Séminaire Delange-Pisot-Poitou.
Théorie des nombres

HASSAN SAFFARI

Conjecture de Minkowski sur le corps des complexes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 5 (1963-1964), exp. nº 11, p. 1-13

<http://www.numdam.org/item?id=SDPP_1963-1964__5__A8_0>

CONJECTURE DE MINKOWSKI SUR LE CORPS DES COMPLEXES

par Hassan SAFFARI

La conjecture suivante, que nous appelons "proposition A", est attribuée à MINKOWSKI :

PROPOSITION (A). - Etant données n formes linéaires

$$\sum_{j=1}^{n} \alpha_{ij}\, x_j \qquad (i = 1\,,\, 2\,,\, \ldots\,,\, n) \qquad \text{où} \quad \alpha_{ij} \in \underset{\sim}{R}\,,$$

à tout point $a = (a_1\,,\, \ldots\,,\, a_n) \in \underset{\sim}{R}^n$ correspond au moins un point $X = (x_1\,,\, \ldots\,,\, x_n) \in \underset{\sim}{Z}^n$ tel que

$$\prod_{i=1}^{n} \Big| \sum_{j=1}^{n} \alpha_{ij}\, x_j + a_i \Big| \leqslant \frac{|\Delta|}{2^n}\,,$$

où $\Delta = |\alpha_{ij}| \neq 0$ est le déterminant des coefficients des n formes.

Cette proposition a été démontrée pour $n = 2$, 3 et 4 (voir [11]).

Dans ce qui suit, nous donnons d'abord une équivalente de cette conjecture sur le corps des complexes, puis nous étudions certains cas où cette conjecture équivalente est vraie :

PROPOSITION (B). - Etant données n formes linéaires

$$\sum_{j=1}^{n} \beta_{ij}\, z_j \qquad (i = 1\,,\, 2\,,\, \ldots\,,\, n) \qquad \text{où} \quad \beta_{ij} \in \underset{\sim}{C}\,,$$

à tout point $b = (b_1\,,\, \ldots\,,\, b_n) \in \underset{\sim}{C}^n$ correspond au moins un point $Z = (z_1\,,\, \ldots\,,\, z_n)$, dont les coordonnées sont les entiers d'un corps quadratique imaginaire $K(i\sqrt{m})$, tel que

$$\prod_{i=1}^{n} \Big| \sum_{j=1}^{n} \beta_{ij}\, z_j + b_i \Big| \leqslant \begin{cases} \dfrac{(m+1)^{n/2}}{2^n}\, |\Delta| & \text{si} \quad m \equiv 1 \quad \text{ou} \quad 2 \pmod 4 \\[2ex] \dfrac{(m+4)^{n/2}}{4^n}\, |\Delta| & \text{si} \quad m \equiv 3 \pmod 4 \end{cases}$$

où $|\Delta| \neq 0$ est le module du déterminant de la matrice des coefficients.

Cette proposition qui, sous sa forme générale, est nouvelle a été démontrée dans les cas $n = 2$, $m = 2$ (voir [4] , [1] , [8] et [9]) et $n = 2$, $m = 3$ [8].

THÉORÈME 1. - (B) $\Longrightarrow$ (A) .

<u>Démonstration</u>. - Considérons, par exemple, le cas où les coordonnées du point Z appartiennent au corps de Gauss $K(i)$. Supposons que les $\beta_{ij} = \alpha_{ij}$ sont tous réels, et appliquons la proposition (B) au point $b = a + ia$ où $a \in \underset{\sim}{R}^n$; on a alors :

$$\prod_{i=1}^{n} \left| \sum_{j=1}^{n} \alpha_{ij} z_j + a_i + ia_i \right| \leqslant \frac{|\Delta|}{2^{n/2}} \qquad (^*)$$

