Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Hassan Saffari

Réduction des formes quadratiques définies positives

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 2 (1960-1961), exp. n° 9, p. 1-30

<http://www.numdam.org/item?id=SDPP_1960-1961__2__A9_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
2e année, 1960/61, n° 9

6 et 13 mars 1961

RÉDUCTION DES FORMES QUADRATIQUES DÉFINIES POSITIVES

par Hassan SAFFARI

Considérons la forme quadratique polynomiale $\sum_{i,j=1}^{n} s_{ij}\, x_i\, x_j$, c'est-à-dire une forme homogène du second degré à n variables, où $s_{ij} \in R$ et $s_{ij} = s_{ji}$; la matrice (s_{ij}) est donc symétrique. Si $|s_{ij}| = 0$, la forme s'appelle dégénérée. Dans tout ce qui suit S représente une matrice symétrique d'ordre n à éléments réels ; un vecteur colonne $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ sera noté $\underset{\sim}{x}$ et son transposé $\underset{\sim}{x}'$.

La forme quadratique précédente peut donc être écrite sous la forme

$$\sum_{i,j=1}^{n} s_{ij}\, x_i\, x_j = \underset{\sim}{x}'S\underset{\sim}{x} = S[\underset{\sim}{x}] \quad .$$

Plus généralement U étant une matrice d'ordre n , l'expression $U'SU$ sera représentée par $S[U]$.

L'un des problèmes essentiels étudiés dans la théorie arithmétique des formes quadratiques est celui de la représentation intégrale des nombres réels par la forme et le nombre des représentations possibles : étant donné un nombre $\alpha \in R$, on dit qu'il est représenté intégralement par une forme $S[\underset{\sim}{x}]$ s'il existe un vecteur $\underset{\sim}{x}$ à coordonnées entières tel que $S[\underset{\sim}{x}] = \alpha$. La représentation s'appelle "propre" si le vecteur est primitif, c'est-à-dire si ses coordonnées sont premières entre elles dans leur ensemble.

Ce problème est un cas particulier d'un autre, celui de la représentation intégrale d'une forme par une autre : étant données 2 formes f et g à n et m variables, $n > m$, dont les matrices sont A et B , on dit que f représente intégralement g s'il existe une matrice à éléments entiers T , à m lignes et n colonnes telle que $T'AT = B$. Le cas $m = 1$ correspond au problème de la représentation des nombres.

1. Exemples historiques de la représentation des nombres.

1° Théorème de Lagrange. - La forme quaternaire $x_1^2 + x_2^2 + x_3^2 + x_4^2$ représente tous les nombres entiers.

JACOBI a démontré, en utilisant les fonctions elliptiques Θ , que le nombre des représentations possibles est $\sum_{\substack{d \mid n \\ 4 \nmid d}} d$, où n est le nombre représenté.

2° Théorème de Fermat et d'Euler. - La forme binaire $x_1^2 + x_2^2$ représente tous les entiers dont les facteurs premiers sont de la forme $4n + 1$, ou de la forme $4n + 3$ mais à une puissance paire, et ne représente que ces entiers.

Le nombre des représentations possibles également trouvé par JACOBI, est $4(\sigma_1(n) - \sigma_3(n))$ où $\sigma_1(n)$ et $\sigma_3(n)$ représentent le nombre des diviseurs de n de la forme $4n + 1$ et $4n + 3$.

3° Théorème de Gauss. - La forme ternaire $x_1^2 + x_2^2 + x_3^2$ représente tous les entiers sauf ceux qui sont de la forme $4^m(8n + 7)$, m et n entiers.

Le problème de la représentabilité d'un nombre par une forme ou d'une forme par une forme a été étudié par SIEGEL, G. PALL, HASSE et d'autres ; celui du nombre des représentations possibles étudié particulièrement par SIEGEL est basé sur les généralisations qu'il a données des notions de fonctions modulaires et les fonctions Θ . Nous n'étudions pas ces problèmes. Mais nous allons étudier un problème de base, celui de chercher dans l'ensemble des formes un sous-ensemble dont les éléments ne représentent pas exactement les mêmes nombres. La résolution de tous les autres problèmes sur les formes est basée sur celui-ci.

Soit $S[\underset{\sim}{x}] = \underset{\sim}{x}'S\underset{\sim}{x} = \sum_{i,j=1}^{n} s_{ij}\, x_i\, x_j$. Considérons la transformation linéaire $x_k = \sum_{\ell=1}^{n} t_{k\ell}\, y_\ell$, $t_{k\ell}$ entiers et $T = (t_{k\ell})$ non singulière. En substituant dans $S[\underset{\sim}{x}]$, $\underset{\sim}{x} = T\underset{\sim}{y}$ on obtient la forme

$$g[\underset{\sim}{y}] = \underset{\sim}{y}'T'ST\underset{\sim}{y} = S[T\underset{\sim}{y}]$$

et il est évident que $g[\underset{\sim}{y}]$ représente tous les nombres que $S[\underset{\sim}{x}]$ peut représenter. La réciproque est vraie si $|T| = \pm 1$, et dans ce cas la matrice T s'appelle "unimodulaire". On dit alors que les formes $g[\underset{\sim}{y}]$ et $S[\underset{\sim}{x}]$ sont équivalentes. Comme les matrices unimodulaires forment un groupe, l'équivalence des formes est une relation d'équivalence. On obtient ainsi des classes d'équivalences dont les éléments représentent les mêmes nombres. Le problème se pose alors de trouver dans chaque classe un représentant ayant dans un certain sens des propriétés "simples". C'est ce qu'on appelle la "réduction des formes quadratiques". Il est évident que des formes équivalentes ont même déterminant ; la proposition réciproque est fausse.

2. Classification des formes quadratiques.

THÉORÈME 1. - Toute forme quadratique $S[\underset{\sim}{x}] = \sum_{i,j=1}^{n} s_{ij}\, x_i\, x_j$ à coefficients dans un corps où $2 \neq 0$ peut être mise sous la forme

$$G[\underset{\sim}{y}] = b_1\, y_1^2 + b_2\, y_2^2 + \cdots + b_r\, y_r^2$$

par une transformation linéaire dont les coefficients sont des fonctions rationnelles des coefficients de la forme et dont le déterminant est 1 .

DÉMONSTRATION. - Soit $S[\underset{\sim}{x}] = \sum_{i,j=1}^{n} s_{ij}\, x_i\, x_j$ et supposons $s_1 = s_{11} \neq 0$; alors

$$S[\underset{\sim}{x}] = s_1\, x_1^2 + 2\, s_{12}\, x_1\, x_2 + \cdots + 2\, s_{1n}\, x_1\, x_n + Q(x_2\,,\ \cdots\ ,\ x_n)$$

$$= s_1 \left(x_1 + \frac{s_{12}}{s_1}\, x_2 + \cdots + \frac{s_{1n}}{s_1}\, x_n\right)^2 - \frac{s_{12}^2}{s_1}\, x_2^2 - \frac{2\, s_{12}\, s_{13}}{s_1}\, x_2\, x_3 - \cdots$$

$$- \frac{s_{1n}^2}{s_1}\, x_n^2 + Q(x_2\,,\ \cdots\ ,\ x_n)$$

$$= s_1 \left(x_1 + \frac{s_{12}}{s_1}\, x_2 + \cdots + \frac{s_{1n}}{s_1}\, x_n\right)^2 + R(x_2\,,\ \cdots\ ,\ x_n)$$

où Q et R sont des formes quadratiques à $n - 1$ variables $x_2\,,\ \cdots\ ,\ x_n$. La transformation linéaire

$$(1) \qquad \begin{cases} y_1 = x_1 + \dfrac{s_{12}}{s_1}\, x_2 + \cdots + \dfrac{s_{1n}}{s_1}\, x_n \\ y_i = x_i\,, \qquad i > 1 \end{cases}$$

qui vérifie les conditions de l'énoncé donne la forme $s_1\, y_1^2 + R(y_2\,,\ \cdots\ ,\ y_n)$. Il suffit pour compléter la démonstration d'appliquer la même méthode à R puis aux formes à $n - 2$, $n - 3$, ... variables ainsi obtenues.

Soient S_1 la matrice de la forme R , S_2 celle de la forme Q ; la matrice de la transformation linéaire (1) s'écrit

$$\begin{pmatrix} 1 & s_1^{-1}\, q' \\ \underset{\sim}{0} & E \end{pmatrix}$$

où E est la matrice unité d'ordre $n-1$ et où q est une colonne à $n-1$ éléments définie par $S = \begin{pmatrix} s_1 & q' \\ q & S_2 \end{pmatrix}$. On a

$$S = \begin{pmatrix} s_1 & q' \\ q & S_2 \end{pmatrix} = \begin{pmatrix} s_1 & 0' \\ 0 & S_1 \end{pmatrix} \begin{bmatrix} 1 & s_1^{-1} q' \\ 0 & E \end{bmatrix}$$

qui entraîne

$$S_1 = S_2 - s_1^{-1} q\, q' \quad \text{et} \quad |S| = s_1 |S_2| \qquad (2)$$

Plus généralement posons $x = \begin{pmatrix} y \\ z \end{pmatrix}$ où y est une colonne à k éléments et z une colonne à $n-k$ éléments. De même faisons une partition de S sous la forme $S = \begin{pmatrix} S_1 & Q \\ Q' & S_2 \end{pmatrix}$ où S_1 est une matrice carrée d'ordre k ; on a :

$$S[x] = \begin{pmatrix} S_1 & Q \\ Q' & S_2 \end{pmatrix} \begin{bmatrix} y \\ z \end{bmatrix} = y' S_1 y + y' Q z + z' Q' y + z' S_2 z$$

$$= (y' + S_1^{-1} z' Q') S_1 (y + S_1^{-1} Q z) + z' (S_2 - Q' S_1^{-1} Q) z$$

ou bien

$$S[x] = S_1[y + S_1^{-1} Q z] + w[z]$$

où

$$w = S_2 - Q' S_1^{-1} Q \qquad (3)$$

En notation matricielle cela s'écrit

$$S = \begin{pmatrix} S_1 & 0 \\ 0 & w \end{pmatrix} \begin{bmatrix} E & S_1^{-1} Q \\ 0 & E \end{bmatrix}$$

où l'ordre des matrices nulles et unités est évident, ceci entraîne

$$|S| = |S_1|\,|w| \qquad (4)$$

Dans la suite nous utilisons à plusieurs reprises les formules (3) et (4).

