HASSAN SAFFARI

Conjecture de Minkowski et la décomposition des matrices

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 4 (1962-1963), exp. n° 12, p. 1-9
<http://www.numdam.org/item?id=SDPP_1962-1963__4__A10_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
4e année, 1962/63, n° 12

11 février 1963

CONJECTURE DE MINKOWSKI ET LA DÉCOMPOSITION DES MATRICES

par Hassan SAFFARI

1. - La conjecture suivante est attribuée à MINKOWSKI :

Etant données n formes linéaires à coefficients réels

$$\sum_{j=1}^{n} a_{ij}\, x_j \qquad (i = 1 , 2 , \ldots , n)$$

quel que soit le point $\alpha = (\alpha_1 , \ldots , \alpha_n) \in \underset{\sim}{R}^n$, il existe un point $x = (x_1 , x_2 , \ldots , x_n) \in \underset{\sim}{Z}^n$ tel que :

$$\Big| \prod_{i=1}^{n} \Big(\sum_{j=1}^{n} a_{ij}\, x_j + \alpha_i \Big) \Big| \leqslant 2^{-n} |\Delta|$$

où $\Delta \neq 0$ est le déterminant des coefficients des n formes. Si tous les coefficients sont rationnels la proposition est vraie (voir par exemple [1], page 322); dans le cas général, il existe plusieurs démonstrations pour $n = 2$, 3 démonstrations pour $n = 3$ et une démonstration pour $n = 4$ (voir [6], ou [1] chapitre 11).

En 1961, A. M. MACBEATH a démontré le théorème général suivant [4] :

Si la matrice des coefficients des n formes est décomposable sous la forme DOTU, la conjecture de Minkowski est vraie ; où

D est une matrice diagonale,

O une matrice orthogonale,

T une matrice unitriangulaire supérieure (c'est-à-dire, triangulaire supérieure dont les éléments diagonaux sont unités).

U est une matrice unimodulaire.

L'auteur pose alors, la question suivante :

Est-ce que toute matrice réelle et régulière est décomposable sous cette forme ?

Dans ce qui suit, après avoir démontré le théorème de Macbeath, je montre que la réponse à cette question est affirmative pour $n = 2$ (ce qui donne une démonstration de plus pour le cas $n = 2$ de la conjecture de Minkowski), mais en général négative pour n impaire $\neq 1$.

2. - Soit $x = (x_1, x_2, \ldots, x_n) \in \underset{\sim}{R}^n$, appelons Πx la valeur absolue du produit des coordonnées de x, et "Matrice de Minkowski" toute matrice $n\times n$, régulière, M, telle que à tout point $a \in \underset{\sim}{R}^n$ correspond un point $x \in \underset{\sim}{Z}^n$ vérifiant la relation

$$\Pi\,(Mx - a) \leq 2^{-n}|M|$$

ce qui est une formulation de la conjecture de Minkowski.

THÉORÈME de Macbeath. - <u>Toute matrice de la forme</u> DOTU <u>est une matrice de Minkowski.</u>

LEMME 1. - Si M est une matrice de Minkowski, MU l'est aussi.

En effet le groupe unimodulaire est le groupe des automorphismes du réseau des points à coordonnées entières, donc la multiplication par U ne fait que remplacer le point x par un autre point de $\underset{\sim}{Z}^n$.

LEMME 2. - Si M est une matrice de Minkowski DM l'est aussi.

En effet, on a :

$$\Pi\, D\mathfrak{M} = |D|\ \Pi\, \mathfrak{M} \tag{1}$$

où $\mathfrak{M}$ est un vecteur quelconque.