Soit $z_j = x_j + iy_j$, où x_j et y_j sont des entiers rationnels ; on a alors

$$\prod_{i=1}^{n} \left| \left(\sum_{j=1}^{n} \alpha_{ij} x_j + a_i\right) + i\left(\sum_{j=1}^{n} \alpha_{ij} y_j + a_i\right) \right| \leqslant \frac{|\Delta|}{2^{n/2}} ,$$

soit

$$\prod_{i=1}^{n} \left| \left(\sum_{j=1}^{n} \alpha_{ij} x_j + a_i\right) + i\left(\sum_{j=1}^{n} \alpha_{ij} y_j + a_i\right) \right|^2 \leqslant \frac{|\Delta|^2}{2^{n}} ;$$

mais, pour tout i , on a :

$$\left| \left(\sum_{j=1}^{n} \alpha_{ij} x_j + a_i\right) + i\left(\sum_{j=1}^{n} \alpha_{ij} y_j + a_i\right) \right|^2 \geqslant 2 \left| \sum_{j=1}^{n} \alpha_{ij} x_j + a_i \right| \left| \sum_{j=1}^{n} \alpha_{ij} y_j + a_i \right| ,$$

donc :

$$\prod_{i=1}^{n} \left| \sum_{j=1}^{n} \alpha_{ij} x_j + a_i \right| \prod_{i=1}^{n} \left| \sum_{j=1}^{n} \alpha_{ij} y_j + a_i \right| \leqslant \frac{|\Delta|^2}{2^{2n}} .$$

Cette inégalité montre que l'un au moins des 2 produits du premier membre est $\leqslant \frac{|\Delta|}{2^n}$.

D'après le théorème 1, à toute proposition concernant le cas complexe correspond une proposition pour le cas réel.

Le théorème suivant est une généralisation d'un théorème de A. M. MACBEATH [7] ou [12].

THÉORÈME 2. - Si la matrice des coefficients des n formes est décomposable sous la forme DUTV où :

(*) On a employé le même symbole i pour $\sqrt{-1}$ et l'indice, mais cela ne prête à aucune confusion.

D est une matrice diagonale,

U est une matrice unitaire (c'est-à-dire $U^{-1} = \overline{U}^*$),

T est une matrice diagonale supérieure dont tous les éléments diagonaux ont même module,

V est une matrice unimodulaire, dont les éléments sont les entiers du corps quadratique $K(i\sqrt{m})$ considéré,

alors la proposition (B) est vraie.

La démonstration de ce théorème repose sur les 3 lemmes suivants :

LEMME 1. - Si la proposition (B) est vraie pour n formes dont la matrice des coefficients est M , elle est également vraie pour n formes dont la matrice des coefficients est DM , où D est une matrice diagonale.

LEMME 2. - Si la proposition (B) est vraie pour n formes dont la matrice des coefficients est M , elle est également vraie pour n formes dont la matrice des coefficients est MV , où V est unimodulaire et ses éléments appartiennent au corps quadratique $K(i\sqrt{m})$.

LEMME 3. - La proposition (B) est vraie pour n formes dont la matrice des coefficients est de la forme UT , où U est une matrice unitaire et T une matrice triangulaire supérieure dont tous les éléments diagonaux ont même module.

<u>Démonstration du lemme</u> 1. - Etant donné un vecteur X de $\underset{\sim}{C}^n$ ou de $\underset{\sim}{R}^n$, nous appelons $\Pi(X)$ le produit des modules de toutes ses coordonnées :

$$\Pi(X) = |x_1 \; x_2 \; \ldots \; x_n|$$

et

$$|X| = (|x_1|^2 + \ldots + |x_n|^2)^{1/2} .$$

L'inégalité entre la moyenne arithmétique et la moyenne géométrique entraîne :

$$\frac{|X|^2}{n} \geqslant (\Pi(X))^{2/n} . \tag{1}$$

Il est évident que si, pour un certain vecteur X , on a

$$\Pi(X) \leqslant d ,$$

où d est une certaine constante, on a également

$$\Pi(DX) \leqslant |D| d , \tag{2}$$

où D est une matrice diagonale et $|D|$ le module de son déterminant.