Considérons maintenant la forme diagonale $G[\underset{\sim}{y}] = b_1\ y_1^2 + \ldots + b_r\ y_r^2$ transformée de la forme $S[\underset{\sim}{x}] = \sum_{i,j=1}^{n} s_{ij}\ x_i\ x_j$.

La transformation $z_j = \sqrt{|b_j|}\ y_j$, $j = 1$, $\ldots$, r , permet de l'écrire sous la forme

$$H[\underset{\sim}{z}] = z_1^2 + z_2^2 + \ldots + z_i^2 - z_{i+1}^2 - \ldots - z_r^2$$

où on a permuté les indices pour rassembler les termes positifs et négatifs

r s'appelle le rang de la forme (ou de la matrice S)

i s'appelle l'indice de la forme

$2i - r = i - (r - i)$ s'appelle la signature de la forme.

Si $i = r = n$, la forme s'appelle <u>définie positive</u> ou simplement <u>positive</u>. Dans ce cas on a $S[\underset{\sim}{x}] > 0$ quel que soit $\underset{\sim}{x} \neq 0$. On dit alors que la matrice S est positive, et on écrit $S > 0$.

Si $i = r < n$, la forme s'appelle <u>semi-définie positive</u>, et il est évident que dans ce cas il existe des $\underset{\sim}{x} \neq 0$ pour lesquels $S[\underset{\sim}{x}] = 0$. On a donc $S[x] \geq 0$.

Si $i = 0$, la forme s'appelle <u>négative</u>.

Si $0 < i < r$, la forme s'appelle <u>indéfinie</u>.

Dans ce qui suit, nous nous occupons du cas le plus simple de réduction : celui des formes positives ; pour cela nous allons rappeler, sans démonstration, plusieurs lemmes, sur les matrices positives ou non, qui n'ont pas de caractères arithmétiques particuliers. Les démonstrations de ces lemmes se trouvent dans tous les traités sur les matrices ; voir par exemple : MIRSKY, [2], chapitres XII et XIII.

LEMME 1. - Si $S > 0$, A une matrice réelle, $|A| \neq 0$, alors $T = S[A] > 0$.

LEMME 2. - $S > 0 \rightleftarrows |S_r| > 0$, $r = 1$, 2 , $\ldots$, n , où S_r est la matrice composée de r premières lignes et r premières colonnes de S .

Ce lemme est un cas particulier du suivant :

LEMME 2'. - L'indice d'une matrice symétrique est égal au nombre de permanence de signe dans la suite 1 , $|S_1|$, $|S_2|$, $\ldots$, $|S_n|$.

Il en résulte en particulier que, pour une matrice négative, on a $|S_1| < 0$, $|S_2| > 0$, $|S_3| < 0$, ...

LEMME 3. - Soit $S = (s_{ij}) > 0$, on a alors $|S| \leq s_1 \, s_2 \cdots s_n$, où $s_i = s_{ii}$, l'égalité n'a lieu que si S est diagonale.

Ce lemme est un cas particulier du suivant :

LEMME 3'. - Si $S > 0$ et $S = \begin{pmatrix} S_1 & S_{12} \\ S'_{12} & S_2 \end{pmatrix}$, où S_1 est une matrice carrée, on a :

$$|S| \leq |S_1||S_2| \quad \text{(inégalité de Fischer)}$$

l'égalité a lieu $\rightleftarrows S_{12} = 0$

LEMME 4 (Transformation de Jacobi). - Si $S > 0$, il existe une et une seule matrice diagonale D , et une et une seule matrice triangulaire $V = (d_{ij})$, avec $d_{ii} = 1$ et $d_{ij} = 0$ pour $i > j$ telles que

$$S = D[V] = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \begin{bmatrix} 1 & d_{12} & \cdots & d_{1n} \\ 0 & 1 & & d_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & & & 1 \end{bmatrix}$$

plus généralement on a

$$S = \begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix} \begin{bmatrix} E & T \\ 0 & E \end{bmatrix}$$

avec S_1 , S_2 , T uniques.

LEMME 5. - Étant donné le vecteur $\underset{\sim}{x}$, à coordonnées entières, primitif, on peut toujours former des matrices unimodulaires telles que $\underset{\sim}{x}$ soit la première colonne de ces matrices.

3. Minimum des formes positives.

Soit $S[\underset{\sim}{x}] > 0$, les valeurs propres d_1 , d_2 , ... , d_n de S sont toutes positives. m et M étant la plus petite et la plus grande de ces valeurs propres et $\underset{\sim}{x}$ un vecteur quelconque, il est évident que

$$m\, \underset{\sim}{x}'\, \underset{\sim}{x} \leq S[\underset{\sim}{x}] \leq M\, \underset{\sim}{x}'\, \underset{\sim}{x} \quad .$$

Soit $t > 0$ un nombre réel assez grand ; si $S[\underset{\sim}{x}] < t$, on a $m\, \underset{\sim}{x}'\, \underset{\sim}{x} < t$ donc toutes les coordonnées de $\underset{\sim}{x}$ sont bornées, et il n'existe qu'un nombre fini de vecteurs entiers pour lesquels on ait $S[\underset{\sim}{x}] < t$. Ceci montre que si $\underset{\sim}{x}$ parcourt tous les vecteurs entiers non nuls, $S[x]$ passe par un minimum $\mu(S)$, autrement dit, il existe un $\underset{\sim}{x} \neq 0$ tel que

$$S[\underset{\sim}{x}] = \mu(S)$$

$\underset{\sim}{x}$ est primitif, car si $\underset{\sim}{x} = q\, \underset{\sim}{y}$, q entier > 1, y est primitif, et on a

$$\mu(S) = S[\underset{\sim}{x}] = q^2\, S[\underset{\sim}{y}] > S[\underset{\sim}{y}] \quad .$$

Si $S \sim T$, on a $\mu(S) = \mu(T)$, car si U est une matrice unimodulaire, telle que $S = T[U]$, et $\underset{\sim}{x}$ un vecteur primitif, tel que $\mu(S) = S[\underset{\sim}{x}]$, on a

$$\mu(S) = S[\underset{\sim}{x}] = T[U\underset{\sim}{x}] \geq \mu(T)$$

et si $\mu(T) = T[\underset{\sim}{y}]$, on a

$$\mu(T) = T[\underset{\sim}{y}] = S[U^{-1}\, y] \geq \mu(S)$$

4. Estimation de $\mu(S)$.

Remarquons d'abord que si $S > 0$ est multipliée par $t > 0$, $\mu(tS) = t\mu(S)$ tandis que $|tS| = t^n |S|$. Ceci montre qu'il est raisonnable de comparer $\mu(S)$ avec $|S|^{1/n}$.

THÉORÈME 2 (HERMITE). - Il existe une constante C_n ne dépendant que de n telle que $\mu(S) \leq C_n |S|^{1/n}$.

DÉMONSTRATION. - Pour $n = 1$, le théorème est évident : $C_1 = 1$, $x = \pm 1$ $\mu(S) = s_1$, $|S| = s_1 > 0$.

Supposons le théorème vrai pour $n - 1$. Soit $\underset{\sim}{x}$ primitif tel que $\mu(S) = S[\underset{\sim}{x}]$, complétons $\underset{\sim}{x}$ pour former une matrice unimodulaire U (lemme 5). Alors $T = S[U] = U'\, S\, U$ a pour le premier élément diagonal $\mu(S)$. Comme on a $|S| = |T|$ et $\mu(S) = \mu(T)$ on peut supposer que le premier élément diagonal s_1 de S est $\mu(S)$. Si on pose

$$\underset{\sim}{x} = \begin{pmatrix} x_1 \\ \underset{\sim}{y} \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} s_1 & \underset{\sim}{q}' \\ \underset{\sim}{q} & S_1 \end{pmatrix}$$

on a d'après les les formules (3) et (4)

$$S[\underset{\sim}{x}] = s_1 (x_1 + s_1^{-1}\, \underset{\sim}{q}'\, \underset{\sim}{y})^2 + w[\underset{\sim}{y}]$$

où

$$w = S_1 - q\, s_1^{-1}\, q' \qquad \text{et} \quad |S| = s_1 |w| \quad .$$

Mais $w > 0$, donc on peut choisir $\underset{\sim}{y}$ tel que $w[\underset{\sim}{y}]$ soit minimum. Une fois $\underset{\sim}{y}$ choisi, on peut choisir x_1 tel que

$$-\frac{1}{2} \leq x_1 + s_1^{-1}\, \underset{\sim}{q}'\, \underset{\sim}{y} \leq \frac{1}{2}$$

et l'hypothèse d'induction entraîne

$$\mu(S) \leq S[\underset{\sim}{x}] \leq \frac{\mu(S)}{4} + C_{n-1} |w|^{1/(n-1)}$$

mais

$$|w| = \frac{|S|}{\mu(S)}$$

donc

$$\mu(S) \leq \left(\frac{4}{3} C_{n-1}\right)^{(n-1)/n} |S|^{1/n}$$

on trouve à partir de $C_1 = 1$ et $C_n = \left(\frac{4}{3} C_{n-1}\right)^{(n-1)/n}$ que $C_n = \left(\frac{4}{3}\right)^{(n-1)/2}$.

On ne sait rien sur la meilleure constante C_n possible. Toutefois pour $n = 2$, $C_2 = \sqrt{4/3}$, qu'on obtient ainsi, est la meilleure. En effet la forme $x^2 + xy + y^2 \geq 1$ atteint son minimum pour $x \neq 0$ (par exemple $x = 1$, $y = 0$) et on a $|S| = 3/4$ donc $1 = \left(\frac{4}{3}\right)^{1/2} |S|^{1/2}$.