Si $a \in \underset{\sim}{R}^n$, on a aussi $D^{-1}a \in \underset{\sim}{R}^n$ et, d'après l'hypothèse,

$$\Pi\,(Mx - D^{-1}a) \leq 2^{-n}|M| .$$

Appliquons (1) en y remplaçant le vecteur $\mathfrak{M}$ par $Mx - D^{-1}a$, nous aurons :

$$\Pi\,(DMx - a) = |D|\ \Pi\,(Mx - D^{-1}a) \leq 2^{-n}|DM| .$$

<u>Démonstration du théorème.</u> - D'après les lemmes 1 et 2, il suffit de montrer que toute matrice de la forme OT est une matrice de Minkowski. Soient $e_1, e_2, \ldots, e_n$ les vecteurs colonnes de O et

$$T = \begin{pmatrix} 1 & t_{12} & \ldots & t_{1,n-1} & t_{1n} \\ 0 & 1 & \ldots & t_{2n-1} & t_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & t_{n-1n} \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

Si $a \in \underset{\sim}{R}^n$ et $x = (x_1, \dots, x_n) \in \underset{\sim}{R}^n$, comme $e_1, \dots, e_n$ forment un système orthonormé on a

$$a = \alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n$$

et

$$a - OTx = \beta_1 e_1 + \dots + \beta_n e_n$$

et un calcul immédiat donne :

$$\begin{aligned} \beta_n &= \alpha_n - x_n \\ \beta_{n-1} &= \alpha_{n-1} - x_{n-1} - t_{n-1n} x_n \\ &\dots \\ \beta_1 &= \alpha_1 - x_1 - t_{12} x_2 - \dots - t_{1n} x_n . \end{aligned}$$

Choisissons un entier x_n tel que $|\beta_n| \leqslant \frac{1}{2}$, puis l'entier x_{n-1} tel que $|\beta_{n-1}| \leqslant \frac{1}{2}$, etc.

Alors $x \in \underset{\sim}{Z}^n$, et on a

$$|a - OTx|^2 = \beta_1^2 + \dots + \beta_n^2 \leqslant \frac{n}{4} .$$

Appliquons l'inégalité entre la moyenne arithmétique et la moyenne géométrique, et on trouve

$$\Pi\ (OTx - a) \leqslant 2^{-n} = 2^{-n} |OT|$$

et le théorème est démontré.

3. Problème de décomposition.

LEMME 3. - Une condition nécessaire et suffisante pour que la matrice réelle et régulière A soit décomposable sous la forme DOTU, c'est qu'il existe une matrice unimodulaire U' et une matrice unitriangulaire supérieure T', telles que $AU'T'$. Soit une matrice dont les vecteurs lignes sont deux à deux orthogonaux.

Démonstration.

1° Soit $A = DOTU$, on a $AU^{-1} T^{-1} = DO$. Mais U^{-1} est unimodulaire et T^{-1} unitriangulaire supérieure et les vecteurs lignes de DO sont deux à deux orthogonaux, donc la condition est nécessaire.

2° Soit $AU'T' = B$, B ayant des vecteurs lignes deux à deux orthogonaux et soit ${}^tB$ la transposée de B, on a $B\,{}^tB = D_1$, où D_1 est une matrice diagonale aux éléments positifs, donc on peut poser $D_1 = D^2$. Il en résulte

$$AU'T'\ {}^tT'\ {}^tU'\ {}^tA = D^2$$

donc

$$(D^{-1}\ AU'T')({}^tT'\ {}^tU'\ {}^tA\ {}^tD^{-1}) = I$$

ce qui montre que la matrice $D^{-1}\ AU'T'$ est orthogonale et

$$D^{-1}\ AU'T' = O \implies A = DOTU$$

avec $U = U'^{-1}$ et $T = T'^{-1}$. La condition est donc suffisante.