Cela posé, pour démontrer le lemme 1, il suffit d'écrire la proposition (B) pour un point $D^{-1} b$, puis appliquer la relation (2) où le vecteur X a pour coordonnées

$$\sum_{j=1}^{n} \beta_{ij} z_j + d_i^{-1} b_i \qquad (i = 1, 2, \ldots, n),$$

et les d_i^{-1} sont les éléments de D^{-1}.

<u>Démonstration du lemme</u> 2. - Ce lemme est évident en remarquant que, si a est un vecteur dont les coordonnées sont des entiers d'un certain corps, l'équation $VX = a$, où V est une matrice unimodulaire dont les éléments sont des entiers du même corps, possède une solution entière dans le même corps.

<u>Démonstration du lemme</u> 3. - Soit

$$T = \begin{pmatrix} t_{11} & t_{12} & \cdots & \cdots & t_{1n} \\ 0 & t_{22} & \cdots & \cdots & t_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & t_{n-1,n-1} & t_{n-1,n} \\ 0 & \cdots & \cdots & 0 & t_{nn} \end{pmatrix}$$

où on a

$$|t_{11}| = |t_{22}| = \cdots = |t_{nn}| = d .$$

D'après la notation employée au début de la démonstration du lemme 1, il suffit de démontrer l'existence d'un vecteur entier Z tel qu'on ait :

$$\prod(UTZ + b) \leqslant \begin{cases} \dfrac{(m+1)^{n/2}}{2^n} |UT| & \text{si } m \equiv 1 \text{ ou } 2 \pmod 4 \\[2ex] \dfrac{(m+4)^{n/2}}{4^n} |UT| & \text{si } m \equiv 3 \pmod 4 . \end{cases}$$

Les vecteurs colonnes de la matrice unitaire U forment un système orthonormé ; projetons le vecteur $UTZ + b$ sur ce système. Soient $\beta_1, \beta_2, \ldots, \beta_n$ les coordonnées du vecteur b ; on vérifie immédiatement que les coordonnées du vecteur $UTZ + b$ dans ce nouveau système sont les suivantes :

$$\begin{aligned}
\gamma_1 &= t_{11}\, z_1 + t_{12}\, z_2 + \dots + t_{1n}\, z_n + \beta_1 \\
\gamma_2 &= \qquad\quad t_{22}\, z_2 + \dots + t_{2n}\, z_n + \beta_2 \\
&\dots \\
\gamma_{n-1} &= \qquad t_{n-1,n-1}\, z_{n-1} + t_{n-1,n}\, z_n + \beta_{n-1} \\
\gamma_n &= \qquad\qquad\qquad t_{nn}\, z_n + \beta_n \quad ;
\end{aligned}$$

on a alors :

$$|\gamma_n| = |t_{nn}|\,|z_n + \frac{\beta_n}{t_{nn}}| = d|z_n + \frac{\beta_n}{t_{nn}}| \ .$$

Si $m \equiv 1$ ou $2 \pmod 4$, les entiers du corps quadratique $K(i\sqrt{m})$ sont de la forme $x + iy\sqrt{m}$ où x et y sont des entiers rationnels ; alors si on pose

$$\frac{\beta_n}{t_{nn}} = p + iq \qquad (\ p \ \text{ et } \ q \ \text{ réels quelconques}),$$

on a

$$|z_n + \frac{\beta_n}{t_{nn}}| = |(x + p) + i\sqrt{m}(y + \frac{q}{\sqrt{m}})| \ ,$$

et on peut choisir les entiers x et y tels que

$$|x + p| \leqslant \frac{1}{2} \ , \quad |y + \frac{q}{\sqrt{m}}| \leqslant \frac{1}{2} \ ;$$