Une autre estimation, plus fine, de C_n est donnée par le théorème suivant :

THÉORÈME 3 (MINKOWSKI). - Si $S > 0$, on a

$$\mu(S) \leq \frac{4}{\pi} \{\Gamma(\tfrac{n}{2} + 1)\}^{2/n} |S|^{1/n} \quad .$$

DÉMONSTRATION. - Considérons l'ensemble des $\underset{\sim}{x} \in R^n$ pour lesquels $S[x] < \rho$; cet ensemble est manifestement ouvert et symétrique par rapport à l'origine, d'ailleurs $S > 0 \Longrightarrow m\, \underset{\sim}{x}'\, \underset{\sim}{x} < \rho$ qui montre que cet ensemble est borné. Montrons qu'il est convexe, remarquons pour cela que $S > 0$ peut se mettre sous la forme

A^tA où A est une matrice carrée. En effet, il existe une matrice orthogonale V telle que $S = V' DV$, où D, la forme diagonale de S, a tous ses éléments positifs, donc

$$S = V' D_1^2 V = V' D_1' D_1 V = A'A \quad \text{où} \quad A = D_1 V \quad .$$

Cela posé, on peut écrire $S[\underset{\sim}{x}] = \underset{\sim}{x}' S \underset{\sim}{x} = \underset{\sim}{x}' A'A \underset{\sim}{x}$. La démonstration de la convexité consiste à démontrer, à partir des inégalités $S[\underset{\sim}{x}_1] < \rho$, $S[\underset{\sim}{x}_2] < \rho$, l'inégalité $S[\frac{\underset{\sim}{x}_1 + \underset{\sim}{x}_2}{2}] < \rho$. La transformation affine $A\underset{\sim}{x}_1 = \underset{\sim}{y}_1$, $A\underset{\sim}{x}_2 = \underset{\sim}{y}_2$ montre alors qu'il suffit de démontrer :

$$(\underset{\sim}{y}_1' \underset{\sim}{y}_2 + \underset{\sim}{y}_2' \underset{\sim}{y}_1) \leq \underset{\sim}{y}_1' \underset{\sim}{y}_1 + \underset{\sim}{y}_2' \underset{\sim}{y}_2$$

ce qui est évident. La même transformation affine permet de calculer le volume de ce domaine, celui d'une hyperellipsoïde, qui est :

$$v = \frac{\rho^{n/2} \pi^{n/2}}{\Gamma(n/2+1)} |S|^{1/2} \quad .$$

Pour $\rho = \mu(S)$ ce domaine ne contient aucun point de coordonnées entières, en dehors de l'origine. Son volume est donc, d'après un théorème bien connu de Minkowski, $\leq 2^n$ ce qui donne la formule cherchée.

En appliquant par exemple la formule de Stirling, on remarque que, pour n assez grand, l'estimation de MINKOWSKI est meilleure que celle de HERMITE.

5. Les formes positives semi-réduites.

Soit R_h l'espace des matrices symétriques à éléments réels. C'est un espace vectoriel à $h = \frac{n(n+1)}{2}$ dimensions. A cet espace correspond, par un isomorphisme canonique, un espace euclidien à h dimensions sur lequel nous définissons une topologie à partir de la distance. Celle-ci, par isomorphisme, induit une topologie sur R_h. Considérons le sous-ensemble $\mathcal{P}$ des matrices positives de R_h. On a les propriétés suivantes :

1° R_h est localement compact.

2° L'ensemble des éléments de R_h pour lesquels un mineur principal donné a un déterminant positif, est une réunion d'ouverts, donc est un ouvert de R_h.

Cette propriété montre (lemme 2) que $\mathcal{P}$ est l'intersection d'un nombre fini

d'ouverts, donc est un ouvert.

Soient S une matrice de la frontière de $\mathcal{P}$ dans R_h, et $S_1, S_2, \cdots$, une suite de matrices de $\mathcal{P}$ qui convergent vers S ; pour $\underset{\sim}{x} \neq 0$, on a $S_k[\underset{\sim}{x}] > 0$ et par continuité $S[\underset{\sim}{x}] \geqslant 0$. $\underset{\sim}{x}$ étant arbitraire, on a $S \geqslant 0$. Réciproquement si S est une matrice semi-définie positive dans R_h, E la matrice unité d'ordre n et $\varepsilon > 0$, $S + \varepsilon E$ est une matrice positive. Cela montre que dans tout voisinage de S il y a des points de $\mathcal{P}$. Donc la frontière de $\mathcal{P}$ dans R_h n'est autre que l'ensemble des matrices semi-définies positives de R_h.

Soit Γ le groupe des matrices unimodulaires. Γ opère sur R_h comme un groupe de transformations $S \to S[U]$, $S \in R_h$, où U et $-U$ donnent le même transformé, et où les seuls éléments de Γ qui laissent fixes tous les éléments de R_h sont $\pm E$. Si donc on identifie U et $-U$ dans Γ, $S \to S[U]$ donne une représentation de Γ_0 dans R_h où $\Gamma_0 = \Gamma/\pm E$. Si $S \in R_h$ et U parcourt Γ, $S[U]$ parcourt tous les éléments de la classe de S. Nous allons chercher dans chaque classe de $\mathcal{P}$ une matrice possédant de "belles" propriétés. Soit $T \in \mathcal{P}$, et supposons que $\underset{\sim}{u}$ parcourt les premières colonnes de toutes les matrices de Γ, c'est-à-dire tous les vecteurs entiers primitifs. $T[\underset{\sim}{u}]$ a un minimum que nous supposons atteint pour $\underset{\sim}{u} = \underset{\sim}{u_1}$. $\underset{\sim}{u_1}$ n'est pas unique, car $-\underset{\sim}{u_1}$ aussi satisfait cette condition. Comme $T > 0$, il n'y a qu'un nombre fini de $\underset{\sim}{u}$ tels que $T[\underset{\sim}{u}] = T[\underset{\sim}{u_1}] = \mu(T)$. Laissons $\underset{\sim}{u_1}$ fixe, et supposons que $\underset{\sim}{u}$ parcourt les secondes colonnes des $U \in \Gamma$ dont la première colonne est $\underset{\sim}{u_1}$. Les $\underset{\sim}{u}$ ne sont plus tous les vecteurs primitifs, et on a par exemple $\underset{\sim}{u} \neq \underset{\sim}{u_1}$. $T[\underset{\sim}{u}]$ a de nouveau un minimum pour $\underset{\sim}{u} = \underset{\sim}{u_2}$, et on a $T[\underset{\sim}{u_1}] \leqslant T[\underset{\sim}{u_2}]$. Il n'y a de même qu'un nombre fini de $\underset{\sim}{u}$ tels que $T[\underset{\sim}{u}] = T[\underset{\sim}{u_2}]$. Considérons toutes les matrices unimodulaires dont les 2 premières colonnes sont $\underset{\sim}{u_1}$ et $\underset{\sim}{u_2}$, et déterminons $\underset{\sim}{u_3}$ tel que $T[\underset{\sim}{u_3}]$ soit minimum. En continuant ainsi, on trouve une matrice unimodulaire $U = (\underset{\sim}{u_1}, \underset{\sim}{u_2}, \cdots, \underset{\sim}{u_n})$, et une matrice positive $S = T[U]$ telles que $S \backsim T$ et d'après notre construction même, S n'est pas unique dans la classe de T.

Nous allons étudier plus profondément S et U. Supposons qu'on a construit $\underset{\sim}{u_1}, \cdots, \underset{\sim}{u_{k-1}}$, pour construire la k-ième colonne, on considère toutes les matrices V unimodulaires dont les $k-1$ premières colonnes sont $\underset{\sim}{u_1}, \underset{\sim}{u_2}, \cdots, \underset{\sim}{u_{k-1}}$; U étant la matrice précédente on a :

(5) $$U^{-1} V = \begin{pmatrix} E_{k-1} & A \\ 0 & B \end{pmatrix}$$

où E_{k-1} est la matrice unité d'ordre $k-1$, et A et B sont des matrices entières. U et V étant unimodulaires, B l'est aussi. Si $\underset{\sim}{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$ est la première colonne de la matrice $\begin{pmatrix} A \\ B \end{pmatrix}$, comme B est unimodulaire, on a

(6) $$(w_k , w_{k+1} , \cdots , w_n) = 1$$

et la k-ième colonne $\underset{\sim}{u}_k$ de V est $U\underset{\sim}{w}$. Réciproquement $\underset{\sim}{w}$ étant un vecteur entier vérifiant (6), $w_k , \cdots , w_n$ peuvent occuper la première colonne d'une matrice unimodulaire d'ordre $n - k + 1$. En choisissant une matrice entière A quelconque de $k-1$ lignes et $n-k+1$ colonnes dont la première colonne est $w_1 , \cdots , w_{k-1}$, on construit à partir de la relation (5) une matrice V dont les $k-1$ premières colonnes sont $\underset{\sim}{u}_1 , \cdots , \underset{\sim}{u}_{k-1}$. Donc la k-ième colonne de toutes les matrices unimodulaires, dont les $k-1$ premières colonnes sont $\underset{\sim}{u}_1 , \cdots , \underset{\sim}{u}_{k-1}$ est de la forme $U\underset{\sim}{w}$ où $\underset{\sim}{w}$ est un vecteur entier arbitraire, tel que $(w_k , \cdots , w_n) = 1$.

Considérons la matrice $S = T[U]$. D'après le choix de $\underset{\sim}{u}_k$ nous aurons, $\underset{\sim}{w}$ vérifiant (6) :

$$S[\underset{\sim}{w}] = T[U\underset{\sim}{w}] \geq T[\underset{\sim}{u}_k] = s_{kk} = s_k \quad \text{où} \quad S = (s_{ij}) \quad .$$

Nous avons démontré donc que dans chaque classe de T, il existe une matrice S vérifiant les conditions suivantes :

a. $s_1 > 0$

b. $S[\underset{\sim}{w}] \geq s_k$, $k = 1 , \cdots , n$ pour toute colonne entière $\underset{\sim}{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$ où $(w_k , \cdots , w_n) = 1$.

Les matrices vérifiant les conditions (a) et (b) s'appellent semi-réduites, et le sous-ensemble des matrices semi-réduites de $\mathcal{P}$ sera noté $\mathcal{R}_0$.

