Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 12 (1939-1940)

Artikel: Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini.
Autor: Humbert, Pierre
DOI: https://doi.org/10.5169/seals-12808

Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini

Par PIERRE HUMBERT, Lausanne

Introduction

Dans la théorie des formes quadratiques, les classes de formes équivalentes relativement à un groupe de substitutions linéaires et homogènes jouent un rôle important. Lorsque ce groupe est celui des substitutions non dégénérées à coefficients réels, on peut représenter chaque classe par la forme canonique $\sum_i \pm x_i^2$. Les seuls invariants sont alors le nombre des carrés pris positivement et celui des carrés pris négativement, c'est-à-dire la signature. Dans l'arithmétique des formes quadratiques, on envisage l'équivalence relativement au groupe des substitutions à coefficients entiers rationnels et de déterminant ± 1 (substitutions unimodulaires). La signature et le déterminant de la forme sont des invariants, mais ils sont loin de caractériser complètement chaque classe. On sait, par exemple, que pour une signature et un déterminant donnés, il peut y avoir plusieurs classes de formes à coefficients entiers (toutefois un nombre fini).

Le problème de reconnaître si deux formes quadratiques sont arithmétiquement équivalentes ou non a été résolu par Lagrange[1]) pour les formes binaires définies positives au moyen de la théorie de la réduction, théorie qui a été étendue par Seeber[2]) au cas ternaire et généralisée par Minkowski[3]) au cas de n variables. D'illustres mathématiciens, entre autres Gauss, Dirichlet, Hermite, se sont aussi occupés de cette théorie, dont l'idée est la suivante: Dans chaque classe de formes quadratiques définis positives on détermine, par certaines conditions de minimum, une forme réduite. L'ensemble de toutes les réduites constitue, dans l'espace des formes, un domaine fondamental R relativement au groupe des transformations unimodulaires. L'équivalence de deux formes revient à l'identité de leurs réduites, exception faite pour la frontière de R, où il peut exister plusieurs formes réduites équivalentes.

---

[1]) *Lagrange*, Oeuvres, t. III, p. 723—728 (Paris, 1869).

[2]) *Seeber*, Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen, (Freiburg i. B. 1831).

[3]) *Minkowski*, Gesammelte Abhandlungen, Bd. 2, S. 53 (Leipzig und Berlin, 1911).

C'est à Minkowski que l'on doit les résultats essentiels de cette théorie: le domaine R est l'intérieur d'un angle solide convexe limité par un nombre fini d'hyperplans, et touche à un nombre *fini* seulement de domaines équivalents (transformés de R par des substitutions unimodulaires). Ces résultats, outre leur intérêt pour la théorie des formes quadratiques, interviennent avec fruit dans l'étude des représentations rationnelles des groupes d'ordre fini.

L'objet du présent travail est d'étendre la théorie de la réduction des formes quadratiques définies positives, au cas où le groupe unimodulaire rationnel est remplacé par le groupe des substitutions à coefficients entiers dans un corps algébrique K fini de degré g et dont le déterminant est une unité de K (groupe unimodulaire dans K). Mais ce groupe n'est pas proprement discontinu dans l'espace des formes quadratiques, aussi est-on conduit à considérer des systèmes de g formes, transformées respectivement par g substitutions unimodulaires conjuguées. A chacun des corps conjugués réels $K^{(i)}$ de K correspond dans un de ces systèmes une forme définie positive, et à deux corps $K^{(l)}$, $\overline{K}^{(l)}$ imaginaires conjugués correspondent deux formes hermitiennes définies positives et imaginaires conjuguées. Le groupe envisagé est proprement discontinu dans l'espace de ces systèmes, et les résultats de Minkowski subsistent: Il existe un domaine fondamental formé par la réunion d'un ou de plusieurs angles solides convexes R_μ limités par un nombre fini d'hyperplans; chacun des R_μ n'est en contact qu'avec un nombre fini de domaines équivalents à des R_ν. Il s'ensuit par exemple que le groupe unimodulaire de degré n dans K possède un nombre fini d'éléments générateurs.

La méthode que j'ai employée diffère peu dans ses grandes lignes de celle que Minkowski utilisa pour le groupe unimodulaire rationnel; les idées directrices sont les mêmes. Au lieu du principe des „tiroirs" de Dirichlet, j'ai fait usage du théorème plus profond de Minkowski sur les formes linéaires, théorème qui a de si belles applications en théorie des nombres. En outre le passage d'un système de formes donné au système réduit équivalent se fait en deux étapes, ce qui permet de tourner la difficulté due au nombre des classes de K et à l'introduction simultanée de tous les conjugués de K. C'est la deuxième étape qui donne lieu aux différents domaines R_u dont se compose le domaine fondamental.

Encouragé, orienté par M. C. L. Siegel, qui m'a mis sur la voie de ce travail, je suis heureux de lui exprimer ici ma profonde reconnaissance pour ses conseils et pour l'intérêt qu'il m'a témoigné lors de mon séjour à Göttingue.

§ 1. Enoncé du problème et méthode

Soit K un corps algébrique fini donné, de degré g. Si g_1 désigne le nombre des conjugués réels et $2g_2$ celui des conjugués imaginaires de K, on a

$$g = g_1 + 2g_2 .$$

On pose

$$\gamma = g_1 + g_2 .$$

Les conjugués sont numérotés de telle manière que les corps $K^{(1)}, \ldots, K^{(g_1)}$ soient réels, et les corps $K^{(g_1+\varrho)}$ et $K^{(g_1+g_2+\varrho)}$ imaginaires conjugués $(\varrho = 1, \ldots, g_2)$.

Par *substitution unimodulaire dans* K nous entendrons une substitution linéaire et homogène dont les coefficients sont des entiers de K et le déterminant une unité de K. $\mathfrak{U}$ désignant la matrice d'une pareille substitution, on aura

$$\mathfrak{U} \text{ entière dans } K; \quad |\mathfrak{U}| = \varepsilon = \text{unité de } K.$$

Les substitutions unimodulaires dans K d'un même degré n forment un groupe, *le groupe unimodulaire de degré n dans K*.

Par *système* S nous entendrons un ensemble de γ formes quadratiques à n variables, constitué par

g_1 *formes définies positives*, de matrices symétriques réelles $\mathfrak{S}^{(1)}, \ldots, \mathfrak{S}^{(g_1)}$,

g_2 *formes hermitiennes définies positives*, de matrices complexes $\mathfrak{H}^{(1)}, \ldots, \mathfrak{H}^{(g_2)}$.

Si l'accent désigne la matrice transposée, on a

$$\mathfrak{S}^{(k)\prime} = \mathfrak{S}^{(k)} .$$

$\overline{\mathfrak{H}}$ désignant la matrice dont les éléments sont conjugués complexes de ceux de $\mathfrak{H}$, on a

$$\overline{\mathfrak{H}}^{(k)} = \mathfrak{H}^{(k)\prime} .$$

Deux systèmes S_1 et S_2 sont dits *équivalents*, $S_1 \sim S_2$, s'il existe une matrice $\mathfrak{U}$ unimodulaire dans K, telle que l'on ait

$$\mathfrak{U}^{(k)\prime}\, \mathfrak{S}_1^{(k)}\, \mathfrak{U}^{(k)} = \mathfrak{S}_2^{(k)} \qquad k = 1, 2, \ldots, g_1$$

et

$$\mathfrak{U}^{(g_1+k)\prime}\, \mathfrak{H}_1^{(k)}\, \overline{\mathfrak{U}}^{(g_1+k)} = \mathfrak{H}_2^{(k)} \qquad k = 1, 2, \ldots, g_2 .$$

La notation $\mathfrak{U}^{(k)}$ désigne la matrice formée des $k^{\text{ièmes}}$ conjugués des éléments de $\mathfrak{U}$.