donc

$$|z_n + \frac{\beta_n}{t_{nn}}| \leqslant \frac{(m+1)^{1/2}}{2} \ .$$

Ainsi, on peut choisir l'entier z_n tel que

$$|\gamma_n| \leqslant \frac{d(m+1)^{1/2}}{2} \ ;$$

ayant choisi z_n , on peut ensuite choisir z_{n-1} tel que

$$|\gamma_{n-1}| \leqslant \frac{d(m+1)^{1/2}}{2} \ ;$$

puis, de proche en proche, $z_{n-2}, \dots, z_1$ tels que $|\gamma_{n-2}|, \dots, |\gamma_1|$ vérifient la même inégalité.

Si $m \equiv 3 \pmod 4$, les entiers du corps quadratique sont de la forme $x - \frac{y}{2} + \frac{iy}{2}\sqrt{m}$ où x et y sont toujours des entiers rationnels ; on a donc :

$$|z_n + \frac{\beta_n}{t_{nn}}| = |(x - \frac{y}{2} + p) + \frac{i\sqrt{m}}{2}(y + \frac{2q}{\sqrt{m}})| .$$

Dans ce cas, on peut choisir d'abord y , puis x , tels que :

$$|y + \frac{2q}{\sqrt{m}}| \leqslant \frac{1}{2} , \qquad |x - \frac{y}{2} + p| \leqslant \frac{1}{2} ,$$

ce qui entraîne

$$|\gamma_n| \leqslant \frac{d(m+4)^{1/2}}{4} .$$

Puis on choisit z_{n-1} , ... , z_1 tels que $|\gamma_{n-1}|$, ... , $|\gamma_1|$ vérifient la même inégalité ; on a ainsi dans l'un ou l'autre système de coordonnées :

$$|UTZ + b|^2 \leqslant \begin{cases} \dfrac{nd^2(m+1)}{4} & \text{si } m \equiv 1 \text{ ou } 2 \pmod 4 \\ \dfrac{nd^2(m+4)}{16} & \text{si } m \equiv 3 \pmod 4 . \end{cases}$$

L'inégalité (1) entraîne alors :

$$\Pi(UTZ) + b) \leqslant \begin{cases} \dfrac{(m+1)^{n/2}}{2^n} d^n & \text{si } m \equiv 1 \text{ ou } 2 \pmod 4 \\ \dfrac{(m+4)^{n/2}}{4^n} d^n & \text{si } m \equiv 3 \pmod 4 . \end{cases}$$

Compte tenu de ce que $|UT| = d^n$, le lemme 3 est démontré.

Remarque importante. - La validité du lemme 3 ne dépend pas de la forme triangulaire supérieure de la matrice T , mais plutôt de l'existence d'une approximation simultanée pour les n formes non homogènes γ_1 , γ_2 , ... , γ_n ; donc le lemme 3, ainsi que le théorème 2, restent valables lorsqu'on remplace la matrice T par une autre matrice déduite de T par un changement de lignes ou de colonnes, et en particulier pour une matrice triangulaire inférieure ou pseudotriangulaire supérieure ou inférieure. Cependant, il faut remarquer que toutes ces matrices se déduisent de T en la multipliant, à gauche ou à droite, par une matrice unimodulaire ; donc, on ne trouve pas un théorème plus général que le théorème 2. Au contraire, s'il existe une matrice B à coefficients complexes :

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

qui ne soit pas le produit d'une matrice triangulaire supérieure (vérifiant la condition $|t_{11}| = |t_{22}| = \dots = |t_{nn}|$) et d'une matrice unimodulaire, et telle qu'il existe n entiers $z_1 , \dots , z_n$ d'un corps quadratique vérifiant le système

$$|\beta_{j1} z_1 + \beta_{j2} z_2 + \dots + \beta_{jn} z_n + b_j| \leqslant C \sqrt[n]{|\Delta|} \quad (j = 1 , 2 , \dots , n) , \ \Delta = |B| \neq 0 \tag{3}$$

$$C = \begin{cases} \dfrac{(m+1)^{1/2}}{2} & \text{si } m \equiv 1 \text{ ou } 2 \pmod 4 \\[2ex] \dfrac{(m+4)^{1/2}}{4} & \text{si } m \equiv 3 \pmod 4 \end{cases} .$$

Alors, la proposition est valable pour toute matrice de la forme DUBV , et on trouve un théorème plus général que le théorème 2.