Cela posé, supposons :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

avec $\Delta = |A| \neq 0$ et appelons $a_1, a_2, \dots, a_n$ ses vecteurs lignes qui sont des vecteurs réels.

$$U' = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & {}_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$$

avec $|U'| = \pm 1$, et appelons $\alpha_1, \alpha_2, \dots, \alpha_n$ des vecteurs colonnes qui sont des vecteurs à coordonnées entières, et

$$T' = \begin{pmatrix} 1 & x_{21} & x_{31} & \cdots & x_{n1} \\ 0 & 1 & x_{32} & \cdots & x_{n2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \quad \text{avec} \quad |T'| = +1$$

on a

$$AU' = \begin{pmatrix} a_1 \cdot \alpha_1 & a_1 \cdot \alpha_2 & \cdots & a_1 \cdot \alpha_n \\ a_2 \cdot \alpha_1 & a_2 \cdot \alpha_2 & \cdots & a_2 \cdot \alpha_n \\ \cdots & \cdots & \cdots & \cdots \\ a_n \cdot \alpha_1 & a_n \cdot \alpha_2 & \cdots & a_n \cdot \alpha_n \end{pmatrix}$$

où $a_i \circ \alpha_j$ indique le produit scalaire des deux vecteurs a_i et α_j

$$M = AU'T' = \begin{pmatrix} a_1\circ\alpha_1 & (a_1\circ\alpha_1)x_{21}+(a_1\circ\alpha_2) & \cdots & (a_1\cdot\alpha_1)x_{n1}+(a_1\circ\alpha_2)x_{n2}+\cdots+(a_1\circ\alpha_n) \\ a_2\circ\alpha_1 & (a_2\circ\alpha_1)x_{21}+(a_2\circ\alpha_2) & \cdots & (a_2\cdot\alpha_1)x_{n1}+(a_2\circ\alpha_2)x_{n2}+\cdots+(a_2\cdot\alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ a_n\circ\alpha_1 & (a_n\circ\alpha_1)x_{21}+(a_n\cdot\alpha_2) & \cdots & (a_n\circ\alpha_1)x_{n1}+(a_n\cdot\alpha_2)x_{n2}+\cdots+(a_n\cdot\alpha_n) \end{pmatrix}.$$

En écrivant, par exemple, que les produits scalaires des vecteurs lignes de cette matrice, deux à deux, sont nuls, on obtient un système de $\frac{n(n-1)}{2}$ équations du second degré, en $\frac{n(n-1)}{2}$ variables $x_{21}, \ldots, x_{n,n-1}$, et il s'agit de voir s'il est possible de choisir les paramètres entiers $\alpha_{11}, \ldots, \alpha_{nn}$ de façon que le déterminant $|U'|$ de ces paramètres soit égal à ± 1 et que le système considéré ait au moins une solution réelle.

Remarquons que $|M| = \pm \Delta$, le signe $\pm$ correspondant au signe du déterminant de la matrice unimodulaire.

4. Cas $n = 2$.

THÉORÈME 2. - Toute matrice A d'ordre 2, régulière et aux éléments réels peut être décomposée sous la forme DOTU.

LEMME 4. - $\alpha_{11}, \ldots, \alpha_{1n}$ étant n entiers tels que $[\alpha_{11}, \ldots, \alpha_{1n}] = \pm 1$, on peut former des matrices unimodulaires dont α_1 soit le premier vecteur colonne.

Pour la démonstration, voir par exemple [7], page 6.

LEMME 5. - Etant données n formes linéaires $(a_i\cdot\alpha_1)$ $(i = 1, 2, \ldots, n)$ avec $|A| = |a_{ij}| \neq 0$, il existe $\alpha_1 \in \mathbb{Z}^n$ tel que

$$\prod_i |a_i\circ\alpha_1| \leq \frac{n!}{n^n} |A| .$$

Pour la démonstration, voir [3] théorème 450, ou [1] page 82.