La relation $S_1 \sim S_2$ est réflexive, symétrique, transitive, puisque les substitutions unimodulaires $\mathfrak{U}$ forment un groupe. Les systèmes S sont ainsi partagés en classes de systèmes équivalents. Le problème qui se pose est le suivant:

Deux systèmes S_1 et S_2 étant donnés, reconnaître s'ils sont équivalents ou non. On le résoudra ici en généralisant la théorie de la réduction des formes quadratiques définies positives de Minkowski[4]*). Il s'agira de construire un domaine fondamental pour les systèmes S relativement au groupe unimodulaire dans K, ces systèmes se transformant comme il a été indiqué.*

Dans ses grandes lignes la méthode est la suivante: soit un système S formé des γ matrices $\mathfrak{S}^{(k)} = (s_{ij}^{(k)})$, $k = 1, \ldots, g_1$, $\mathfrak{H}^{(\varrho)} = (h_{ij}^{(\varrho)})$, $\varrho = 1, \ldots, g_2$. Appelons pour un instant *famille de S* l'ensemble de tous les systèmes obtenus à partir de S par transformation avec des substitutions entières dans K et non dégénérées, c'est-à-dire l'ensemble des systèmes de γ matrices $\mathfrak{A}^{(k)'}\mathfrak{S}^{(k)}\mathfrak{A}^{(k)}$, $k=1, \ldots, g_1$, $\mathfrak{A}^{(g_1+\varrho)'}\mathfrak{H}^{(\varrho)}\mathfrak{A}^{(g_1+\varrho)}$, $\varrho=1, \ldots, g_2$, $\mathfrak{A}$ parcourant toutes les matrices à éléments entiers de K et telles que $|\mathfrak{A}| \neq 0$. Parmi les systèmes de la famille de S, extrayons tous ceux pour lesquels la somme $t_{11} = \sum_{k=1}^{g_1} s_{11}^{(k)} + \sum_{k=1}^{g_2} h_{11}^{(k)}$ est minimum. Puis parmi ces derniers systèmes, ayant tous la même valeur minimum pour la somme t_{11}, extrayons ceux pour lesquels la somme $t_{22} = \sum_{k=1}^{g_1} s_{22}^{(k)} + \sum_{k=1}^{g_2} h_{22}^{(k)}$ est minimum. Continuant ainsi jusqu'à la somme t_{nn}, on obtient finalement un (ou éventuellement plusieurs) système $\dot{S}$ de la famille de S. $\dot{S}$ est le transformé de S par une substitution entière dans K, non dégénérée, de matrice $\mathfrak{A}_0$ (première transformation). On démontre (théorème 1) que cette matrice $\mathfrak{A}_0$, si elle n'est pas unimodulaire, a néanmoins un déterminant de norme bornée, la borne étant indépendante du système initial S. Il en résulte (théorème 2) que $\mathfrak{A}_0 = \mathfrak{U}\mathfrak{A}_\nu$, où $\mathfrak{A}_\nu$ appartient à un ensemble fini de matrices entières non dégénérées $\mathfrak{A}_1, \ldots, \mathfrak{A}_N$, et où $\mathfrak{U}$ est unimodulaire dans K. En transformant le système $\dot{S}$ par l'inverse $\mathfrak{A}_\nu^{-1}$ de $\mathfrak{A}_\nu$, on obtient un système $\ddot{S}$ équivalent à S et qui est le système réduit de S (deuxième transformation).

A chacune des matrices $\mathfrak{A}_\nu$ correspond un certain domaine R_ν de l'espace des S, domaine défini par les inégalités exprimant les conditions de minimum auxquelles le système $\dot{S}$ est assujetti. La réunion de ces R_ν, $\nu = 1, \ldots, N$, constitue un domaine fondamental R pour les systèmes S

[4]) *H. Minkowski*, Diskontinuitätsbereich für arithmetische Äquivalenz, Journal de Crelle, 129, p. 220 ; ou Gesammelte Abhandlungen von H. Minkowski, Bd. 2, S. 53.

relativement au groupe unimodulaire dans K (théorème 3). On démontre (théorème 6) que les substitutions unimodulaires transformant les uns dans les autres les systèmes frontières du domaine R sont en nombre *fini*. Il s'ensuit immédiatement que le domaine fondamental touche un nombre fini seulement de domaines équivalents, c'est-à-dire transformés de R par des substitutions unimodulaires. On voit enfin (théorème 7), que chacun des domaines R_ν est l'intérieur d'un angle solide convexe limité par un nombre *fini* d'hyperplans passant par l'origine de l'espace des S.

§ 2. Préliminaires. – Notations

Dans la mesure du possible, on se servira de matrices dans les calculs. Les majuscules allemandes désignent des matrices quadratiques, parfois rectangulaires. Les minuscules allemandes désignent toujours des colonnes, ou *vecteurs*, matrices d'un type particulier. $\mathfrak{E}_k$ est la matrice unité de degré k, et $\mathfrak{E}$ la matrice unité de degré convenable (pour autant que l'omission du degré ne nuise pas à la clarté). $\mathfrak{D}(a_1, \ldots, a_n)$ désigne la matrice diagonale d'éléments diagonaux $a_1, \ldots, a_n$, c'est-à-dire la matrice ayant $a_1, \ldots, a_n$ dans sa diagonale principale et partout ailleurs des zéros. Ainsi $\mathfrak{E} = \mathfrak{D}(1, \ldots, 1)$.

$\mathfrak{A}$ étant une matrice quelconque, $\mathfrak{A}'$ désigne sa transposée, c'est-à-dire la matrice ayant pour lignes les colonnes de $\mathfrak{A}$ et vice-versa. Si une matrice $\mathfrak{A} = (\alpha_{ij})$ a tous ses éléments α_{ij} dans le corps K, on représente par $\mathfrak{A}^{(k)}$ la matrice formée par les $k^{\text{ièmes}}$ conjugués des éléments de $\mathfrak{A}$, soit

$$\mathfrak{A}^{(k)} = (\alpha_{ij}^{(k)}) \ .$$

On dit qu'une matrice est bornée, si tous ses éléments le sont. Pour une colonne $\mathfrak{x} = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ la notation $|\mathfrak{x}| \leqslant c$ est une abréviation pour

$$|\xi_i| \leqslant c \ , \quad i = 1, \ldots, n \ .$$

Il y aura parfois avantage à se servir de la matrice:

$$S = \begin{pmatrix} \mathfrak{S}^{(1)} & & & & 0 \\ & \ddots & & & \\ & & \mathfrak{S}^{(\sigma_1)} & & \\ & & & \mathfrak{H}^{(1)} & \\ & & & & \ddots \\ 0 & & & & \mathfrak{H}^{(\sigma_2)} \end{pmatrix}$$

ayant les $\mathfrak{S}$ et les $\mathfrak{H}$ d'un système S dans sa diagonale principale et partout ailleurs des zéros. Il n'y a pas de confusion à craindre si l'on désigne

cette matrice par la même lettre S que le système S. S est une matrice hermitienne définie positive d'un type particulier, de degré $n\gamma$. Si U désigne d'une façon analogue la matrice

$$U = \begin{pmatrix} \mathfrak{U}^{(1)} & 0 \\ & \ddots \\ 0 & \mathfrak{U}^{(\gamma)} \end{pmatrix}$$

on peut écrire $U' S_1 \overline{U} = S_2$ pour l'équivalence de deux systèmes S_1 et S_2. Cette notation abrégée sera quelquefois employée par la suite. Une majuscule allemande désignant une matrice à coefficients dans K, la majuscule latine correspondante représentera la matrice formée comme U l'aide de $\mathfrak{U}$.