Nous désignerons, dans ce qui suit, par $e_1 , \cdots , e_n$ les n-colonnes de la matrice E_n, et nous appellerons k-vecteur admissible tout vecteur entier vérifiant (6). Comme e_{k+1} est un k-vecteur admissible, on a d'après (b)

(7) $\qquad s_{k+1} = S[e_{k+1}] \geq s_k \implies s_1 \leq s_2 \leq \cdots \leq s_n \quad .$

Soit $\underset{\sim}{u} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ un vecteur entier tel que $x_k = 1$, $x_\ell = 1$, $x_i = 0$ pour $i \neq k$, ℓ et $k < \ell$, alors $\underset{\sim}{u}$ est un ℓ-vecteur admissible, et on a :

$$s_k + 2\, s_{k\ell} + s_\ell = S[\underset{\sim}{u}] \geq s_\ell \implies 2\, s_{k\ell} \geq - s_k \quad .$$

En changeant le signe de x_k dans $\underset{\sim}{u}$, on trouve $2\, s_{k\ell} \leq s_k$. On a donc

(8) $\qquad - s_k \leq 2\, s_{k\ell} \leq s_k \qquad 1 \leq k < \ell \leq n \quad .$

REMARQUE. - Soient S une matrice réelle symétrique vérifiant (b), et S_1 la matrice obtenue en éliminant les lignes et les colonnes h_1 , h_2 , ... , h_ℓ de S ; S_1 a alors les mêmes propriétés que S , car il suffit de considérer des vecteurs admissibles w où les éléments de rang h_1 , h_2 , ... , h_ℓ sont égaux à zéro.

A partir des formules (7), (8) et de la remarque précédente qui sont toutes des conséquences de (b) nous allons démontrer le théorème suivant :

THÉORÈME 4. - Si S est une matrice réelle symétrique vérifiant (b), on a $S \geq 0$ et si elle vérifie aussi (a), on a $S > 0$.

DÉMONSTRATION. - Si $s_1 = 0$, (8) $\implies 0 = - s_1 \leq 2\, s_{1\ell} \leq s_1 = 0$ donc $S = \begin{pmatrix} 0 & 0' \\ 0 & S_1 \end{pmatrix}$. Si $s_2 = 0$, comme S_1 a les mêmes propriétés que S , une telle décomposition existe pour S_1 . Donc, ou bien on a $S = 0$, ou bien on trouve un $s_k \neq 0$ et $S = \begin{pmatrix} 0 & 0 \\ 0 & S_k \end{pmatrix}$ où s_k est le premier élément diagonal de S_k . Nous allons démontrer que $S_k > 0$. Mais S_k vérifie les conditions (a) et (b), il suffit de démontrer donc que si S vérifie (a) et (b) on a $S > 0$. Le théorème est vrai pour $n = 1$. Supposons-le vrai pour $n - 1$, et posons $S = \begin{pmatrix} S_1 & \underset{\sim}{q} \\ \underset{\sim}{q}' & s_n \end{pmatrix}$. S_1 vérifie (a) et (b) et l'hypothèse de l'induction $\implies S_1 > 0$. Mais d'après (7), on a $s_n \geq s_1$ donc $s_n > 0$. Soit $\underset{\sim}{x} = \begin{pmatrix} \underset{\sim}{y} \\ z \end{pmatrix}$ une colonne à n éléments, $\underset{\sim}{y}$ ayant $n - 1$ élément et z un nombre réel. On a d'après les formules (3)

$$S[\underset{\sim}{x}] = S_1[\underset{\sim}{y} + S_1^{-1}\ \underset{\sim}{q}\ z] + (s_n - \underset{\sim}{q}'\ S_1^{-1}\ \underset{\sim}{q})\ z^2 \quad .$$

Il nous suffit de montrer que $s_n - \underset{\sim}{q}'\ S_1^{-1}\ \underset{\sim}{q} > 0$. Supposons le contraire, et soit $s_n \leqslant \underset{\sim}{q}'\ S_1^{-1}\ \underset{\sim}{q}$, alors pour $\varepsilon > 0$ et tout $\underset{\sim}{x} \neq \underset{\sim}{0}$ on a :

$$S[\underset{\sim}{x}] \leqslant S_1[\underset{\sim}{y} + S_1^{-1}\ \underset{\sim}{q}\ z] + \varepsilon z^2 \quad . \tag{9}$$

La forme quadratique du second membre de (9) est > 0 d'ordre n et a , d'après (4), pour déterminant $|S_1|\ \varepsilon$. On peut trouver donc un vecteur entier $\underset{\sim}{x} = \begin{pmatrix} \underset{\sim}{y} \\ z \end{pmatrix}$ tel que la valeur de cette forme atteigne son minimum et le théorème de Hermite donne :

$$S_1[\underset{\sim}{y} + S_1^{-1}\ \underset{\sim}{q}\ z] + \varepsilon z^2 \leqslant C_n |S_1|^{1/n}\ \varepsilon^{1/n}$$

mais d'après (b) on a pour le vecteur primitif $\underset{\sim}{x}$, $s_1 \leqslant S[\underset{\sim}{x}]$, donc

$$0 < s_1 \leqslant S[\underset{\sim}{x}] \leqslant C_n |S_1|^{1/n}\ \varepsilon^{1/n} \quad .$$

Comme ε est arbitrairement petit, cette relation entraîne une contradiction, donc $s_n - \underset{\sim}{q}'\ S_1^{-1}\ \underset{\sim}{q} > 0 \implies S > 0$. Ce théorème montre que toute matrice vérifiant (a) et (b) appartient à $\mathcal{P}$.

THÉORÈME 5 (MINKOWSKI). - Si $S > 0$ et semi-réduite, on a :

$$1 \leqslant \frac{s_1 \cdots s_n}{|S|} \leqslant b_n$$

où b_n est une constante qui ne dépend que de n .

DÉMONSTRATION. - La première inégalité n'est autre que le lemme (3), vrai pour tout $S \in \mathcal{P}$. Démontrons la seconde par induction. Pour $n = 1$, le théorème est vrai avec le signe d'égalité, et $b_1 = 1$. Supposons donc le théorème démontré pour tout $k < n$. Considérons les rapports $\frac{s_n}{s_{n-1}}$, $\frac{s_{n-1}}{s_{n-2}}$, ... , $\frac{s_2}{s_1}$. S étant semi-réduite, tous ces rapports sont $\geqslant 1$. Soit $\gamma = \frac{n(n-1)}{4}$, alors il y a l'une des 2 possibilités suivantes :

1° Il existe un k , $2 \leqslant k \leqslant n$, tel que

$$\frac{s_n}{s_{n-1}} < \gamma\ ,\ \frac{s_{n-1}}{s_{n-2}} < \gamma\ ,\ \cdots\ ,\ \frac{s_{k+1}}{s_k} < \gamma \quad \text{mais} \quad \frac{s_k}{s_{k-1}} \geqslant \gamma \tag{10}$$

2° On a $\frac{s_n}{s_{n-1}}, \dots, \frac{s_2}{s_1} < \gamma$. Remarquons que ce cas ne peut pas avoir lieu pour $n = 2$, car $\gamma = \frac{1}{2}$ et $\frac{s_2}{s_1} \geqslant 1$.

Dans le premier cas posons $S = \begin{pmatrix} S_{k-1} & Q \\ Q' & R \end{pmatrix}$, où S_{k-1} est une matrice carrée d'ordre $k-1$, et soit $\underset{\sim}{x} = \begin{pmatrix} \underset{\sim}{y} \\ \underset{\sim}{z} \end{pmatrix}$ où $\underset{\sim}{y}$ est une colonne à $k-1$ éléments. Les formules (3) et (4) donnent :

$$S[\underset{\sim}{x}] = S_{k-1}[\underset{\sim}{y} + S_{k-1}^{-1} Q \underset{\sim}{z}] + (R - Q' S_{k-1}^{-1} Q)[\underset{\sim}{z}]$$

et

$$|R - Q' S_{k-1}^{-1} Q| = |S| / |S_{k-1}| \quad .$$

Choisissons $\underset{\sim}{z}$, entier et primitif, tel que $(R - Q' S_{k-1}^{-1} Q)[\underset{\sim}{z}]$ soit minimum, le théorème 2 donne :

$$(11) \qquad (R - Q' S_{k-1}^{-1} Q)[\underset{\sim}{z}] \leqslant C_{n-k+1} \left(\frac{|S|}{|S_{k-1}|} \right)^{1/(n-k+1)} \quad .$$

Posons $\underset{\sim}{y} + S_{k-1}^{-1} Q \underset{\sim}{z} = \underset{\sim}{w}$, $\underset{\sim}{w} = \begin{pmatrix} w_1 \\ \vdots \\ w_{k-1} \end{pmatrix}$. Une fois $\underset{\sim}{z}$ choisi, on peut choisir $\underset{\sim}{y}$ tel que

$$(12) \qquad -\frac{1}{2} \leqslant w_i \leqslant \frac{1}{2} , \quad i = 1 , 2 , \dots , k-1 \quad .$$

D'après le choix de $\underset{\sim}{z}$, $\underset{\sim}{x} = \begin{pmatrix} \underset{\sim}{y} \\ \underset{\sim}{z} \end{pmatrix}$ est un k-vecteur admissible, et on a

$$(13) \qquad s_k \leqslant S[x] \quad .$$

D'ailleurs S_{k-1} est aussi semi-réduite, et on a :

$$S_{k-1}[\underset{\sim}{w}] = \sum_{p,q=1}^{k-1} s_{pq} w_p w_q \leqslant s_{k-1} \sum_{p,q=1}^{k-1} \frac{1}{2} \cdot \frac{1}{2} \leqslant \frac{(k-1)\,k}{8} s_{k-1}$$

mais (10) $\Longrightarrow$ $s_{k-1} \leqslant \frac{s_k}{\gamma} = \frac{4 s_k}{k(k-1)}$ donc

$$(14) \qquad S_{k-1}[\underset{\sim}{w}] \leqslant \frac{s_k}{2}$$

et d'après l'expression de $S[x]$ ainsi que les relations (11), (13) et (14) on trouve

(15) $$s_k \leqslant 2\, C_{n-k+1}\,(|S|/|S_{k-1}|)^{1/(n-k+1)} \quad .$$

Mais

$$\frac{s_1\, s_2 \cdots s_n}{|S|} = \frac{s_1 \cdots s_{k-1}}{|S_{k-1}|} \cdot \frac{|S_{k-1}|}{|S|}\, s_k^{n-k+1} \cdot \frac{s_k \cdots s_n}{s_k^{n-k+1}} \quad .$$

L'hypothèse de l'induction, (15) et (10) entraîne

$$\frac{s_1 \cdots s_n}{|S|} \leqslant b_{k-1}\,(2\, C_{n-k+1})^{n-k+1} \cdot \gamma^{\frac{(n-k)(n-k+1)}{2}} \quad .$$