Démonstration du théorème 2. - Ecrivons que le produit scalaire des lignes de la matrice

$$M = \begin{pmatrix} a_1\cdot\alpha_1 & (a_1\cdot\alpha_1)\ x + (a_1\cdot\alpha_2) \\ a_2\cdot\alpha_1 & (a_2\circ\alpha_1)\ x + (a_2\cdot\alpha_2) \end{pmatrix}$$

est nul ; on obtient l'équation du second degré :

$$(a_1 \cdot \alpha_1)(a_2 \cdot \alpha_1)x^2 + [(a_1 \cdot \alpha_1)(a_2 \cdot \alpha_2) + (a_2 \cdot \alpha_1)(a_1 \cdot \alpha_2)]x + (a_1 \cdot \alpha_1)(a_2 \cdot \alpha_1) + (a_1 \cdot \alpha_2)(a_2 \cdot \alpha_2) = 0.$$

Cette équation aura des racines réelles si :

$$\delta = [(a_1 \cdot \alpha_1)(a_2 \cdot \alpha_2) - (a_2 \cdot \alpha_1)(a_1 \cdot \alpha_2)]^2 - 4(a_1 \cdot \alpha_1)^2 \ (a_2 \cdot \alpha_1)^2 \geq 0$$

l'expression entre les crochets est $|M|^2$, donc on doit avoir

$$|M|^2 - 4(a_1 \cdot \alpha_1)^2 \ (a_2 \cdot \alpha_1)^2 \geq 0 \ .$$

Soit

$$|(a_1 \cdot \alpha_1)(a_2 \cdot \alpha_1)| \leq \frac{1}{2} \ |M| \ .$$

D'après le lemme 5 on peut toujours trouver α_{11} et α_{12} premiers entre eux tels que cette inégalité soit vraie, et d'après le lemme 4 on peut former la matrice unimodulaire U' .

5. Cas général.

LEMME 6. - Si $(n - 1)$ vecteurs d'un espace a'n dimensions sont deux à deux orthogonaux, la somme des carrés des n déterminants mineurs d'ordre $(n - 1)$ qu'on peut former à partir de la matrice de ces vecteurs, est égale au carré du produit des longueurs de ces vecteurs.

Au point de vue du calcul extérieur ce lemme exprime que le produit extérieur de $n - 1$ vecteurs, deux à deux orthogonaux, d'un espace à n dimensions appartient à ce même espace, et sa longueur est égale au produit des longueurs de ces vecteurs. Pourtant on peut donner facilement une démonstration directe.

LEMME 7. - Si les vecteurs ligne de la matrice $M = AU'T'$ sont deux à deux orthogonaux, le produit des éléments de la dernière colonne de cette matrice est constant, et à un signe près, égal à

$$\frac{\Delta a_1 \alpha_n \Delta a_2 \alpha_n \ldots \Delta a_n \alpha_n}{\Delta^{n-2}}$$

où Δ est le déterminant de la matrice A , $\Delta a_i \alpha_n$ le cofacteur de l'élément $a_i \cdot \alpha_n$ dans la matrice AU' .

Démonstration. - Soient ℓ_1 , ℓ_2 , ... , ℓ_n les longueurs des vecteurs ligne. Considérons $(n - 1)$ vecteurs ligne de la matrice M , et soient Δ_1 , ... , Δ_n les n déterminants mineurs du lemme 6 ; le vecteur $(\varepsilon_1 \Delta_1 , \ldots , \varepsilon_n \Delta_n)$, où $\varepsilon_i = \pm 1$ et chaque ε_i est choisi tel que $\varepsilon_i \Delta_i$ soit le cofacteur correspondant à un élément de la n-ième ligne, est colinéaire avec la n-ième ligne, car leur produit scalaire, en valeur absolue, est égal à $|\Delta| = \ell_1 \ell_2 \dots \ell_n$; c'est-à-dire, d'après le lemme 6, égal au produit de leur longueur. Remarquons que le cofacteur de l'élément $(a_j.\alpha_1) x_{n1} + \dots + (a_j.\alpha_n)$ est égal au cofacteur de l'élément $a_j.\alpha_n$ de la matrice AU', on a donc :

$$\left|\frac{(a_j.\alpha_1) x_{n1} + (a_j.\alpha_2) x_{n2} + \dots + (a_j.\alpha_n)}{\Delta_{a_j\alpha_n}}\right| = \frac{\ell_j}{\ell_1 \ell_2 \dots \ell_{j-1} \ell_{j+1} \dots \ell_n} .$$