On dira qu'une matrice symétrique ou hermitienne $\mathfrak{S}$ est *positive* si la forme correspondante est *définie positive*, et l'on écrira: $\mathfrak{S} > 0$. On appellera matrices *semi-positives* les matrices de formes *semi-définies positives*, et l'on écrira pour elles $\mathfrak{S} \geqslant 0$. On a $|\mathfrak{S}| > 0$ pour les premières et $|\mathfrak{S}| = 0$ pour les secondes.

On peut simplifier les notations en désignant les matrices réelles $\mathfrak{S}^{(k)}$ et les matrices hermitiennes $\mathfrak{H}^{(k)}$ d'un système S par un même symbole $\mathfrak{S}^{(k)}$, k variant alors de 1 à γ. Une matrice positive réelle étant un cas particulier de matrice hermitienne positive, on pourra considérer l'ensemble des $\mathfrak{S}^{(k)}$ comme un système S de γ matrices hermitiennes positives, avec la convention que les g_1 premières d'entre elles soient réelles:

$$\mathfrak{S}^{(k)} = \overline{\mathfrak{S}}^{(k)} \text{ pour } k = 1, \ldots, g_1 .$$

On calcule alors avec les $\mathfrak{S}^{(k)}$ comme avec des matrices hermitiennes. Par exemple, la valeur de la forme de matrice $\mathfrak{S}^{(k)}$ pour la valeur $\mathfrak{x} = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ de la colonne $\mathfrak{x}$ des variables est $\mathfrak{x}' \mathfrak{S}^{(k)} \bar{\mathfrak{x}}$.

Pour abréger, on emploiera la notation de M. Siegel: $\mathfrak{S}[\mathfrak{A}] = \mathfrak{A}' \mathfrak{S} \overline{\mathfrak{A}}$, $\mathfrak{A}$ étant une matrice à n lignes et pouvant avoir un nombre quelconque de colonnes, pour la matrice transformée de $\mathfrak{S}$ par $\mathfrak{A}$.

Unités générales

Les matrices unimodulaires $\mathfrak{F}$ transformant tous les systèmes S en eux-mêmes forment un sous-groupe invariant du groupe multiplicatif des matrices unimodulaires $\mathfrak{U}$ de K. Ces $\mathfrak{F}$ sont définies par les conditions:

$$\mathfrak{S}[\mathfrak{F}^{(k)}] = \mathfrak{F}'^{(k)}\,\mathfrak{S}\,\overline{\mathfrak{F}}^{(k)} = \mathfrak{S} \qquad k = 1, \ldots, g$$

pour toute $\mathfrak{S} > 0$.

Nous allons déterminer ces $\mathfrak{F}$, que nous appellerons *unités générales*. Pour simplifier les notations, supprimons dans $\mathfrak{F}^{(k)}$ l'indice de conjugaison k.

Montrons d'abord que $\mathfrak{S}[\mathfrak{F}] = \mathfrak{S}$ a lieu identiquement en $\mathfrak{S}$. Soit donc $\mathfrak{S}$ une matrice hermitienne quelconque, définie ou indéfinie, de déterminant nul ou non, assujettie à la seule condition d'être réelle si le corps conjugué de K auquel appartiennent les éléments de $\mathfrak{F}$ est réel. Soit, comme précédemment, $\mathfrak{x} = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ la colonne des variables de la forme hermitienne $\mathfrak{S}[\mathfrak{x}]$. Considérons toutes les valeurs des ξ_i telles que $\mathfrak{x}'\bar{\mathfrak{x}} = 1$, c'est-à-dire que $|\xi_1|^2 + \cdots + |\xi_n|^2 = 1$. Pour toutes ces valeurs la forme hermitienne $\mathfrak{S}[\mathfrak{x}]$ est bornée en valeur absolue; il existe un nombre positif μ tel que

$$\mu > |\mathfrak{S}[\mathfrak{x}]| \quad \text{si} \quad \mathfrak{x}'\bar{\mathfrak{x}} = 1\,.$$

A cause de l'homogénéité de $\mathfrak{S}[\mathfrak{x}]$ on a alors:

$$(\mu\mathfrak{E} - \mathfrak{S})\,[\xi] > 0 \quad \text{pour tout} \quad \mathfrak{x} \neq 0\,.$$

La matrice hermitienne $\mu\mathfrak{E} - \mathfrak{S}$ est donc positive, $\mathfrak{F}$ la transforme en elle-même: $(\mu\mathfrak{E} - \mathfrak{S})\,[\mathfrak{F}] = \mu\mathfrak{E} - \mathfrak{S}$. Mais $\mathfrak{F}'\overline{\mathfrak{F}} = \mathfrak{E}[\mathfrak{F}] = \mathfrak{E}$, car $\mathfrak{E}$ est positive, donc $\mathfrak{S}[\mathfrak{F}] = \mathfrak{S}$ c. q. f. d.

En prenant pour $\mathfrak{S}$ des matrices particulièrement simples, on arrive aisément en utilisant ce résultat à déterminer la forme générale de $\mathfrak{F}$. Soient $\mathfrak{S} = (s_{ij})$, $\mathfrak{F} = (\alpha_{ij})$. Prenons pour $\mathfrak{S}$ la matrice dont les éléments sont

$$s_{kk} = 1,\ k \text{ fixe}; \qquad s_{ij} = 0 \text{ si } i, j \neq k\,.$$

On obtient:

$$\alpha_{ki}\,\bar{\alpha}_{kj} = \begin{cases} 0 \text{ si } i, j \neq k\,, \\ 1 \text{ si } i = j = k\,. \end{cases}$$

On a donc $|\alpha_{kk}|^2 = 1$, ce qui implique $\alpha_{kk} \neq 0$. Pour $j = k$ l'égalité précédente donne alors:

$$\alpha_{ik} = 0 \text{ si } i \neq k\,.$$

On voit ainsi que $\mathfrak{F}$ est une matrice diagonale:

$$\mathfrak{F} = \mathfrak{D}\,(\alpha_1, \ldots, \alpha_n) \quad \text{avec} \quad |\alpha_k| = 1\,.$$

Particularisons ensuite $\mathfrak{S}$ en prenant:

$$s_{kl} = 1 \; ; \quad k, l \text{ fixes}, \; k < l \; .$$
$$s_{ij} = 0 \text{ si } (i, j) \neq (k, l) \text{ ou } (l, k) \; .$$

On obtient

$$\alpha_k \bar{\alpha}_l = 1 \; .$$

Multipliant cette égalité par α_l on trouve, à cause de $|\alpha_l| = 1$,

$$\alpha_k = \alpha_l \; .$$

La matrice $\mathfrak{F}$ a donc la forme suivante:

$$\mathfrak{F} = \alpha \mathfrak{E} \quad \text{avec} \quad |\alpha| = 1 \; .$$

Cela devant avoir lieu pour toutes les conjuguées de la matrice $\mathfrak{F}$, α est une racine de l'unité. Désignant les racines de l'unité du corps K par ω, on aura:

$$\mathfrak{F} = \omega \mathfrak{E} \; .$$

Réciproquement, on vérifie immédiatement que toute matrice de la forme $\mathfrak{F} = \omega \mathfrak{E}$ transforme un système S en lui-même. On peut donc formuler le résultat suivant:

Le groupe des unités générales $\mathfrak{F}$ est un groupe multiplicatif d'ordre w (w = nombre des racines de l'unité de K) constitué par les matrices $\omega \mathfrak{E}$ (ω = racine de l'unité de K).

