F^*(y^{(k)}) = m^{*(k)} \quad (k = 1, 2, \dots, n).$$

Ces minima satisfont à des inégalités analogues à (4).

Par un théorème général de la géométrie des nombres (IGN 213 f. et 219 f.), les deux ensembles de minima successifs sont reliés l'un à l'autre par le système de n inégalités

$$1 \leq m^{(k)} m^{*(n-k+1)} \leq n! \quad (k = 1, 2, \dots, n). \quad (5)$$

Les deux ensembles de minima successifs de K et K^* sont également reliés au problème des approximations inhomogènes. Soit x^0 un point arbitraire dans $\mathbb{R}^n$. Il existe alors un point du réseau x tel que (IGN 313 f.)

$$F(x - x^0) \leq \frac{nm^{(n)}}{2} \leq \frac{n \cdot n!}{2m^{*(1)}}. \quad (6)$$

3. Nous donnons maintenant deux types d'applications des résultats qui viennent d'être énoncés aux problèmes inhomogènes; tous deux peuvent être généralisés.

Soit d'abord $n = N + 1$ où $N \geq 1$. Numérotions les indices des coordonnées $0, 1, \dots, N$ plutôt que $1, 2, \dots, n$ comme précédemment. Soient $\alpha_1, \dots, \alpha_N$ un ensemble de N nombres réels fixes arbitraires et A, B deux paramètres positifs. Alors les expressions

$$F(x) = A(|x_1 - \alpha_1 x_0| + \dots + |x_N - \alpha_N x_0|) + B|x_0|$$

et

$$F^*(y) = \max \left(\frac{|y_1|}{A}, \dots, \frac{|y_N|}{A}, \frac{|y_0 + \alpha_1 y_1 + \dots + \alpha_N y_N|}{B} \right)$$

forment une paire de fonctions de distance polaires réciproques. Avec un léger changement de notation, soient $m^{(0)}, m^{(1)}, \dots, m^{(N)}$ et $m^{*(0)}, m^{*(1)}, \dots, m^{*(N)}$ les deux ensembles correspondants de $N + 1$ minima successifs.

On supposera que

$$F^*(y) \geq 1 \quad \text{pour tous les points du réseau } y \neq 0.$$

Ceci équivaut à l'hypothèse selon laquelle

$$m^{*(0)} \geq 1.$$

Par conséquent, moyennant un changement de notation trivial, la formule (6) implique que pour tout point donné x^0 , il existe un point du réseau x satisfaisant à

$$F(x - x^0) \leq \frac{(N + 1)(N + 1)!}{2}.$$

Ces estimations peuvent être exprimées sous une forme plus explicite. Posons

$$\beta_0 = x_0^0, \quad \beta_1 = \alpha_1 x_0^0 - x_1^0, \dots, \beta_N = \alpha_N x_0^0 - x_N^0,$$

où x^0 a pour coordonnées $x^0 = (x_0^0, x_1^0, \dots, x_N^0)$. Pour $N + 1$ constantes données $\beta_0, \beta_1, \dots, \beta_N$, il existe toujours un unique point x^0 satisfaisant à ces équations.

Le résultat obtenu peut désormais s'énoncer sous la forme suivante.

Théorème 1. *Soient $\alpha_1, \alpha_2, \dots, \alpha_N$, $A > 0$ et $B > 0$ des nombres réels tels que*

$$|y_0 + \alpha_1 y_1 + \dots + \alpha_N y_N| \geq B$$

pour tous les points du réseau y satisfaisant à

$$y \neq 0, \quad \max(|y_1|, |y_2|, \dots, |y_N|) \leq A.$$

Alors, pour tout choix des nombres réels $\beta_0, \beta_1, \dots, \beta_N$, il existe un point du réseau x tel que

$$|x_0 - \beta_0| \leq \frac{(N+2)!}{2B}, \quad |\alpha_1 x_0 - x_1 - \beta_1| + \dots + |\alpha_N x_0 - x_N - \beta_N| \leq \frac{(N+2)!}{2A}.$$

Supposons, en particulier, que les $N + 1$ nombres $1, \alpha_1, \alpha_2, \dots, \alpha_N$ soient linéairement indépendants sur le corps des rationnels. Alors, pour tout nombre arbitrairement grand $A > 0$, il existe un nombre $B > 0$ satisfaisant à l'hypothèse du théorème. Par conséquent, les N quantités

$$|\alpha_k x_0 - x_k - \beta_k| \quad (k = 1, 2, \dots, N)$$

peuvent simultanément être rendues inférieures à tout nombre prescrit $\epsilon > 0$ par un choix convenable du point du réseau x . De plus, si J est un intervalle quelconque de longueur $\frac{(N+2)!}{B}$, il existe un point du réseau x possédant cette propriété pour lequel $x_0 \in J$.

4. Pour la seconde application, posons $n = N$ et désignons par $\alpha_1, \alpha_2, \dots, \alpha_N$ un ensemble de N nombres réels où $\alpha_N \neq 0$. Soient de plus A et B deux nouveaux paramètres positifs. Les deux expressions

$$F(x) = \frac{A}{|\alpha_N|} (|\alpha_N x_1 - \alpha_1 x_N| + \dots + |\alpha_N x_{N-1} - \alpha_{N-1} x_N|) + \frac{B}{|\alpha_N|} |x_N|$$

et

$$F^*(y) = \max \left(\frac{|y_1|}{A}, \dots, \frac{|y_{N-1}|}{A}, \frac{|\alpha_1 y_1 + \dots + \alpha_N y_N|}{B} \right)$$

forment alors une paire de fonctions de distance polaires réciproques. Désignons par $m^{(1)}, \dots, m^{(N)}$ et $m^{*(1)}, \dots, m^{*(N)}$ les deux ensembles correspondants de minima successifs.