Je dois affirmer que, dans les exemples concrets que j'ai pu construire, les matrices vérifiant la condition (3) sont toujours le produit d'une matrice triangulaire de la forme précédente et d'une matrice unimodulaire, de façon que je ne sais rien sur l'existence d'autres matrices vérifiant la relation (3).

THÉORÈME 3. - Si tous les coefficients des n formes appartiennent à un même corps quadratique imaginaire et euclidien, la proposition (B) est vraie avec des entiers appartenant au corps des coefficients.

Remarque préliminaire. - On sait qu'il existe exactement 5 corps quadratiques imaginaires et euclidiens $K(i\sqrt{m})$, à savoir

$$m = 1 , 2 , 3 , 7 \text{ et } 11 .$$

Démonstration. - On peut toujours supposer que tous les coefficients sont des entiers d'un tel corps ; sinon, A étant la matrice des coefficients, il existe une matrice scalaire D' telle que

$$A = D' A'$$

et que A' soit à coefficients entiers. On applique à la matrice A' le procédé ordinaire de triangulation des matrices à coefficients entiers rationnels, qui consiste en l'application de l'algorithme d'Euclide, et on trouve ainsi

$$A' = T' V$$

où V est unimodulaire. Enfin, par une infinité de manières, on peut choisir une matrice diagonale D'' telle que

$$T' = D'' T$$

où T vérifie la condition

$$|t_{11}| = \dots = |t_{nn}| ;$$

on a donc

$$A = D' D'' TV = DTV .$$

Il suffit alors d'appliquer le théorème 2, où on remplace U par la matrice identique.

COROLLAIRE. - La proposition (A) est vraie si les coefficients des n formes réelles appartiennent au corps des rationnels.

THÉORÈME 4. - Si la proposition (B) est vraie pour tout système de r formes à r variables, alors elle est également vraie pour un système de n formes à n variables $(n > r)$, à condition que les coefficients de $n - r$ de ces formes appartiennent à un même corps quadratique imaginaire euclidien.

Remarque préliminaire. - D'après J. W. S. CASSELS, ce théorème a été démontré, pour les formes réelles, par un mathématicien Soviétique, KARANIKOLOV (voir [6]).

Démonstration. - La matrice des coefficients des n formes peut être écrite sous la forme suivante :

$$A = \begin{pmatrix} \beta_{11} & \beta_{12} & \dots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \dots & \beta_{2n} \\ \dots & \dots & \dots & \dots \\ \beta_{n-r,1} & \beta_{n-r,2} & \dots & \beta_{n-r,n} \\ \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \dots & \dots & \dots & \dots \\ \alpha_{r1} & \alpha_{r2} & \dots & \alpha_{rn} \end{pmatrix}$$

où les α sont des nombres complexes quelconques, et les β appartiennent à un même corps quadratique imaginaire euclidien. On peut toujours supposer que tous les β sont des entiers du corps quadratique considéré, car dans le cas contraire il existe une matrice scalaire D' telle que

$$A = D' A' ,$$

et que dans A' les β sont des entiers du corps.