C'est un groupe cyclique, comme on le sait.

Si $g_1 > 0$, K ne contient pas d'autres racines de l'unité que ± 1, et les seules matrices $\mathfrak{F}$ sont $\pm \mathfrak{E}$.

$\mathfrak{U}$ étant une matrice unimodulaire quelconque, on a $\mathfrak{S}[\mathfrak{U}] = \mathfrak{S}[\mathfrak{U}\mathfrak{F}]$. En outre, si $\mathfrak{U} \neq \mathfrak{F}$, il existe au moins un système S de γ matrices hermitiennes positives $\mathfrak{S}^{(k)}$ tel que

$$\mathfrak{S}^{(k)}[\mathfrak{U}^{(k)}] \neq \mathfrak{S}^{(k)} \qquad k = 1, \ldots, \gamma \; .$$

Le problème posé est donc d'une façon plus précise celui de la détermination d'un domaine fondamental pour les systèmes S, relativement aux transformations du groupe quotient $\mathfrak{U}|\mathfrak{F}$.

Un lemme

Soit $\mathfrak{x}$ un vecteur de composantes ξ_i, $i = 1, \ldots, n$, c'est-à-dire une matrice formée de la seule colonne des ξ_i. Les ξ_i étant des entiers algébriques de K, on désignera par x la colonne formée par les γ colonnes conjuguées $\mathfrak{x}^{(k)}$ superposées. Enfin on emploiera le signe τ, qu'on lira *trace*, pour indiquer la sommation de $k = 1$ à $k = \gamma$ sur un indice supérieur k omis dans l'expression sous le signe τ. Ces notations permettent d'écrire:

$$x' S \bar{x} = S[x] = \sum_{k=1}^{\gamma} \mathfrak{S}^{(k)}[\mathfrak{x}^{(k)}] = \tau(\mathfrak{S}[\mathfrak{x}]) .$$

Lemme. Pour un système S donné, il existe un nombre fini seulement de vecteurs $\mathfrak{x}$ entiers de K tels que

$$\tau(\mathfrak{S}[\mathfrak{x}]) = S[x] < c .$$

Cela résulte d'une inégalité connue relative aux formes définies positives. Si $\mu > 0$ désigne le minimum de $S[x]$ pour toutes les valeurs complexes de x telles que

$$x' \bar{x} = 1 , \qquad \mathfrak{x}^{(k)} \text{ réel si } k \leqslant g_1 ,$$

on a

$$S[x] \geqslant \mu\, x' \bar{x} .$$

Par conséquent $S[x] \leqslant c$ entraîne:

$$\mu x' \bar{x} \leqslant c \text{ ou } \mu\tau(\mathfrak{x}' \bar{\mathfrak{x}}) \leqslant c$$

ou encore

$$\sum_{k=1}^{\gamma} \sum_{i=1}^{n} |\xi_i^{(k)}|^2 \leqslant \frac{c}{\mu} .$$

Toutes les composantes $\xi_i^{(k)}$ de x sont donc en valeur absolue inférieures à $\sqrt{\frac{c}{\mu}}$, donc tous les conjugués de ξ_i sont bornés, et par conséquent ξ_i n'est susceptible que d'un nombre fini de valeurs entières de K.

§ 3. Première transformation du système S

Dans ce paragraphe, $\mathfrak{a}, \mathfrak{b}, \ldots, \mathfrak{x}$ désigneront, à moins de mention expresse du contraire, des colonnes ou *vecteurs* dont les n composantes sont des *entiers* du corps K:

$$\mathfrak{a} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \qquad \mathfrak{b} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}, \ldots, \qquad \mathfrak{x} = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix},$$

$\alpha_i, \beta_i, \ldots, \xi_i$ = entiers de K.

Soit un système S. Nous allons lui faire subir la première transformation. Comme on l'a vu au § 1, il s'agit de trouver un système $\dot{S}$ transformé de S par une matrice $\mathfrak{A}$ entière dans K, non dégénérée, de sorte que les quantités $\tau(\dot{s}_{ii}) = \sum_{k=1}^{\gamma} \dot{s}_{ii}^{(k)}$ soient minima, à commencer par $i = 1$ jusqu'à $i = n$.

D'une façon générale, considérons une matrice hermitienne $\mathfrak{H} = (h_{ij})$ et transformons-la par la matrice $\mathfrak{X}$ de même degré n que $\mathfrak{H}$. Soient $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ les colonnes de $\mathfrak{X} = (\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$. La transformée $\mathfrak{T}$ de $\mathfrak{H}$ par $\mathfrak{X}$ est $\mathfrak{T} = \mathfrak{X}' \mathfrak{H} \overline{\mathfrak{X}} = \mathfrak{H}[\mathfrak{X}]$; les éléments t_{ij} de $\mathfrak{T}$ se calculent par les formules

$$t_{ij} = \mathfrak{x}_i' \mathfrak{H} \bar{\mathfrak{x}}_j .$$

En particulier les éléments diagonaux de $\mathfrak{T}$ sont

$$t_{ii} = \mathfrak{x}_i' \mathfrak{H} \bar{\mathfrak{x}}_i = \mathfrak{H}[\mathfrak{x}_i] .$$

Reprenons notre système S et appliquons ce qui précède en prenant $\mathfrak{H} = \mathfrak{S}^{(k)}$, $\mathfrak{X} = \mathfrak{A}^{(k)}$. Le système $\dot{S}$ transformé de S par $\mathfrak{A}$ est formé par les matrices $\dot{\mathfrak{S}}^{(k)} = \mathfrak{S}^{(k)}[\mathfrak{A}^{(k)}]$. Si $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ sont les colonnes de $\mathfrak{A} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, les éléments diagonaux des $\dot{\mathfrak{S}}^{(k)}$ sont $\dot{s}_{ii}^{(k)} = \mathfrak{S}^{(k)}[\mathfrak{a}_i^{(k)}]$. Les quantités à rendre minima sont par conséquent $\tau(\mathfrak{S}[\mathfrak{a}_i])$, $i = 1, \ldots, n$.

Nous commençons donc par déterminer un vecteur entier $\mathfrak{a}_1 \neq 0$ de K tel que l'on ait

$$\tau(\mathfrak{S}[\mathfrak{a}_1]) \leqslant \tau(\mathfrak{S}[\mathfrak{x}])$$

pour tout $\mathfrak{x}$ entier de K et $\neq 0$. Un tel vecteur $\mathfrak{a}_1$ existe certainement, en vertu du lemme précédent. Car si $\mathfrak{x}_0$ est un vecteur entier non nul arbitrairement choisi, on a

$$\tau(\mathfrak{S}[\mathfrak{x}]) \leqslant \tau(\mathfrak{S}[\mathfrak{x}_0])$$

pour un nombre fini seulement de $\mathfrak{x}$, et parmi ces $\mathfrak{x}$ en nombre fini, il y en a un ou plusieurs qui rendent $\tau(\mathfrak{S}[\mathfrak{x}])$ minimum, et qui peuvent être pris pour vecteur $\mathfrak{a}_1$. On a là un moyen permettant de déterminer effectivement le vecteur $\mathfrak{a}_1$. Ce vecteur $\mathfrak{a}_1$ n'est pas unique, par exemple $\omega \mathfrak{a}_1$ convient également, ω étant une racine de l'unité de K. Parmi tous les vecteurs $\mathfrak{a}_1$ convenables, en nombre fini, prenons en un arbitrairement.