On supposera à nouveau que

$$F^*(y) \geq 1 \quad \text{pour tous les points du réseau } y \neq 0,$$

de sorte que

$$m^{*(1)} \geq 1.$$

D'après la formule (6), il existe alors pour chaque point x^0 un point du réseau x satisfaisant à l'inégalité

$$F(x - x^0) \leq \frac{N \cdot N!}{2}. \quad (7)$$

Supposons que x satisfasse à l'inégalité (7). Alors

$$\sum_{k=1}^{N-1} |\alpha_N(x_k - x_k^0) - \alpha_k(x_N - x_N^0)| \leq \frac{(N+1)!|\alpha_N|}{2A}, \quad (8)$$

$$|x_N - x_N^0| \leq \frac{(N+1)!|\alpha_N|}{2B}.$$

Désignons par $x_0, \beta_1, \beta_2, \dots, \beta_N$ un ensemble de $N+1$ nombres réels et posons

$$\lambda_k = \alpha_k x_0 - x_k - \beta_k \quad (k = 1, 2, \dots, N).$$

Alors

$$x_k - x_k^0 = \alpha_k x_0 - x_k^0 - \beta_k - \lambda_k$$

et par conséquent

$$\alpha_N(x_k - x_k^0) - \alpha_k(x_N - x_N^0) = \alpha_k(x_N^0 + \beta_N) - \alpha_N(x_k^0 + \beta_k) + (\alpha_k \lambda_N - \alpha_N \lambda_k).$$

Afin d'établir un résultat simple, nous fixons finalement $x_1^0, x_2^0, \dots, x_{N-1}^0$ en fonction de $x_0, \beta_1, \beta_2, \dots, \beta_N$ en posant

$$x_k^0 = \frac{\alpha_k}{\alpha_N}(x_N^0 + \beta_N) - \beta_k \quad (k = 1, 2, \dots, N-1)$$

puis en définissant x_0 par l'équation

$$\lambda_N = \alpha_N x_0 - x_N - \beta_N = 0.$$

Il s'ensuit que

$$x_N - x_N^0 = \alpha_N x_0 - x_N^0 - \beta_N$$

et

$$\alpha_N(x_k - x_k^0) - \alpha_k(x_N - x_N^0) = -\alpha_N \lambda_k \quad (k = 1, 2, \dots, N-1).$$

En vertu de $\lambda_N = 0$, les formules (8) impliquent donc que

$$\sum_{k=1}^N |\lambda_k| = \sum_{k=1}^N |\alpha_k x_0 - x_k - \beta_k| \leq \frac{(N+1)!}{2A}$$

et

$$|\alpha_N x_0 - x_N^0 - \beta_N| \leq \frac{(N+1)!|\alpha_N|}{2B}.$$

Dans la première de ces inégalités, les paramètres x_N^0 et β_N sont encore à notre disposition. Nous choisissons leurs valeurs de telle sorte que la quantité

$$d = \frac{x_N^0 + \beta_N}{\alpha_N}$$

soit égale à un nombre prescrit quelconque. Le résultat final est donc le suivant.

Théorème 2. *Soient $\alpha_1, \alpha_2, \dots, \alpha_N$, $A > 0$ et $B > 0$ des nombres réels tels que $\alpha_N \neq 0$, et que*

$$|\alpha_1 y_1 + \dots + \alpha_N y_N| \geq B$$

pour tous les points du réseau y satisfaisant à

$$y \neq 0, \quad \max(|y_1|, |y_2|, \dots, |y_{N-1}|) \leq A.$$

Alors, pour chaque choix des $N + 1$ nombres réels $\beta_1, \beta_2, \dots, \beta_N$ et d , il existe un point du réseau x et un nombre réel x_0 pour lesquels

$$d \leq x_0 \leq d + \frac{(N+1)!}{B}, \quad \sum_{k=1}^N |\alpha_k x_0 - x_k - \beta_k| \leq \frac{(N+1)!}{2A}.$$

Supposons, en particulier, que les N nombres $\alpha_1, \alpha_2, \dots, \alpha_N$ soient linéairement indépendants sur le corps des rationnels. Alors $\alpha_N \neq 0$, et pour tout nombre arbitrairement grand $A > 0$, il existe un nombre $B > 0$ satisfaisant à l'hypothèse du théorème. Par conséquent, les N quantités

$$|\alpha_k x_0 - x_k - \beta_k| \quad (k = 1, 2, \dots, N)$$

peuvent simultanément être rendues inférieures à tout nombre prescrit $\epsilon > 0$ par un choix convenable du point du réseau x et du nombre réel x_0 . De plus, pour tout intervalle J de longueur $\frac{(N+1)!}{B}$, il existe une telle solution x, x_0 avec $x_0 \in J$.

Les démonstrations des théorèmes 1 et 2 expliquent très clairement pourquoi des conditions différentes doivent être imposées à $\alpha_1, \alpha_2, \dots, \alpha_N$ selon que l'on exige une solution avec un x_0 entier ou seulement avec un x_0 réel.

Australian National University
Canberra, A.C.T.
(Reçu le 20 avril 1966)