J'applique la méthode de triangulation aux $n - r$ premières lignes de A' ;

cette méthode qui consiste en l'application de l'algarithme d'Euclide, est équivalente à la multiplication de A' , à droite, par plusieurs matrices unimodulaires. On trouve ainsi :

$$A' = A'' V$$

où les éléments de la matrice unimodulaire V appartiennent au corps $K(i\sqrt{m})$ euclidien considéré, et

$$A'' = \begin{pmatrix} \beta''_{11} & 0 & 0 & \dots & \dots & \dots & 0 \\ \beta''_{21} & \beta''_{22} & 0 & \dots & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \beta''_{n-r,1} & \beta''_{n-r,2} & \dots & \beta''_{n-r,n-r} & 0 & \dots & 0 \\ \alpha''_{11} & \alpha''_{12} & \dots & \dots & \dots & \dots & \alpha''_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha''_{r1} & \alpha''_{r2} & \dots & \dots & \dots & \dots & \alpha''_{rn} \end{pmatrix}$$

on peut toujours supposer

$$(4) \qquad |\beta''_{11}| = |\beta''_{22}| = \dots = |\alpha''_{n-r,n-r}| = d \ ,$$

car dans le cas contraire on peut choisir d'une infinité de manières une matrice diagonale D'' qui, multipliée à gauche par A'' , donne la relation (4). On trouve ainsi

$$A = DA'' V \ ,$$

où A'' vérifie la relation (4).

D'après les lemmes 1 et 2, il suffit de démontrer le théorème pour des formes dont la matrice est A'' . Pour cela, on applique exactement la méthode du lemme 3 du théorème 2 aux $n - r$ premières lignes de la matrice A'' , et on trouve ainsi $n - r$ entiers du corps considéré tels que chacune des $n - r$ formes linéaires non homogènes représentées par les $n - r$ premières lignes de A'' soit, en module, plus petite ou égale à :

$$\frac{(m+1)^{1/2}}{2} d \quad \text{si} \quad m \equiv 1 \quad \text{ou} \quad 2 \pmod 4$$

$$\frac{(m+4)^{1/2}}{4} d \quad \text{si} \quad m \equiv 3 \pmod 4) \ .$$

Si on substitue ces $n - r$ entiers dans les r formes linéaires non homogènes représentées par les r dernières lignes, on trouve r formes linéaires non homogènes à r variables pour lesquelles, par hypothèse, la propriété (B) est vraie, et on trouve ainsi

$$\prod_{i=1}^{r} \left| \sum_{j=1}^{r} \lambda_{ij} z_j + b_i \right| \leqslant \begin{cases} \dfrac{(m+1)^{r/2}}{2^r} |\delta| & \text{si } m \equiv 1 \text{ ou } 2 \pmod 4 \\ \dfrac{(m+4)^{r/2}}{4^r} |\delta| & \text{si } m \equiv 3 \pmod 4 \end{cases}$$

où les λ_{ij} sont les éléments des r dernières lignes et les r dernières colonnes de A'', et $|\delta|$ est le module du déterminant mineur composé de ces éléments.

Le théorème se démontre dans toute sa généralité si on remarque que

$$|A''| = |\beta''_{11}| |\beta''_{22}| \dots |\beta''_{n-r,n-r}| |\delta| = d^n |\delta| .$$

Il importe de savoir dans quelles conditions une certaine matrice à coefficients complexes est décomposable sous la forme DUTV. Le théorème suivant donne une condition nécessaire pour une telle décomposition.

THÉORÈME 5. - Une condition nécessaire pour qu'une matrice (α_{ij}), $|\alpha_{ij}| \neq 0$, soit décomposable sous la forme DUTV, c'est qu'il existe n entiers v_j ($j = 1, \dots, n$) appartenant au même corps quadratique que les éléments de V, tels que

$$\prod_{i=1}^{n} \left| \sum_{j=1}^{n} \alpha_{ij} v_j \right| \leqslant \frac{|\Delta|}{n^{n/2}}$$

où $|\Delta| \neq 0$ est le module du déterminant de la matrice (α_{ij}).