Puis déterminons d'une façon analogue un vecteur $\mathfrak{a}_2$ entier de K, linéairement indépendant de $\mathfrak{a}_1$: rang $(\mathfrak{a}_1, \mathfrak{a}_2) = 2$, et tel que l'on ait

$$\tau(\mathfrak{S}[\mathfrak{a}_2]) \leqslant \tau(\mathfrak{S}[\mathfrak{x}])$$

pour tout $\mathfrak{x}$ entier de K et linéairement indépendant de $\mathfrak{a}_1$: rang $(\mathfrak{a}_1, \mathfrak{x}) = 2$. Comme tout à l'heure, on voit que $\mathfrak{a}_2$ existe. Il n'est pas non plus déterminé d'une façon unique; dans tous les cas $\omega\mathfrak{a}_2$ convient également. Ici on ne choisira pas $\mathfrak{a}_2$ au hasard parmi ses déterminations possibles, bien au contraire. Voici comment se fait le choix de $\mathfrak{a}_2$:

1er cas.

$g_1 > 0$. Les seuls ω sont ± 1, on peut donc choisir entre $\pm \mathfrak{a}_2$. On détermine le signe de sorte que:

$$\mathfrak{a}_1'^{(1)}\, \mathfrak{S}^{(1)}\, \bar{\mathfrak{a}}_2^{(1)} \geqslant 0 \ .$$

2me cas.

$g_1 = 0$. Il se peut que $w > 2$. Considérons la quantité

$$\dot{s}_{12}^{(1)} = \mathfrak{a}_1'^{(1)}\, \mathfrak{S}^{(1)} \bar{\mathfrak{a}}_2^{(1)} \ .$$

Si l'on remplace $\mathfrak{a}_2$ par $\omega\mathfrak{a}_2$, cette quantité $\dot{s}_{12}^{(1)}$ devient $\bar{\omega}^{(1)}\, \dot{s}_{12}^{(1)}$. Or, un nombre complexe $s \neq 0$ étant donné, il existe une racine de l'unité ω de K et une seule telle que

$$-\frac{\pi}{w} < \arg\ \omega s \leqslant \frac{\pi}{w} \ .$$

Le secteur $-\frac{\pi}{w} < \arg\ s \leqslant \frac{\pi}{w}$ du plan des s complexes est un domaine fondamental relativement à la multiplication des s par les racines de l'unité ω de K. Si $s = 0$, on peut prendre ω arbitraire, il y a w possibilités. On peut donc choisir le vecteur $\mathfrak{a}_2$ de façon que

$$-\frac{\pi}{w} < \arg\ \dot{s}_{12}^{(1)} \leqslant \frac{\pi}{w} \ .$$

Pour des raisons qui seront claires par la suite, nous nous contenterons de

$$-\frac{\pi}{w} \leqslant \arg\ \dot{s}_{12}^{(1)} \leqslant \frac{\pi}{w} \ ,$$

ce qui donnera lieu, dans certains cas, à une ambiguité pour le choix de $\mathfrak{a}_2$.

Si $w = 2$, les seuls ω sont ± 1, et la condition précédente s'écrit:

$$-\frac{\pi}{2} \leqslant \arg \dot{s}_{12}^{(1)} \leqslant \frac{\pi}{2}$$

ou aussi $\Re s_{12}^{(1)} \geqslant 0$, ce qui montre que l'on peut faire rentrer le 1er cas dans le 2me.

Le vecteur $\mathfrak{a}_2$ étant ainsi fixé, on détermine $\mathfrak{a}_3$ par les trois conditions:

$$\operatorname{rang}\,(\mathfrak{a}_1,\ \mathfrak{a}_2,\ \mathfrak{a}_3) = 3\,,$$

$$\tau(\mathfrak{S}[\mathfrak{a}_3]) \leqslant \tau(\mathfrak{S}[\mathfrak{x}])$$

pour tout $\mathfrak{x}$ tel que $\operatorname{rang}\,(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{x}) = 3$,
et

$$-\frac{\pi}{w} \leqslant \arg\ \mathfrak{a}_1'^{(1)}\, \mathfrak{S}^{(1)}\, \bar{\mathfrak{a}}_3^{(1)} \leqslant \frac{\pi}{w}\ .$$

Il est inutile de distinguer les cas $g_1 > 0$ et $g_1 = 0$; cela n'a été fait précédemment que pour plus de clarté.

On continue de la sorte. D'une façon générale, $\mathfrak{a}_1, \ldots, \mathfrak{a}_{l-1}$ étant fixés, on détermine $\mathfrak{a}_l$ par les trois conditions:

$$\operatorname{rang}\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_l) = l\ ; \tag{1}$$

$$\tau(\mathfrak{S}[\mathfrak{a}_l]) \leqslant \tau(\mathfrak{S}[\mathfrak{x}]) \text{ pour tout } \mathfrak{x} \text{ tel que } \operatorname{rang}\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_{l-1}, \mathfrak{x}) = l\ ; \tag{2}$$

$$-\frac{\pi}{w} \leqslant \arg\ \mathfrak{a}'^{(1)}_1\, \mathfrak{S}^{(1)}\, \bar{\mathfrak{a}}_l^{(1)} \leqslant \frac{\pi}{w} \text{ si } l \geqslant 2\ ; \tag{3}$$

cela pour $l = 1, 2, \ldots, n$.

Les n vecteurs $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ainsi obtenus forment une matrice $\mathfrak{A} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ entière dans K de déterminant $|\mathfrak{A}| \neq 0$. On l'appellera la *matrixe auxiliaire du système S.*

On transforme alors chacune des matrices $\mathfrak{S}^{(k)}$ par la $k^{\text{ième}}$ conjuguée $\mathfrak{A}^{(k)}$ de $\mathfrak{A}$. Les matrices obtenues par cette première transformation seront désignées par $\dot{\mathfrak{S}}^{(k)}$. Elle sont donc définies par:

$$\dot{\mathfrak{S}}^{(k)} = \mathfrak{S}^{(k)}[\mathfrak{A}^{(k)}] \qquad k = 1, \ldots, \gamma\,.$$

Elles forment un nouveau système $\dot{S}$. En introduisant conformément aux conventions du § 2 la matrice

$$A = \begin{pmatrix} \mathfrak{A}^{(1)} & & 0 \\ & \ddots & \\ 0 & & \mathfrak{A}^{(\gamma)} \end{pmatrix}$$

on aura

$$\dot{S} = S[A] .$$

Cherchons les inégalités que vérifient les $\dot{\mathfrak{S}}^{(k)}$. Pour les $\mathfrak{S}^{(k)}$, on a:

$$\tau(\mathfrak{S}[\mathfrak{a}_l]) \leqslant \tau(\mathfrak{S}[\mathfrak{x}]) \qquad \text{(I)}$$

pour tout $\mathfrak{x}$ entier dans K tel que

$$\text{rang } (\mathfrak{a}_1, \ldots, \mathfrak{a}_{l-1}, \mathfrak{x}) = l \qquad l = 1, 2, \ldots, n .$$

$$-\frac{\pi}{w} \leqslant \arg \mathfrak{a}_1'^{(1)} \mathfrak{S}^{(1)} \bar{\mathfrak{a}}_l^{(1)} \leqslant \frac{\pi}{w} \qquad l = 2, \ldots, n . \qquad \text{(II)}$$

D'après la manière dont les formes quadratiques se transforment, ces relations s'écrivent d'une facon très simple au moyen des $\dot{\mathfrak{S}}^{(k)} = (\dot{s}_{ij}^{(k)})$. On a en effet

$$\dot{s}_{ll}^{(k)} = \mathfrak{S}^{(k)}[\mathfrak{a}_l^{(k)}] .$$

Donc

$$\tau(\mathfrak{S}[\mathfrak{a}_l]) = \tau(\dot{s}_l) .$$

(Pour alléger l'écriture, on contracte deux indices égaux en un seul.)