Si on écrit la même relation pour toutes les lignes et si on appelle P la valeur absolue du produit des éléments de la dernière colonne, on obtient

$$P = \frac{|\Delta_{a_1\alpha_n} \Delta_{a_2\alpha_n} \dots \Delta_{a_n\alpha_n}|}{(\ell_1 \ell_2 \dots \ell_n)^{n-2}} = \left|\frac{\Delta_{a_1\alpha_n} \dots \Delta_{a_n\alpha_n}}{\Delta^{n-2}}\right| .$$

THÉORÈME 3. - Si $\Delta_{a_1\alpha_n} \Delta_{a_2\alpha_n} \dots \Delta_{a_n\alpha_n} \neq 0$, où n est un nombre impair $\neq 1$, la décomposition de la matrice A sous la forme DOTU est impossible.

Démonstration. - Ecrivons que le produit scalaire de deux vecteurs ligne quelconques de M est nul. On obtient $\frac{n(n-1)}{2}$ équations :

$$(a_i.\alpha_1)(a_j.\alpha_1) + [(a_i.\alpha_1) x_{21} + (a_i.\alpha_2)][(a_j.\alpha_1) x_{21} + (a_j.\alpha_2)] + \dots$$

$$= - [(a_i.\alpha_1) x_{n1} + \dots + (a_i.\alpha_n)][(a_j.\alpha_1) x_{n1} + \dots + (a_j.\alpha_n)]$$

$$(i = 1, 2, \dots, n-1), \quad (j = 2, 3, \dots, n), \quad i < j .$$

Essayons de trouver, par multiplication de ces relations, la constante du lemme 7 au second membre. Comme n est impair, ceci n'est possible qu'en multipliant n relations, convenablement choisies ; par exemple on peut prendre

$$i = 1, 2, \dots, n-1 \text{ et } 1,$$

$$\text{respectivement } j = 2, 3, \dots, n \text{ et } n .$$

Ainsi chacun des éléments de la dernière colonne de M apparait deux fois au second membre et on trouve :

$$\prod_{\substack{i=1,2,\dots,n-1,1 \\ j=2,3,\dots,n,n}} \{(a_i.\alpha_1)(a_j.\alpha_1) + [(a_i.\alpha_1)x_{21}+(a_i.\alpha_2)][(a_j.\alpha_1)x_{21}+(a_j.\alpha_2)] + \dots\}$$

$$= (-1)^n \left[\frac{\Delta_{a_1\alpha_n} \dots \Delta_{a_n\alpha_n}}{\Delta^{n-2}}\right]^2 .$$

Il est évident que si le système précédent possède une solution, celle-ci doit vérifier cette équation. Or nous verrons que cette équation ne possède aucune racine réelle, ce qui démontre le théorème.

En effet le premier membre est le produit de n facteurs qui ne peuvent s'annuler. Comme chaque facteur est un polynôme du second degré par rapport aux variables, il conserve un signe fixe quelles que soient les valeurs de ces variables. Attribuons des valeurs numériques arbitraires à toutes les variables, sauf par exemple, à la première ; on obtient un polynôme du second degré à une variable, dont le signe est celui de $(a_i . \alpha_1)(a_j . \alpha_1)$. Ainsi le signe du produit est celui de

$$[(a_1 . \alpha_1)(a_2 . \alpha_1) \dots (a_n . \alpha_1)]^2$$

donc positif.

Mais n étant impair, le signe du second mambre est $-$, la proposition est donc démontrée.