Dans le second cas, on a :

$$\frac{s_1 \cdots s_n}{s_1^n} < \gamma^{\frac{n(n-1)}{2}} \quad \text{et} \quad \frac{s_1 \cdots s_n}{|S|} = \frac{s_1 \cdots s_n}{s_1^n} \cdot \frac{s_1^n}{|S|} \quad .$$

En remarquant que s_1 est le minimum de la forme quadratique semi-réduite, et en appliquant l'inégalité d'Hermite, on trouve

$$\frac{s_1 \cdots s_n}{|S|} < C_n^n\, \gamma^{\frac{n(n-1)}{2}} \quad .$$

On ne sait rien sur la meilleure constante possible dans le cas général. Pour $n = 2$, $b_2 = \frac{4}{3}$ est la meilleure : en effet, si $ax^2 + 2bxy + cy^2$ est semi-réduite et positive, on a, d'après (7) et (8) : $2b \leqslant a \leqslant c$. Le déterminant de la forme est $d = ac - b^2$ donc

(16) $$ac = ac - b^2 + b^2 \leqslant d + \frac{a^2}{4} \leqslant d + \frac{ac}{4} \implies ac \leqslant \frac{4}{3}\, d \quad .$$

Mais la forme positive et semi-réduite $x^2 + xy + y^2 \geqslant 1$ a pour déterminant $\frac{3}{4}$, et $ac = 1$, donc $1 = \frac{4}{3}\, d \implies \frac{4}{3}$ est la meilleure constante.

6. Deux régions auxiliaires. - Soit $\mathcal{R}_0$ l'espace des matrices semi-réduites. Définissons l'ensemble des points $\mathcal{R}_t^*$ pour $t > b_n \geqslant 1$ comme l'ensemble des $S \in \mathcal{P}$ satisfaisant à :

(17) $$\begin{cases} 0 < s_k < t\, s_{k+1} \ , \quad k = 1 \ , \ \cdots \ , \ n-1 \\ -t < \dfrac{s_{k\ell}}{s_k} < t \ , \quad 1 \leqslant k < \ell \leqslant n \\ \dfrac{s_1 \cdots s_n}{|S|} < t \end{cases}$$

(7), (8) et le théorème (5) $\Longrightarrow$ $\mathcal{R}_0 \subset \mathcal{R}_t^*$. Ce qui est plus important c'est que

$$\lim_{t\to\infty} \mathcal{R}_t^* = \mathcal{P} \qquad . \tag{18}$$

En effet soit $S \in \mathcal{P}$, choisissons t plus grand que le maximum des valeurs de $\frac{s_k}{s_{k+1}}$, $k = 1 , \dots , n-1$, $\pm \frac{s_{k\ell}}{s_k}$, $1 \leqslant k < \ell \leqslant n$, $\frac{s_1 \cdots s_n}{|S|}$ et b_n , on a pour cette valeur de t : $S \in \mathcal{R}_t^*$.

Soit $S \in \mathcal{R}_t^*$, on a d'après le lemme (4) :

$$S = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \begin{bmatrix} 1 & t_{12} & \cdots & t_{1n} \\ 0 & 1 & \ddots & \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & 1 \end{bmatrix} = D[T] \tag{19}$$

qui entraîne

$$s_{k\ell} = d_k\, t_{k\ell} + \sum_{h=1}^{k-1} d_h\, t_{hk}\, t_{h\ell} \ , \quad 1 \leqslant k \leqslant \ell \leqslant n \tag{20}$$

pour $k = \ell$, on a $t_{kk} = 1$, $s_{kk} = s_k$, $t_{hk}\, t_{hk} > 0$ et comme les $d_i > 0$, on trouve

$$\frac{s_k}{d_k} \geqslant 1 \qquad . \tag{21}$$

Comme $|S| = d_1 \cdots d_n$, on a

$$\prod_{k=1}^{n} \frac{s_k}{d_k} = \frac{s_1 \cdots s_n}{|S|} < t \qquad ,$$

et comme $t > 1$, ceci entraîne

$$\frac{s_k}{d_k} < t \ , \quad k = 1 , \dots , n \tag{22}$$

alors

$$\frac{d_k}{d_{k+1}} = \frac{d_k}{s_k} \cdot \frac{s_k}{s_{k+1}} \cdot \frac{s_{k+1}}{d_{k+1}} < t^2 \qquad . \tag{23}$$

Mais (17) donne : $s_{1\ell} = d_1 \cdot t_{1\ell}$, donc

$$|t_{1\ell}| = \frac{|s_{1\ell}|}{d_1} = \frac{|s_{1\ell}|}{s_1} \cdot \frac{s_1}{d_1} < t^2 \quad .$$

Supposons qu'on a démontré (v. a. = valeur absolue) :

$$\text{(24)} \qquad \text{v. a. } t_{g\ell} < u_0 \ , \quad 1 \leq g \leq k-1 \ , \quad g < \ell \leq n$$

où u_0 est une constante dépendant de t et de n , alors en remarquant que

$$\frac{d_h}{d_k} = \frac{d_h}{d_{h+1}} \cdot \frac{d_{h+1}}{d_{h+2}} \cdots \frac{d_{k-1}}{d_k}$$

et appliquant (20), (23) et (24) on trouve

$$\text{v. a. } t_{k\ell} \leq \text{v. a. } \frac{s_{k\ell}}{d_k} + \sum_{h=1}^{k-1} \frac{d_h}{d_k} \text{ v. a. } t_{hk} \text{ v. a. } t_{h\ell} < u_1$$

u_1 dépendant de t et de n .

Si alors u est le maximum de u_0 , u_1 , t^2 on trouve les inégalités suivantes concernant les éléments de D et de T dans (19)

$$\text{(25)} \qquad \begin{cases} 0 < d_k < u\, d_{k+1} & k = 1 \ , \ \dots \ , \ n-1 \\ \\ \text{v. a. } t_{k\ell} < u & k < \ell \quad . \end{cases}$$

Nous définissons maintenant l'ensemble $\mathcal{R}_u^{**}$ comme les points $S \in \mathcal{P}$, tels que si $S = D[T]$, $D = [d_1 \ , \ \dots \ , \ d_n]$ est diagonal et $T = (t_{k\ell})$ est triangulaire, D et T vérifiant les conditions (25). Comme d'après le lemme (4), la transformation (19) est unique, la région $\mathcal{R}_u^{**}$ est définie. Si donc $\mathcal{R}_t^{*}$ est donné, il existe un $u = u(t \ , \ n)$ tel que $\mathcal{R}_t^{*} \subset \mathcal{R}_u^{**}$.

Réciproquement en supposant (25) vérifié, on démontre (17) en utilisant (20) ; ce qui montre que u étant donné, il existe un $t = t(u \ , \ n)$ tel que $\mathcal{R}_u^{**} \subset \mathcal{R}_t^{*}$ alors

$$\text{(26)} \qquad (18) \implies \lim_{u \to \infty} \mathcal{R}_u^{**} = \mathcal{P} \quad .$$

THÉORÈME 6. - Soient S et T deux matrices dans $\mathcal{R}_t^{*}$, G une matrice entière telle que $S[G] = T$ et v. a. $|G| < t$; alors les éléments de G sont, en valeur

absolue, plus petits qu'une constante C dépendant seulement de t et de n.

La démonstration de ce théorème est basée sur les 2 lemmes suivants.

LEMME 6. - Soit $S \in \mathcal{P}$, t un nombre réel tel que $S \in \mathcal{R}_t^*$ et S_0 la matrice diagonale $[s_1, s_2, \dots, s_n]$, il existe alors une constante $C = C(t, n)$ telle que, quel que soit le vecteur $\underset{\sim}{x}$, on ait

$$\frac{1}{C} S_0[\underset{\sim}{x}] \leqslant S[\underset{\sim}{x}] \leqslant C\, S_0[\underset{\sim}{x}] \quad .$$

DÉMONSTRATION. - Soit p^{-1} la matrice diagonale $[\sqrt{s_1}, \dots, \sqrt{s_n}]$ et $W = S[p]$; on voit très facilement que pour démontrer le lemme il suffit de montrer que

$$\frac{1}{C} \underset{\sim}{x}' \underset{\sim}{x} \leqslant W[x] \leqslant C\, \underset{\sim}{x}' \underset{\sim}{x} \quad .$$

Pour cela, la matrice étant positive, il suffit que les valeurs propres $\lambda_1, \dots, \lambda_n$ de W soient bornées par des constantes ne dépendant que de t et de n. Posons $W = (w_{k\ell})$, on a :

$$w_{k\ell} = s_{k\ell} / \sqrt{s_k\, s_\ell}$$

et comme $S \in \mathcal{R}_t^*$, on a :

$$\text{v. a. } w_{k\ell} = \text{v. a. } \frac{s_{k\ell}}{s_k} \sqrt{s_k / s_\ell} < t.C_1 \ , \quad k \leqslant \ell \quad \text{(d'après 17)} \quad .$$

où C_1 ne dépend que de t et de n. W étant symétrique, il en résulte que les éléments de W sont, en valeur absolue, plus petits qu'une constante $C_2 = C_2(t, n)$. Alors tous les coefficients du polynôme caractéristique $f(\lambda) = |\lambda E - W|$ de W sont bornés, en valeur absolue, par une constante $C_3 = C_3(t, n)$. Comme $W > 0$ ses valeurs propres sont bornées par $C_4 = C_4(t, n)$. D'autre part

$$\lambda_1 \dots \lambda_n = |W| = \frac{|S|}{s_1 \dots s_n} > t^{-1}$$

qui entraîne qu'il existe une constante $C_5 = C_5(t, n)$ telle que $\lambda_i > C_5(t, n)$, $i = 1, \dots, n$.

LEMME 7. - Si $S \in \mathcal{R}_t^*$ et $S = \begin{pmatrix} S_1 & S_{12} \\ S_{12}' & S_2 \end{pmatrix}$, tous les éléments de $S_1^{-1} S_{12}$ sont bornés, en valeur absolue, par une constante, ne dépendant que de t et de n.

DÉMONSTRATION. - D'après le lemme (4), on a $S = D[T]$. Comme $\mathcal{R}_t^* \subset \mathcal{R}_u^{**}$ pour $u = u(t , n)$, les éléments de T sont, en valeur absolue, $\leqslant u$ (2e relation (25)).