Soit $\mathfrak{A}^{-1}\mathfrak{x} = \mathfrak{y}$. Le vecteur $\mathfrak{y}$ n'est pas nécessairement entier, mais il est caractérisé par la condition que $\mathfrak{A}\mathfrak{y}$ soit entier. On a

$$\mathfrak{S}[\mathfrak{x}] = \mathfrak{S}[\mathfrak{A}\mathfrak{y}] = \dot{\mathfrak{S}}[\mathfrak{y}] .$$

La condition rang $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{l-1}, \mathfrak{x}) = l$ s'écrit, en multipliant à gauche par $\mathfrak{A}^{-1}$, ce qui conserve le rang:

$$\text{rang} \begin{pmatrix} \mathfrak{E}_{l-1,\,\mathfrak{y}} \\ 0 \end{pmatrix} = l .$$

Cela signifie que le vecteur $\mathfrak{y}$ doit avoir ses dernières composantes à partir de la $l^{\text{ième}}$ non toutes nulles:

Soit $\mathfrak{y} = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}$, on aura $(\eta_l, \ldots, \eta_n) \neq 0$.

Les conditions (I) et (II) deviennent ainsi:

$$\tau(\dot{s}_l) \leqslant \tau(\dot{\mathfrak{S}}[\mathfrak{y}]) \tag{I}$$

pour tout $\mathfrak{y}$ de K tel que $\mathfrak{A}\mathfrak{y} = \text{entier}$, $(\eta_l, \ldots, \eta_n) \neq 0$;

$l = 1, \ldots, n$.

$$-\frac{\pi}{w} \leqslant \arg \dot{s}_{1l}^{(1)} \leqslant \frac{\pi}{w} \; ; \tag{II}$$

$l = 2, \ldots, n$.

§ 4. La matrice auxiliaire

Si la matrice auxiliaire $\mathfrak{A}$ du système S était unimodulaire, c'est-à-dire si $|\mathfrak{A}| = \varepsilon =$ unité de K, les 2 systèmes $\dot{S}$ et S seraient équivalents. Mais ce n'est pas nécessairement le cas. Nous allons voir néanmoins que pour tous les systèmes S, la norme du déterminant de $\mathfrak{A}$ est bornée. C'est ce qui fait l'objet du

Théorème 1. La norme du déterminant de la matrice auxiliaire $\mathfrak{A}$ est bornée: $|N(|\mathfrak{A}|)| \leqslant c$, c étant une constante ne dépendant pas de S, mais seulement de n et de K, $c = c(n, K)$.

La démonstration repose sur un théorème connu de Minkowski relatif aux formes linéaires, théorème que l'on peut énoncer ainsi:

Soient $\mathfrak{C}$ une matrice donnée de degré r, de déterminant $|\mathfrak{C}| \neq 0$, dont les lignes complexes sont 2 à 2 conjuguées, et $z = \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}$ une colonne de variables indépendantes. Il existe alors de valeurs entières rationnelles non toutes nulles de $z_1, \ldots, z_r$ telles que:

$$|\mathfrak{C}\mathfrak{z}| \leqslant \sqrt[r]{||\mathfrak{C}||} \; .$$

On va en déduire le théorème:

Soient $\mathfrak{B}_1, \ldots, \mathfrak{B}_g$ g matrices non dégénérées de degré n, les g_1 premières étant réelles, les $2\,g_2$ suivantes complexes, telles que $\mathfrak{B}_{g_1+g_2+k} = \overline{\mathfrak{B}}_{g_1+k}$ pour $k = 1, \ldots, g_2$, et soit B la valeur absolue du produit de leurs déterminants. K étant un corps algébrique de degré g, ayant g_1 conjugués réels et $2\,g_2$ imaginaires, il existe un vecteur entier $\mathfrak{x}$ non nul du corps K, tel que l'on ait pour tous les conjugués $\mathfrak{x}^{(k)}$ de $\mathfrak{x}$:

$$| \mathfrak{B}_k \mathfrak{x}^{(k)} | \leqslant \sqrt[gn]{B} \cdot \sqrt[2g]{D} .$$

$D = |d|$ est la valeur absolue du discriminant du corps K.

Pour cela, soit $(\omega_1, \ldots, \omega_g)$ une base des entiers de K. Une colonne d'entiers du corps K est donnée par

$$\mathfrak{x} = \omega_1 \mathfrak{v}_1 + \cdots + \omega_g \mathfrak{v}_g ,$$

les colonnes $\mathfrak{v}_i = \begin{pmatrix} v_{i1} \\ \vdots \\ v_{in} \end{pmatrix}$ étant entières rationnelles. Nous numérotons les conjugués de K comme il a été indiqué au début du § 1.

Appliquons le théorème de Minkowski rappelé tout à l'heure en prenant:

$$\mathfrak{C} = \begin{pmatrix} \omega_1^{(1)} \mathfrak{B}_1 & \omega_2^{(1)} \mathfrak{B}_1 \ldots \omega_g^{(1)} \mathfrak{B}_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \omega_1^{(g)} \mathfrak{B}_g & \omega_2^{(g)} \mathfrak{B}_g \ldots \omega_g^{(g)} \mathfrak{B}_g \end{pmatrix} =$$

$$= \begin{pmatrix} \mathfrak{B}_1 & 0 \\ & \ddots \\ 0 & \mathfrak{B}_g \end{pmatrix} \cdot (\Omega \times \mathfrak{E}_n)$$

où Ω est la matrice $\Omega = (\omega_k^{(i)})$, i étant l'indice de ligne, k l'indice de colonne, et où $\Omega \times \mathfrak{E}_n$ désigne le produit de Kronecker:

$$\Omega \times \mathfrak{E}_n = (\omega_k^{(i)} \mathfrak{E}_n) .$$

Il est clair que $\mathfrak{C}$ satisfait aux conditions du théorème: les $g_1 n$ premières lignes de $\mathfrak{C}$ sont réelles, et les n lignes $(\omega_1^{(g_1+k)} \mathfrak{B}_{g_1+k}, \ldots, \omega_g^{(g_1+k)} \mathfrak{B}_{g_1+k})$ sont respectivement conjugées complexes des n lignes

$$(\omega_1^{(g_1+g_2+k)} \mathfrak{B}_{g_1+g_2+k}, \ldots, \omega_g^{(g_1+g_2+k)} \mathfrak{B}_{g_1+g_2+k}) .$$