Remarque 1. - Cette démonstration est en défaut si toutes les variables sont nulles, mais alors des considérations simples concernant le minimum d'une forme quadratique définie positive (voir [5]) montre que, même dans ce cas, la décomposition est en général impossible.

Conséquence. - Une condition nécessaire pour que la décomposition soit possible est que

$$\Delta_{a_1 \alpha_n} \Delta_{a_2 \alpha_n} \dots \Delta_{a_n \alpha_n} = 0 .$$

Remarque 2. - Supposons $C = AB$, où A, B et C sont des matrices carrées d'ordre n. Soit

$$C\begin{pmatrix} i_1 , & i_2 , & \dots , & i_p \\ j_1 , & j_2 , & \dots , & j_p \end{pmatrix}$$

le déterminant mineur d'ordre p déduit de C et composé des éléments des lignes $i_1 , i_2 , \dots , i_p$ et des colonnes $j_1 , j_2 , \dots , j_p$ de C. Alors d'après le théorème Binet-Cauchy (voir [2], tome 1, page 12) on a la formule suivante :

$$C\begin{pmatrix} i_1, i_2, \dots, i_p \\ j_1, j_2, \dots, j_p \end{pmatrix} = \sum_{1 \leq K_1 < K_2 < \dots < K_p \leq n} A\begin{pmatrix} i_1, i_2, \dots, i_p \\ K_1, K_2, \dots, K_p \end{pmatrix} B\begin{pmatrix} K_1, K_2, \dots, K_p \\ j_1, j_2, \dots, j_p \end{pmatrix}$$

Cela posé, pour que $\Delta_{a_1\alpha_n} \Delta_{a_2\alpha_n} \cdots \Delta_{a_n\alpha_n} = 0$ il est nécessaire qu'au moins un facteur, par exemple $\Delta_{a_1\alpha_n}$, soit égal à zéro. En appliquant la formule précédente à la matrice AU' on trouve

$$\sum_{1\leq K_1<K_2<\cdots<K_{n-1}\leq n} A\begin{pmatrix} 2 , & 3 , & \cdots , & n \\ K_1 , & K_2 , & \cdots , & K_{n-1} \end{pmatrix} U'\begin{pmatrix} K_1 , & K_2 , & \cdots , & K_{n-1} \\ 1 , & 2 , & \cdots , & n-1 \end{pmatrix} = 0 .$$

Comme les mineurs de la matrice unimodulaire sont des entiers, cette relation montre que les n déterminants mineurs d'ordre $n-1$, qu'on peut former avec les $n-1$ dernières lignes de A, sont linéairement dépendants sur les entiers rationnels.

BIBLIOGRAPHIE

[1] CASSELS (J. W. S.). - An introduction to the geometry of numbers. - Berlin, Springer-Verlag, 1959 (Die Grundlehren der mathematischen Wissenschaften, 99).

[2] GANTMAKHER (F. P.). - The theory of matrices, Vol. 1-2. - New York, Chelsea publishing Company, 1959.

[3] HARDY (G. H.) and WRIGHT (E. M.). - An introduction to the theory of numbers, 4th edition. - Oxford, at the Clarendon Press, 1958.

[4] MACBEATH (A. M.). - Factorization of matrices and Minkowski's conjecture, Proc. Glasgow math. Ass., t. 5, 1961, p. 86-89.

[5] SAFFARI (Hassan). - Réduction des formes quadratiques définies-positives, Séminaire Delange-Pisot : Théorie des nombres, t. 2, 1960/61, n° 9, 30 p.

[6] SAFFARI (Hassan). - Problèmes non-homogènes de la géométrie des nombres, Séminaire Delange-Pisot : Théorie des nombres, t. 3, 1961/62, n° 6, 18 p.

[7] WATSON (G. L.). - Integral quadratic forms. - Cambridge, at the University Press, 1960 (Cambridge Tracts in Mathematics and mathematical Physics, 51).