Posons

$$T = \begin{pmatrix} T_1 & T_{12} \\ 0 & T_2 \end{pmatrix}, \quad D = \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix}$$

où D_1 et T_1 ont le même nombre de lignes et de colonnes que S_1 ; on trouve :

$$S_1 = D_1[T_1] , \quad S_{12} = T_1' D_1 T_{12} \quad \text{donc} \quad S_1^{-1} S_{12} = T_1^{-1} T_{12} .$$

Comme T_1 est une matrice triangulaire, il en est de même de T_1^{-1} et ses éléments $\leqslant u_1$, en valeur absolue, où $u_1 = u_1(t , n)$. Les éléments de T_{12} sont $\leqslant u_1$ et le lemme est démontré.

Démonstration du théorème 6. - Toutes les constantes $c_1 , c_2 , \cdots$ dans cette démonstration dépendent seulement de t et de n, et, le terme "borné" signifie toujours : borné par de telles constantes et en valeur absolue.

Soit $G = (g_{k\ell})$, $\underset{\sim}{g}_1 , \cdots , \underset{\sim}{g}_n$ les n-colonnes de G, nous avons $S[\underset{\sim}{g}_\ell] = t_\ell$, $\ell = 1 , \cdots , n$. Le lemme (6) donne alors

$$S_0[\underset{\sim}{g}_\ell] \leqslant C_1 \, S[\underset{\sim}{g}_\ell] = C_1 \, t_1$$

mais

$$S_0[\underset{\sim}{g}_\ell] = \sum_k s_k \, g_{k\ell}^2$$

donc

$$s_k \, g_{k\ell}^2 \leqslant C_1 \, t_\ell , \quad \ell , k = 1 , \cdots , n \qquad (27)$$

D'après l'hypothèse, on a $|G| \neq 0$, donc dans l'expension de $|G|$, il existe un terme non nul, c'est-à-dire il existe une permutation $\ell_1 , \cdots , \ell_n$ de $1 , 2 , 3 , \cdots , n$ telle que $g_{1\ell_1} \, g_{2\ell_2} \cdots g_{n\ell_n} \neq 0$.

La relation (27) donne alors :

$$(28) \qquad s_k \leq s_k \, g^2_{k\ell_k} \leq C_1 \, t_{\ell k} \, , \quad k = 1 \, , \ldots \, , n \quad .$$

Considérons les entiers $k \, , \, k+1 \, , \ldots$ et $\ell_k \, , \, \ell_{k+1} \, , \ldots \, , \ell_n$; tous les nombres $\ell_k \, , \, \ell_{k+1} \, , \ldots$ ne sont pas $> k$, donc il existe un $i \geq k$ tel que $\ell_i \leq k$. Alors d'après (17),

$$i \geq k \implies s_k \leq s_i \leq e_1 \, t_{\ell i} \quad \text{et} \quad \ell_i \leq k \implies t_{\ell i} \leq t_k$$

donc d'après (28) on trouve

$$(29) \qquad s_k \leq C_2 \, t_k \, , \quad k = 1 \, , \ldots \, , n$$

on a d'ailleurs

$$\prod_{k=1}^{n} \frac{t_k}{s_k} = \frac{t_1 \cdots t_n}{|T|} \cdot \frac{|S|}{s_1 \cdots s_n} \, |G|^2$$

où les 3 facteurs sont bornés donc

$$\prod_{k=1}^{n} \frac{t_k}{s_k} < C_3$$

et

$$(30) \qquad (44) \implies t_k \leq C_4 \, s_k \, , \quad k = 1 \, , 2 \, , \ldots \, , n \quad .$$

Les deux relations (27) et (30) donnent alors

$$(31) \qquad s_k \, g^2_{k\ell} < C_5 \, s_\ell \, , \quad k \, , \ell = 1 \, , \ldots \, , n \quad .$$

Définissons maintenant p comme le plus grand entier tel que

$$(32) \qquad s_k \geq C_5 \, s_\ell \, , \quad k \geq p \, , \quad \ell \leq p - 1$$

relation qui ne peut pas avoir lieu pour $p = 1$.

D'après cette définition, pour tout entier g , tel que $p + 1 \leq g \leq n$, il existe un $k_g \geq g$ et un $\ell_g < g$, tel que

$$(33) \qquad s_{k_g} < C_5 \, s_{\ell_g} \quad ;$$

relation qui est vraie pour $p = n$, mais non pas pour $p = 1$. Comme on a

$S \in \mathcal{R}_t^*$, il existe une constante C_6 telle que

$$s_k < C_6\, s_\ell \ , \quad k \leqslant \ell \tag{34}$$

alors les relations (33) et (34) entraînent

$$s_g < C_7\, s_{g-1} \ , \quad g \geqslant p+1 \quad \text{où} \quad C_7 = C_5\, C_6^2 \tag{35}$$

et (34) et (35) entraînent

$$\frac{1}{C_8} < \frac{s_k}{s_\ell} < C_8 \ , \quad k \geqslant p \ , \quad \ell \geqslant p \quad . \tag{36}$$

Les relations (31) et (32) entraînent, pour $k \geqslant p$ et $\ell \leqslant p-1$,

$$s_k\, g_{k\ell}^2 < C_5\, s_\ell \leqslant s_k \quad ;$$

comme $s_k \neq 0$, ceci entraîne $g_{k\ell}^2 < 1$. Mais $g_{k\ell}$ est entier, donc

$$g_{k\ell} = 0 \ , \quad k \geqslant p \ , \quad \ell \leqslant p-1 \quad . \tag{37}$$

D'après (37), si on fait une partition de G : $G = \begin{pmatrix} G_1 & G_{12} \\ G_{21} & G_2 \end{pmatrix}$ où G_1 est une matrice entière d'ordre $p-1$, on a

$$G_{21} = 0 \tag{38}$$

supposons maintenant $k \geqslant p$, $\ell \geqslant p$; alors (36) donne :

$$g_{k\ell}^2 < C_5\, \frac{s_\ell}{s_k} < C_5\, C_8 \tag{39}$$

qui signifie que les éléments de G_2 sont bornés. Remarquons que pour $p = 1$, la relation (39) donne une démonstration du théorème, donc dans ce qui suit nous supposons $p > 1$. Pour démontrer le théorème, nous utilisons une induction sur n . Pour $n = 1$, le théorème est vrai ; supposons-le vrai pour $n-1$. Faisons une partition de S et de T sous la forme

$$S = \begin{pmatrix} S_1 & S_{12} \\ S_{12}' & S_2 \end{pmatrix}, \quad T = \begin{pmatrix} T_1 & T_{12} \\ T_{12}' & T_2 \end{pmatrix}$$

où S_1 et T_1 sont des matrices carrées d'ordre $p-1$. Comme on a $S[G] = T$ compte tenu de (38) on trouve

$$(40)\qquad \begin{cases} S_1[G_1] = T_1 \\ G_1' S_1 G_{12} + G_1' S_{12} G_2 = T_{12} \end{cases}$$

on a d'après (38) : $|G| = |G_1||G_2|$, comme G est entière on a v. a. $|G_1| < t$. Mais S_1 et T_1 sont des matrices carrées d'ordre $p-1$ qui sont dans $\mathcal{R}^*_{t,p-1}$, où $\mathcal{R}^*_{t,p-1}$ est le même que $\mathcal{R}^*_t$ mais pour des matrices d'ordre $p-1$. La relation (40) (1re relation) et l'hypothèse d'induction entraînent que G_1 est bornée.

D'après la première relation (40), on a $G_1' S_1 = T_1 G_1^{-1}$, ce qui permet d'écrire la 2e relation (40) sous la forme

$$G_{12} = G_1 T_1^{-1} T_{12} - S_1^{-1} S_{12} G_2$$

et le lemme (7) montre que G_{12} est borné. Le théorème est donc démontré.

En particulier on a :

COROLLAIRE. - Si S et T sont dans $\mathcal{R}^*_t$ et $S[U] = T$, pour un U unimodulaire, U appartient à un ensemble fini de matrices unimodulaires complètement déterminées par t et n .

7. Espaces des matrices réduites. - Nous avons remarqué que si $T > 0$, il existe dans la classe de T une matrice S semi-réduite. Considérons les 2^n matrices unimodulaires de la forme $A = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$ où $a_i = \pm 1$. Si S est semi-réduite $S[A]$ est aussi semi-réduite, car si $\underset{\sim}{x}$ est un k-vecteur admissible $A\underset{\sim}{x}$ est aussi un k-vecteur admissible.

Comme les éléments diagonaux de S et de $S[A]$ sont les mêmes, nous allons choisir A telle que $S[A]$ vérifie d'autres conditions. On a $S[A] = S[-A]$, pn peut donc supposer $a_1 = 1$. Soient $\underset{\sim}{\alpha}_1, \ldots, \underset{\sim}{\alpha}_n$ les n-colonnes de la matrice A . On a $\underset{\sim}{\alpha}_1' S \underset{\sim}{\alpha}_2 = a_2 s_{12}$. Si $s_{12} \neq 0$, on choisit a_2 tel que $a_2 s_{12} \geqslant 0$; si $s_{12} = 0$, on choisit a_2 arbitrairement. Ayant choisi $a_1, \ldots, a_k$, considérons $\underset{\sim}{\alpha}_k' S \underset{\sim}{\alpha}_{k+1} = a_k a_{k+1} s_{k,k+1}$; comme a_k a été choisi, on choisit $a_{k+1} = \pm 1$ par la condition $a_k a_{k+1} s_{k,k+1} \geqslant 0$, si $s_{k,k+1} \neq 0$, sinon on choisit a_{k+1} arbitrairement. Ainsi nous avons montré que dans chaque classe de matrices équivalentes, il existe une matrice S vérifiant :

$$(41)\begin{cases}\alpha.\ s_1 > 0 \\ \beta.\ s_{k,k+1} \geqslant 0\ ,\quad k = 1\ ,\ \dots\ ,\ n-1 \\ \gamma.\ S[\underset{\sim}{x}] - s_k \geqslant 0\ ,\quad k = 1\ ,\ \dots\ ,\ n \text{ pour tout } k\text{-vecteur admissible}\end{cases}.$$

Une telle matrice sera appelée réduite au sens de MINSKOWSKI. Soit $\mathcal{R}$ le sous-ensemble des matrices réduites on a

$$(42) \qquad \mathcal{R} \subset \mathcal{R}_0 \quad .$$

Comme les éléments de $S \in \mathcal{P}$ sont les coordonnées de S, les conditions (β) et (γ) montrent que $\mathcal{R}$ est défini comme l'intersection d'une infinité de demi-espaces fermés de $\mathcal{P}$. Nous notons les fonctions linéaires des conditions (β) et (γ) par L_r, $r = 1, 2, 3, \dots$. Nous laissons de côté le cas où un L_r est identiquement nul. Cela arrive par exemple quand dans (γ), $\underset{\sim}{x}$ est un k-vecteur admissible égal à $\pm e_k$. Ainsi la région $\mathcal{R}$ est définie par

$$(43)\begin{cases}\bar{\alpha}.\ s_1 > 0\ , \\ \bar{\beta}.\ L_r \geqslant 0\ ,\quad r = 1\ ,\ 2\ ,\ 3\ ,\ \dots\end{cases}$$

Nous allons voir que le système d'une infinité d'inéquations linéaires, qu'on a ainsi, peut être remplacé par un nombre fini d'entre elles :

DÉFINITION.