Le déterminant de $\mathfrak{C}$ vaut $|\mathfrak{C}| = |\mathfrak{B}_1| \cdots |\mathfrak{B}_g| \cdot |\Omega|^n$. En valeur absolue il est égal à $||\mathfrak{C}|| = B \cdot \sqrt{D^n} \neq 0$. Il existe donc une colonne entière rationnelle $\mathfrak{w}$ non nulle de gn éléments, que l'on décomposera ainsi:

$$\mathfrak{w} = \begin{pmatrix} \mathfrak{v}_1 \\ \vdots \\ \mathfrak{v}_g \end{pmatrix} \quad \text{avec} \quad \mathfrak{v}_i = \begin{pmatrix} v_{i1} \\ \vdots \\ v_{in} \end{pmatrix}$$

v_{ik} = entiers rationnels et telle que l'on ait:

$$| \mathfrak{C} \mathfrak{w} | \leqslant \sqrt[gn]{|| \mathfrak{C} ||} .$$

Or

$$\mathfrak{C}\,\mathfrak{w} = \begin{pmatrix} \mathfrak{B}_1 & & 0 \\ & \ddots & \\ 0 & & \mathfrak{B}_g \end{pmatrix} \begin{pmatrix} \omega_1^{(1)}\mathfrak{E}_n \dots \omega_g^{(1)}\mathfrak{E}_n \\ \dots\dots\dots\dots \\ \omega_1^{(g)}\mathfrak{E}_n \dots \omega_g^{(g)}\mathfrak{E}_n \end{pmatrix} \begin{pmatrix} \mathfrak{v}_1 \\ \vdots \\ \mathfrak{v}_g \end{pmatrix} =$$

$$= \begin{pmatrix} \mathfrak{B}_1 & & 0 \\ & \ddots & \\ 0 & & \mathfrak{B}_g \end{pmatrix} \begin{pmatrix} \omega_1^{(1)}\mathfrak{v}_1 + \dots + \omega_g^{(1)}\mathfrak{v}_g \\ \dots\dots\dots\dots\dots\dots \\ \omega_1^{(g)}\mathfrak{v}_1 + \dots + \omega_g^{(g)}\mathfrak{v}_g \end{pmatrix} =$$

$$= \begin{pmatrix} \mathfrak{B}_1 & & 0 \\ & \ddots & \\ 0 & & \mathfrak{B}_g \end{pmatrix} \begin{pmatrix} \mathfrak{x}^{(1)} \\ \vdots \\ \mathfrak{x}^{(g)} \end{pmatrix} = \begin{pmatrix} \mathfrak{B}_1\,\mathfrak{x}^{(1)} \\ \vdots \\ \mathfrak{B}_g\,\mathfrak{x}^{(g)} \end{pmatrix} .$$

$\mathfrak{x} = \omega_1\mathfrak{v}_1 + \dots + \omega_g\mathfrak{v}_g \neq 0$ est une colonne d'entiers de K.

On obtient bien le résultat annoncé:

$$|\,\mathfrak{B}_k\mathfrak{x}^{(k)}\,| \leqslant \sqrt[gn]{B}\cdot\sqrt[2g]{D}\,, \quad \mathfrak{x}\neq 0\ . \qquad \text{c.q.f.d.}$$

Appliquons ce théorème en prenant $\mathfrak{B}_k = \mathfrak{A}^{(k)-1}$, les $\mathfrak{A}^{(k)}$ étant les conjuguées de la matrice auxiliaire $\mathfrak{A}$ obtenue lors de la première transformation du système S. Il est clair que ces $\mathfrak{B}_k$ remplissent les conditions énoncées dans l'hypothèse du théorème. La quantité désignée par B vaut $B = \left|N(|\mathfrak{A}|)\right|^{-1}$. Il existe donc un vecteur $\mathfrak{x} \neq 0$ du corps K tel que

$$|\,\mathfrak{A}^{(k)-1}\mathfrak{x}^{(k)}\,| \leqslant \frac{\sqrt[2g]{D}}{\sqrt[gn]{|\,N(|\mathfrak{A}|)\,|}} = G\ .$$

Soit, comme précédemment, $\mathfrak{y} = \mathfrak{A}^{-1}\mathfrak{x}$; on a

$$|\mathfrak{y}^{(k)}| \leqslant G\,; \qquad k = 1, \dots, g\ .$$

$\mathfrak{x}$ n'étant pas nul, $\mathfrak{y} = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}$ ne l'est pas non plus; supposons que $\eta_{l+1} = \dots = \eta_n = 0$, mais que $\eta_l \neq 0$. On applique alors les inégalités (I) de la fin du § 3 à cet $\mathfrak{y}$. Supprimons les points sur les s. On obtient, en tenant compte de $|\mathfrak{y}^{(k)}| \leqslant G$:

$$\tau(s_l) \leqslant \tau(\mathfrak{S}[\mathfrak{y}]) = \sum_{k=1}^{\gamma}\sum_{i,j=1}^{l} s_{ij}^{(k)}\,\eta_i^{(k)}\,\overline{\eta}_j^{(k)} \leqslant G^2 \sum_{k=1}^{\gamma}\sum_{i,j=1}^{l} |\,s_{ij}^{(k)}\,|\ .$$

Or les $\mathfrak{S}^{(k)}$ sont des matrices positives, donc $\mathfrak{S}^{(k)}[\mathfrak{x}] \geqslant 0$ pour toutes valeurs complexes (réelles si $k \leqslant g_1$) des composantes ξ_i du vecteur $\mathfrak{x}$; en particulier pour les valeurs suivantes:

$$\xi_i = 1 \ , \ \xi_j = - e^{i \arg s_{ij}^{(k)}} = - \frac{s_{ij}^{(k)}}{| s_{ij}^{(k)} |} \ , \ i \ , j \text{ fixes} \ ,$$

$$\xi_m = 0 \quad \text{si} \quad m \neq i \ , \ m \neq j \ ,$$

on trouve:

$$2 | s_{ij}^{(k)} | \leqslant s_i^{(k)} + s_j^{(k)} \ . \tag{1}$$

On en déduit:

$$\sum_{i,j=1}^{l} | s_{ij}^{(k)} | \leqslant l \sum_{i=1}^{l} s_i^{(k)} \ . \tag{2}$$

A cause de (2) on obtient alors

$$\tau(s_l) \leqslant G^2 \sum_{k=1}^{\gamma} l \sum_{i=1}^{l} s_i^{(k)} = l G^2 \sum_{i=1}^{l} \tau(s_i) \ .$$

Or les inégalités (I) appliquées à $\mathfrak{y}$ avec

$$\eta_h = 1 \ , \ \eta_i = 0 \qquad \text{si} \qquad i \neq h \ , \ h \geqslant l \ ,$$

donnent:

$$\tau(s_l) \leqslant \tau(s_h) \qquad \text{si} \qquad l \leqslant h \ .$$

On a donc:

$$\tau(s_1) \leqslant \tau(s_2) \leqslant \cdots \leqslant \tau(s_n) \ . \tag{3}$$

inégalités qui seront plus d'une fois appliquées par la suite.

On renforce l'inégalité obtenue en remplaçant $\tau(s_i)$ par $\tau(s_l)$ ce qui donne

$$\tau(s_l) \leqslant l^2 G^2 \tau(s_l) \ .$$

Or $\tau(s_l) > 0$, car les matrices $\mathfrak{S}^{(k)}$ sont positives. Comme $l \leqslant n$, on en déduit:

$$G^{-1} \leqslant n \ .$$

Reprenant la valeur de G qui est $G = D^{\frac{1}{2g}} \cdot \left| N(|\mathfrak{A}|) \right|^{-\frac{1}{gn}}$ on trouve finalement:

$$\left| N(|\mathfrak{A}|) \right| \leqslant D^{\frac{n}{2}} \cdot n^{gn} \ ,$$

ce qui démontre le théorème 1.