Dans le cas $n = 2$, cette condition est à la fois nécessaire et suffisante.

<u>Démonstration</u>. - Soit $(\alpha_{ij}) = A = DUTV$, donc

$$U = D^{-1} A V^{-1} T^{-1} .$$

Soient :

$$D^{-1} = \begin{pmatrix} \delta_1 & 0 & \dots & 0 \\ 0 & \delta_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \delta_n \end{pmatrix} , \quad A = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \alpha_{2n} \\ \dots & \dots & \dots \\ \alpha_{n1} & \dots & \alpha_{nn} \end{pmatrix}$$

$$V^{-1} = \begin{pmatrix} v_{11} & v_{21} & \cdots & v_{n1} \\ v_{12} & v_{22} & \cdots & v_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ v_{1n} & \cdots & \cdots & v_{nn} \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} t_{11} & \cdots & \cdots & t_{1n} \\ 0 & t_{22} & \cdots & t_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & t_{nn} \end{pmatrix}$$

où, pour T^{-1} comme pour T, on a $|t_{11}| = \cdots = |t_{nn}|$.

Appelons $\alpha_1, \alpha_2, \ldots, \alpha_n$ les vecteurs lignes de A, $v_1, \ldots, v_n$ les vecteurs colonnes de V^{-1}, et $(\alpha_i . v_j)$ la somme des produits 2 à 2 des coordonnées des vecteurs α_i et v_j. Chacune de ces sommes des produits est une forme linéaire homogène aux coefficients α_{ij} et aux variables v_{ji}.

Un calcul immédiat montre que les éléments de la première colonne de U sont :

$$t_{11}\, \delta_1(\alpha_1.v_1)\ ,\ t_{11}\, \delta_2(\alpha_2.v_1)\ ,\ \ldots\ ,\ t_{1n}\, \delta_n(\alpha_n.v_1)\ ;$$

on a donc les 2 relations suivantes :

(5) $$|t_{11}|^2\, [|\delta_1|^2\, |(\alpha_1.v_1)|^2 + \cdots + |\delta_n|^2\, |(\alpha_n.v_1)|^2] = 1$$

(6) $$|\delta_1\, \delta_2 \cdots \delta_n\, t_{11}\, t_{22} \cdots t_{nn}|\,|\Delta| = 1 .$$

L'inégalité entre la moyenne arithmétique et la moyenne géométrique entraîne :

$$|\delta_1|^2|(\alpha_1.v_1)|^2 + \cdots + |\delta_n|^2|(\alpha_n.v_1)|^2 \geq n(|\delta_1\, \delta_2 \cdots \delta_n|\,|\alpha_1.v_1| \cdots |\alpha_n.v_1|)^{2/n},$$

ce qui, d'après la relation (5), **entraîne** :

$$|t_{11}|^n|\delta_1\, \delta_2 \cdots \delta_n|\,|\alpha_1.v_1|\,|\alpha_2.v_1| \cdots |\alpha_n.v_1| \leqslant \frac{1}{n^{n/2}}\ ;$$

compte-tenu de la relation (6) et du fait que

$$|t_{11}|^n = |t_{11}\, t_{22} \cdots t_{nn}|\ ,$$

on trouve

(7) $$|\alpha_1.v_1|\,|\alpha_2.v_1| \cdots |\alpha_n.v_1| \leqslant \frac{|\Delta|}{n^{n/2}}\ ,$$

qui, d'après les notations employées, est équivalente à la condition de l'énoncé.

Si on écrit explicitement le produit des matrices, qui donne la valeur de U, on vérifie immédiatement que cette condition, dans le cas $n = 2$, est à la fois nécessaire et suffisante.

Le théorème précédent ramène l'étude de la possibilité d'une décomposition sous la forme DUTV , à l'étude de l'existence des solutions entières pour l'inégalité (7). Malheureusement, nos informations sur les minima arithmétiqués des produits des formes linéaires homogènes, même dans le cas réel, sont très réduites.