1° S s'appelle un point intérieur de $\mathcal{R}$ si $s_1 > 0$ et $L_r(S) > 0$ pour tout r.

2° On dit que c'est un point frontière de $\mathcal{R}$, si $s_1 > 0$ et $L_r(S) \geqslant 0$, pour tout r, mais $L_r(S) = 0$ au moins pour un r.

3° Il est un point extérieur de $\mathcal{R}$, si $s_1 > 0$ et $L_r(S) < 0$ au moins pour un r.

On vérifie très facilement que la forme quadratique

$$S[x] = x_1^2 + \dots + x_n^2 + (p_1 x_1 + \dots + p_n x_n)^2$$

où $p_1, \dots, p_n$ sont n-nombres réels vérifiant les relations

$$0 < p_1 < p_2 < \dots < p_n < 1$$

est un point intérieur de $\mathcal{R}$ ce qui montre que l'ensemble des points intérieurs n'est pas vide.

THÉORÈME 7. - L'ensemble des points intérieurs de $\mathcal{R}$ est un ouvert de $\mathcal{P}$ ainsi que l'ensemble des points extérieurs de $\mathcal{R}$. $\mathcal{R}$ est un ensemble fermé de $\mathcal{P}$, et l'ensemble des points frontières de $\mathcal{R}$ constitue la frontière de $\mathcal{R}$ dans la topologie de $\mathcal{P}$.

DÉMONSTRATION. - Soit S un point intérieur de $\mathcal{R}$, on a $s_1 > 0$, $L_r > 0$ pour tout r. Les inégalités $s_{k,k+1} > 0$ étant en nombre fini peuvent être vérifiées en tous les points d'un voisinage, suffisamment petit, de S. Considérons donc l'infinité des inégalités restantes. Soit S^* un point voisin de S, en ce sens que les éléments de $S^* - S$ sont assez petits, et posons $S^* = (s^*_{k\ell})$. Soient $\varepsilon > 0$ et $\underset{\sim}{x}$ un k-vecteur admissible $\neq \pm \underset{\sim}{e}_k$. On peut choisir S^* suffisamment voisin de S, pour qu'on ait

$$(S^* - S)[\underset{\sim}{x}] \geqslant - \varepsilon \underset{\sim}{x}' \underset{\sim}{x} \quad ;$$

on a alors

$$S^*[\underset{\sim}{x}] - s^*_k = (S^* - S)[\underset{\sim}{x}] + S[\underset{\sim}{x}] - s^*_k \geqslant - \varepsilon \underset{\sim}{x}' \underset{\sim}{x} + S[\underset{\sim}{x}] - s^*_k \quad .$$

Si $m > 0$ est la plus petite valeur propre de S, on peut choisir ε assez petit pour que

$$S^*[x] - s^*_k \geqslant \frac{m}{2} \underset{\sim}{x}' \underset{\sim}{x} - s^*_k \quad .$$

Il n'existe qu'un nombre fini de vecteurs entiers $\underset{\sim}{x}$ pour lesquels on ait $\frac{m}{2} \underset{\sim}{x}' \underset{\sim}{x} \leqslant s^*_k$. On peut donc choisir S^* assez voisin de S pour que

$$S^*[\underset{\sim}{x}] - s^*_k \geqslant \frac{m}{2} \underset{\sim}{x}' \underset{\sim}{x} - s^*_k > 0$$

pour tout k-vecteur admissible $\underset{\sim}{x}$. En choisissant ainsi un voisinage de S pour $k = 1, \ldots, n$ nous remarquons qu'il existe toujours un voisinage de S composé de points S^* qui par construction sont des points intérieurs.

Soit maintenant S un point extérieur de $\mathcal{R}$. On a au moins pour un r, $L_r(S) < 0$. Comme les L_r sont des fonctions linéaires, donc continues, des coordonnées de S on peut choisir un voisinage de S tel qu'on ait $L_r < 0$ en chacun de ses points. Ceci montre que l'ensemble des points extérieurs de $\mathcal{R}$ est aussi ouvert. Remarquons que dans ce cas on a affaire à un seul L_r, contrairement

au cas précédent où on devrait considérer tous les L_r .

Soient maintenant S un point frontière de $\mathcal{R}$ et S^* un point intérieur. Considérons les points T_λ définis par :

$$T_\lambda = \lambda S^* + (1 - \lambda)\, S$$

ce sont les points de la droite joignant S et S^* et tout voisinage de S contient des points T_λ avec $\lambda > 0$ et des points T_λ avec $\lambda < 0$. Considérons les points T_λ pour lesquels $0 < \lambda < 1$. Ce sont les points qui sont entre S et S^* . Soit L_r un des polynômes linéaires qui définissent $\mathcal{R}$. On a $L_r(S) \geq 0$ et $L_r(S^*) > 0$ pour tout r donc :

$$L_r(T_\lambda) = \lambda L_r(S^*) + (1 - \lambda)\, L_r(S) > 0$$

donc T_λ est un point intérieur. Soit maintenant T_λ un point avec $\lambda < 0$, comme S est un point frontière, on a pour un r , $L_r(S) = 0$ et pour tel r : $L_r(T_\lambda) = \lambda L_r(S^*) < 0$ qui montre que T_λ est un point extérieur. Les fonctions linéaires étant continues, la limite d'une suite de points de $\mathcal{R}$ est aussi un point de $\mathcal{R}$. Ceci achève la démonstration du théorème.

THÉORÈME 8. - Soient S et S^* deux points de $\mathcal{R}$, tels que $S[U] = S^*$, pour un U unimodulaire $\neq \pm E$. Alors S et S^* sont des points frontières de $\mathcal{R}$ et U appartient à un ensemble fini de matrices unimodulaires, complètement déterminé par l'entier n . Réciproquement si S est un point frontière de $\mathcal{R}$, il existe une matrice unimodulaire $U \neq \pm E$, appartenant à l'ensemble fini de la 1re partie, telle que S[U] soit aussi un point frontière de $\mathcal{R}$.

DÉMONSTRATION. - Considérons 2 cas : 1°, U est une matrice diagonale, 2°, U n'est pas une matrice diagonale.

1° Soit U une matrice diagonale, $U = [a_1 , \dots , a_n]$, où $a_i = \pm 1$. Comme $S[U] = S[-U]$, on peut supposer $a_1 = 1$. Soit a_{k+1} le premier élément $= -1$, on a alors, avec la notation usuelle :

$$s^*_{k,k+1} = - s_{k,k+1} \quad .$$

Mais S et S^* appartiennent à $\mathcal{R}$ donc

$$0 \leq s^*_{k,k+1} = - s_{k,k+1} \leq 0$$

ou bien

$$s_{k,k+1} = 0 = s^*_{k,k+1} \quad .$$

Donc S et S^* sont tous les deux des points frontières de $\mathcal{R}$.

2° Supposons que U n'est pas diagonale, et appelons $\underset{\sim}{u}_1 , \underset{\sim}{u}_2 , \cdots , \underset{\sim}{u}_n$ ses colonnes. Soit $\underset{\sim}{u}_k$ la première colonne qui est différente de celle d'une matrice diagonale. Donc $\underset{\sim}{u}_i = \pm \underset{\sim}{e}_i$, $i = 1 , \cdots , k-1$ (notons que k peut être égal à 1). Alors $U = \begin{pmatrix} D & A \\ 0 & V \end{pmatrix}$ où D est une matrice diagonale unimodulaire et V est une matrice unimodulaire. De même on a $U^{-1} = \begin{pmatrix} D^{-1} & B \\ 0 & V^{-1} \end{pmatrix}$ qui est aussi unimodulaire. Soit $\underset{\sim}{w}_k$ la k-ième colonne de U^{-1} , on a $\underset{\sim}{w}_k \neq \pm \underset{\sim}{e}_k$. Mais

$$s^*_k = S[\underset{\sim}{u}_k] \geqslant s_k \quad \text{et} \quad s_k = S^*[\underset{\sim}{w}_k] \geqslant s^*_k$$

donc

$$S[\underset{\sim}{u}_k] - s_k = 0 = S^*[\underset{\sim}{w}_k] - s^*_k$$

qui montre que S et S^* sont des points frontières de $\mathcal{R}$. Le corollaire du théorème 6 montre que U appartient à un ensemble fini déterminé par n .

Supposons maintenant que S est un point frontière de $\mathcal{R}$. D'après le théorème 7, il existe une suite de points extérieurs $S_1 , S_2 , \cdots$ qui convergent vers S . Si donc k est assez grand, tous les S_k sont dans un voisinage de S , et on peut trouver un t , tel qu'ils soient tous dans le $\mathcal{R}^*_t$ correspondant. A tout indice k correspond une matrice unimodulaire U_k , telle que $S_k[U_k]$ soit dans $\mathcal{R}$; comme $\mathcal{R} \subset \mathcal{R}^*_t$, pour tout k suffisamment grand, S_k et $S_k[U_k]$ sont tous les deux dans $\mathcal{R}^*_t$. Il en résulte, d'après le théorème 6, que les U_k appartiennent à un ensemble fini de matrices bien déterminées par n . Alors il existe une sous-suite $S_{k_1} , S_{k_2} , \cdots$ convergente vers S telle qu'une matrice U unimodulaire, bien déterminée parmi l'ensemble fini précédent, emmène toutes les S_{k_i} dans $\mathcal{R}$. On a

$$\lim_{n\to\infty} S_{k_n} = S \quad ,$$

donc

$$\lim S_{k_n}[U] = S[U]$$

est un point de $\mathcal{R}$. Comme S est aussi un point de $\mathcal{R}$, il résulte de la première partie que S[U] est aussi un point frontière de $\mathcal{R}$. La matrice $U \neq \pm E$, car les S_k sont tous des points extérieurs et $S_k[\bar{u}] \in \mathcal{R}$.

D'après le théorème précédent, il existe un nombre fini de matrices unimodulaires $U_1 , \ldots , U_g$ qui apparaîssent dans la transformation des points frontières en des points frontières.

Si $\underset{\sim}{u}_k$ est la k-ième colonne de l'une de ces matrices, alors $\underset{\sim}{u}_k$ est un k-vecteur admissible ; supposons-le différent de $\pm \underset{\sim}{e}_k$, alors pour tout $S \in \mathcal{R}$, on a $S[\underset{\sim}{u}_k] - s_k \geqslant 0$. Soient $L_1 , L_2 , \ldots , L_h$ toutes les formes linéaires, non identiquement nulles, qui résultent de tous les $\underset{\sim}{u}_k$, $k = 1 , 2 , \ldots , n$ de toutes les matrices $U_1 , \ldots , U_g$, y compris celles résultant de S_{kk+1} , $k = 1 , \ldots , n - 1$; alors d'après ce que nous avons vu, pour un point frontière S de $\mathcal{R}$, il existe un $r \leqslant h$ tel que $L_r(S) = 0$ (non identiquement). Ainsi pour tous les points de $\mathcal{R}$, on a :

$$(44) \qquad s_1 > 0 , \; L_1(S) \geqslant 0 , \ldots , \; L_h(S) \geqslant 0 \quad .$$

Mais ce qui est plus important, c'est le théorème suivant :

THÉORÈME 9. - Un point $S \in \mathcal{P}$ appartient à $\mathcal{R}$, si et seulement si $s_1 > 0$ et $L_r(S) \geqslant 0$ pour $r = 1 , \ldots , h$.

DÉMONSTRATION. - Il suffit de démontrer que la condition (44) est suffisante : soit $S \in \mathcal{P}$ et vérifiant (44), si S n'appartient pas à $\mathcal{R}$, c'est un point extérieur de $\mathcal{R}$, et on a $L_r(S) < 0$ pour un certain $r > h$. Soit S^* un point intérieur de $\mathcal{R}$, et considérons les points $T_\lambda = \lambda S + (1 - \lambda) S^*$, $0 < \lambda < 1$, du segment ouvert joignant S et S^* ; comme l'ensemble des points intérieurs de $\mathcal{R}$ est ouvert, et S est un point extérieur, il existe un $0 < \lambda_0 < 1$ tel que T_{λ_0} est un point frontière de $\mathcal{R}$. Mais, d'après ce que nous avons remarqué, il existe pour T_{λ_0} un $s \leqslant h$ tel que

$$L_s(T_{\lambda_0}) = 0 = \lambda_0 \, L_s(S) + (1 - \lambda_0) \, L_s(S^*) \quad .$$

Mais

$$(1 - \lambda_0) \, L_s(S^*) > 0 \implies L_s(T_{\lambda_0}) > 0 \quad .$$

C'est une contradiction et on a donc $S \in \mathcal{R}$.

Nous avons donc montré que $\mathcal{R}$ est limité par un nombre fini de plans passant tous à l'origine. $\mathcal{R}$ est donc une pyramide. Soit maintenant $\overline{\mathcal{R}}$ la fermeture de $\mathcal{R}$ dans R_h . En tout point de S de $\overline{\mathcal{R}}$ on a, en raison de la continuité des fonctions linéaires :

$$s_1 \geqslant 0 \ , \quad L_r(S) \geqslant 0 \ , \quad r = 1 \ , 2 \ , 3 \ \cdots \quad .$$

Si $S \in \overline{\mathcal{R}}$ et non pas à $\mathcal{R}$, on a $s_1 = 0$ et les autres inégalités entraînent $S = \begin{pmatrix} 0 & 0 \\ 0 & S_1 \end{pmatrix}$. S_1 a aussi des propriétés analogues ; on a donc, ou bien $S = 0$, ou bien $S = \begin{pmatrix} 0 & 0 \\ 0 & S_k \end{pmatrix}$, où S_k n'est pas singulière, et est une matrice réduite d'ordre r , $0 < r < n$. Nous avons donc montré que les points de $\overline{\mathcal{R}}$ qui ne sont pas dans $\mathcal{R}$ sont des matrices semi-positives.

Considérons maintenant l'espace $\mathcal{P}$ et le groupe Γ . Si $U \in \Gamma$, l'application $S \to S[U]$ est un homéomorphisme qui applique $\mathcal{P}$ sur lui-même. Soit $\mathcal{R}_U$ l'ensemble des matrices $S[U]$ pour $S \in \mathcal{R}$ et un $U \in \Gamma$; comme U et $-U$ donnent le même transformé, on a $\mathcal{R}_U = \mathcal{R}_{-U}$. Comme dans chaque classe de matrices il existe une matrice réduite, on a :

a. $\sum_{U \in \Gamma} \mathcal{R}_{\pm U} = \mathcal{P}$ où dans la sommation on identifie U et $-U$. Ainsi les $\mathcal{R}_{\pm U}$ couvrent $\mathcal{P}$ entièrement.

Soient U et $V \in \Gamma$, $U \neq \pm V$ et $S \in \mathcal{R}_U \cap \mathcal{R}_V$, alors $T_1 = S[U^{-1}]$ et $T_2 = S[V^{-1}]$ sont des points de $\mathcal{R}$ et on a : $T_1 = T_2[VU^{-1}]$ et $VU^{-1} \neq \pm E$. D'après le théorème 8, T_1 est un point frontière de $\mathcal{R}$ et, $S \to S[U]$ étant un homéomorphisme, S est aussi un point frontière de $\mathcal{R}_U$ et de $\mathcal{R}_V$, donc :

b. Si U et V sont unimodulaires, et $UV^{-1} \neq \pm E$, $\mathcal{R}_U$ et $\mathcal{R}_V$ peuvent avoir, au plus, des points frontières en commun. En particulier, si $U \neq \pm E$, $\mathcal{R}$ et $\mathcal{R}_U$ peuvent avoir seulement des points frontières en commun. Si $S \in \mathcal{R} \cap \mathcal{R}_U$, S et $S[U^{-1}]$ sont dans $\mathcal{R}$ et, d'après le théorème 8, U appartient à un ensemble fini de matrices dépendant seulement de n . Si nous appelons $\mathcal{R}_U$ un "voisin" de $\mathcal{R}$, quand $\mathcal{R} \cap \mathcal{R}_U$ n'est pas vide, nous avons montré que

c. $\mathcal{R}$ a seulement un nombre fini de voisins.

Soit maintenant k un sous-ensemble compact de $\mathcal{P}$, il est donc borné dans $\mathcal{P}$, et il existe un $t > 0$ tel que $k \subset \mathcal{R}_t^*$. Supposons que, pour un U unimodulaire, $\mathcal{R}_U$ coupe k, et soit $S \in \mathcal{R}_U \cap k$, alors il existe un $T \in \mathcal{R}$ tel que $T[U] = S$. On a pour t assez grand, $\mathcal{R} \subset \mathcal{R}_t^*$, donc T et S sont dans $\mathcal{R}_t^*$ et, d'après le théorème 6, U appartient à un ensemble fini de matrices. Il existe donc un nombre fini de matrices unimodulaires $U_1, \ldots, U_p$ telles que $k \subset \sum_{i=1}^{p} \mathcal{R}_{U_i}$; ceci montre que :

d. Tout sous-ensemble compact de $\mathcal{P}$ est couvert par un nombre fini d'images $\mathcal{R}_V$ de $\mathcal{R}$.

On a ainsi obtenu les résultats fondamentaux de la théorie de réduction de MINKOWSKI.

8. Application. - Soit S une matrice positive, réduite et entière ; on a $s_1 s_2 \ldots s_n \leqslant b_n |S|$ où $s_1, \ldots, s_n$ sont positifs et b_n ne dépend que de n. Il en résulte que, pour un $|S|$ donné, il existe seulement un nombre fini de valeurs entières pour $s_1, \ldots, s_n$. D'ailleurs on a :

$$- s_k \leqslant 2 s_{k\ell} \leqslant s_k , \quad k < \ell$$

donc, les $s_{k\ell}$ étant entiers, il n'existe qu'un nombre fini de $s_{k\ell}$ vérifiant la relation précédente.

Comme toutes les matrices de la même classe ont le même déterminant, et que dans chaque classe il existe au moins une matrice, nous avons le théorème suivant :

THÉORÈME 10. - Il existe seulement un nombre fini de matrices entières, positives et réduites ayant le même déterminant et un nombre fini de classes de matrices entières et positives ayant un déterminant donné.

BIBLIOGRAPHIE

[1] JONES (Burton W.). - The arithmetic theory of quadratic forms. - The Mathematical Association of America, 1950 (The Carus mathematical Monographs, 10).

[2] MIRSKY (L.). - An introduction to linear algebra. - Oxford, at the Clarendon Press, 1955.

[3] SIEGEL (Carl Ludwig). - Lectures on quadratic forms. - Bombay, Tata Institute of fundamental Research, 1957 (Tata Institute of fundamental Research, Lectures on Mathematics, 7).

[4] SIEGEL (Carl Ludwig). - Einheiten quadratischer Formen, Abh. Math. Sem. Hansischen Univ., t. 13, 1940, p. 209-239.

[5] SIEGEL (Carl Ludwig). - Zur Reduktionstheorie quadratischer Formen. - Tokyo, Mathematical Society of Japan, 1959 (Publ. Math. Soc. Japan, 5).

[6] WATSON (G. L.). - Integral quadratic forms. - Cambridge, Cambridge University Press, 1960 (Cambridge Tracts in Mathematics, 51).