Dans le cas complexe, on connaît seulement certains résultats de FORD, PERRON, POITOU, etc., qui donnent, pour $n=2$, des conditions pour l'existence d'une infinité de solutions. Voir par exemple [3] et [10].

On ne connaît, même pour $n = 2$, la meilleure constante C qui assure l'existence d'au moins une solution pour l'inégalité

$$|\alpha_1 . v_1| |\alpha_2 . v_1| \leqslant C|\Delta| .$$

Il y a deux exceptions à cette affirmation :

1° Un résultat de HOFREITER (voir [5] ou [9]) montre que, dans le cas de $K(i)$, cette meilleure constante est

$$C = \frac{1}{\sqrt{2+\sqrt{3}}} ;$$

comme l'inégalité (7) exige la constante $C = \frac{1}{2}$, il en résulte que, dans le cas du corps de Gauss, la décomposition n'est pas toujours possible.

2° Le résultat classique de Hurwitz et Markoff nous assure que l'inégalité

$$|\alpha_1 . v_1| |\alpha_2 . v_1| \leqslant \frac{|\Delta|}{\sqrt{5}} ,$$

dans le cas réel, possède toujours des solutions entières, et même, d'après [2], cette inégalité possède une infinité de solutions.

On peut vérifier facilement que cette infinité de solutions assure une infinité de décomposition pour la matrice réelle, et il en résulte la proposition suivante :

COROLLAIRE. - La proposition (A) est vraie pour $n = 2$, et possède une infinité de solutions.

Conditions nécessaires et suffisantes pour la décomposition. En suivant la méthode de démonstration du théorème 5, on trouve des conditions nécessaires et suffisantes pour la décomposition d'une matrice sous la forme DUTV . En raison de l'extrême complexité des calculs et la difficulté d'une interprétation concrète de ces conditions, j'ai renoncé à les exposer.

BIBLIOGRAPHIE

[1] CHALK (John H. H.). - Rational approximations in the complex plane, II., J. London math. Soc., t. 31, 1956, p. 216-221.

[2] DAVENPORT (H.) and ROGERS (C. A.). - Diophantine inequalities with an infinity of solutions, Phil. Trans. royal Soc. London, Series A, t. 242, 1950, p. 311-344.

[3] FORD (Lester R.). - On the closeness of approach of complex rational fractions to a complex rational number, Trans. Amer. math. Soc., t. 27, 1925, p. 146-154.

[4] HLAWKA (Edmund). - Über die Approximationen von zwei komplexen inhomogenen Linearformen, Monatsh. für Math., t. 46, 1938, p. 324-334.

[5] HOFREITER (Nikolaus). - Über die Approximationen von komplexen Zahlen durch Zahlen des Körpers K(i) , Monatsh. für Math., t. 56, 1952, p. 61-74.

[6] KARANIKOLOV (Khr.). - Sur un théorème de Minkowski et Čebotarev [en russe], Uspekhi Mat. Nauk, t. 18, 1963, n° 3, p. 163-166 ; Math. Reviews, t. 27, 1964, p. 20-21.

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

[8] MAHLER (Kurt). - On the product of two complex linear polynomials in two variables, J. London math. Soc., t. 15, 1940, p. 213-236.

[9] NIVEN (I.). - Diophantine approximations. - New York, Interscience Publishers, 1963 (Interscience Tracts in pure and applied Mathematics, 14).

[10] POITOU (Georges). - Sur l'approximation des nombres complexes par les nombres des corps imaginaires quadratiques ..., Ann. scient. Ec. Norm. Sup., t. 70, 1953, p. 199-265.

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

[12] SAFFARI (Hassan). - Conjecture de Minkowski et la décomposition des matrices, Séminaire Delange-Pisot : Théorie des nombres, t. 4, 1962/63, n° 12, 9 p.