Théorème 2. Une matrice $\mathfrak{A}$ de degré n, d'éléments entiers algébriques dans un corps K, de déterminant $|\mathfrak{A}| = \alpha \neq 0$, se met sous la forme $\mathfrak{U}\mathfrak{A}_\nu$, où $\mathfrak{A}_\nu$ appartient à un ensemble fini de matrices entières ne dépendant que de α, n et K, et où $\mathfrak{U}$ est unimodulaire dans K.

La démonstration repose sur un

Lemme. Si deux matrices entières $\mathfrak{A}$, $\mathfrak{A}_1$ *de déterminants associés:* $\varepsilon|\mathfrak{A}| = \varepsilon_1|\mathfrak{A}_1| = \alpha$, *sont congrues mod* (α): $\mathfrak{A} \equiv \mathfrak{A}_1\ ((\alpha))$, *la matrice* $\mathfrak{A}\mathfrak{A}_1^{-1} = \mathfrak{U}$ *est unimodulaire.*

Comme $|\mathfrak{A}\mathfrak{A}_1^{-1}| = \varepsilon_1\,\varepsilon^{-1} =$ unité de K, il suffit pour démontrer ce lemme de faire voir que $\mathfrak{A}\mathfrak{A}_1^{-1}$ a ses éléments entiers. Pour cela multiplions la congruence $\mathfrak{A} \equiv \mathfrak{A}_1((\alpha))$ à droite par $\alpha\mathfrak{A}_1^{-1}$, matrice entière; on trouve ainsi

$$\alpha\mathfrak{A}\mathfrak{A}_1^{-1} \equiv \alpha\mathfrak{E}((\alpha)) \ , \quad \text{d'où} \quad \mathfrak{A}\mathfrak{A}_1^{-1} \equiv \mathfrak{E}((1))$$

c'est-à-dire que $\mathfrak{A}\mathfrak{A}_1^{-1}$ est entière.

Considérons alors un ensemble complet de matrices ayant leurs déterminants associés à α, et incongrues mod (α). Il y en a au plus $N((\alpha))^{n^2}$. Soient $\mathfrak{A}_1, \ldots, \mathfrak{A}_M$ ces matrices. Le nombre M dépend uniquement de α, du corps K et de n.

Soit maintenant $\mathfrak{A}$ une matrice quelconque de déterminant associé à α: $|\mathfrak{A}| = \alpha\varepsilon$. La matrice $\mathfrak{A}$ est nécessairement congrue à l'une des $\mathfrak{A}_\nu$ mod (α):

$$\mathfrak{A} \equiv \mathfrak{A}_\nu((\alpha)) \ .$$

D'après le lemme on a $\mathfrak{A}\mathfrak{A}_\nu^{-1} = \mathfrak{U}$, $\mathfrak{U}$ étant unimodulaire, d'où $\mathfrak{A} = \mathfrak{U}\mathfrak{A}_\nu$. c. q. f. d.

Conséquences et définitions.

Il résulte immédiatement des théorèmes 1 et 2 que *la matrice auxiliaire* $\mathfrak{A}$ *se met sous la forme*

$$\mathfrak{A} = \mathfrak{U}\mathfrak{A}_\nu$$

où $\mathfrak{U}$ *est unimodulaire dans* K *et* $\mathfrak{A}_\nu$ *appartient à un ensemble fini de matrices*

$$\mathfrak{A}_1, \ldots, \mathfrak{A}_N \ .$$

Ces matrices $\mathfrak{A}_\nu$ ne sont pas déterminées d'une façon unique, on peut les multiplier à gauche par des matrices unimodulaires arbitraires. Deux matrices $\mathfrak{A}$ et $\mathfrak{B}$ qui diffèrent à gauche par un facteur unimodulaire $\mathfrak{U}$, c'est-à-dire telles que $\mathfrak{A} = \mathfrak{U}\mathfrak{B}$, sont dites *associées à gauche.* La relation d'associativité à gauche est réflexive, symétrique, transitive; on peut donc parler des *classes de matrices associées à gauche.* Et les résultats obtenus au sujet de la matrice $\mathfrak{A}$ peuvent se résumer ainsi: *Il existe un*

nombre fini seulement N de classes d'associées à gauche possibles pour la matrice auxiliaire $\mathfrak{A}$, *quel que soit le système S dont on est parti.* Ces classes sont représentées par les matrices $\mathfrak{A}_1, \ldots, \mathfrak{A}_N$.

Désignons par $R(\mathfrak{A})$ le domaine de l'espace des $s_{ij}^{(k)}$ défini par les inégalités (I) et (II) du § 3 (les points sur les s étant supprimés), et soit R_0 le domaine $R_0 = R(\mathfrak{E})$. On voit aisément que le domaine $R(\mathfrak{A})$ est contenu dans R_0 quelle que soit la matrice $\mathfrak{A}$ entière de K et non dégénérée:

$$R(\mathfrak{A}) \text{ dans } R_0 .$$

$R(\mathfrak{A})$ est *convexe*, car si les systèmes S et T vérifient (I) et (II), il en est de même du système $\lambda S + \mu T$ avec $\lambda + \mu = 1$, $\lambda \geqslant 0$, $\mu \geqslant 0$.

$R(\mathfrak{A})$ est un domaine *fermé*, ce qui provient du fait qu'il est défini par des inégalités où se trouve toujours le signe $\leqslant$.

$R(\mathfrak{A})$ ne dépend que de la classe d'associées à gauche de la matrice $\mathfrak{A}$:

$R(\mathfrak{A}) = R(\mathfrak{U}\mathfrak{A})$ si $\mathfrak{U}$ est unimodulaire, car dans les inégalités (I) les $\mathfrak{y}$ pour lesquels $\mathfrak{A}\mathfrak{y}$ est entier sont les mêmes que les $\mathfrak{y}$ pour lesquels $\mathfrak{U}\mathfrak{A}\mathfrak{y}$ est entier.

Remarquons encore que les inégalités (I) et (II) sont *linéaires et homogènes* en les coordonnées de S, c'est-à-dire en les quantités $Rs_{ij}^{(k)}$ et $Js_{ij}^{(k)}$. Cela est clair pour (I). Quant aux inégalités (II), on peut les écrire sous la forme

$$Rs_{1l}^{(1)} \geqslant 0 \quad \text{et} \quad \pm Js_{1l}^{(1)} \leqslant \operatorname{tg} \frac{\pi}{w} Rs_{1l}^{(1)} \quad l = 2, \ldots, n , \qquad (\text{II}')$$

forme qui met en évidence leur linéarité.

Il s'ensuit que le domaine $R(\mathfrak{A})$ est limité par des hyperplans passant par l'origine des coordonnées. Les inégalités (I) étant en nombre infini, on pourrait s'attendre à ce que ces hyperplans soient aussi en nombre infini. Nous verrons cependant plus loin qu'il n'en est pas ainsi, c'est-à-dire que toutes les inégalités (I) découlent d'un nombre *fini* d'entre elles.

§ 5. Deuxième transformation. Le domaine réduit R

Le système $\dot{S}$, obtenu à partir de S par transformation avec la matrice auxiliaire $\mathfrak{A}$, n'est équivalent à S que si $\mathfrak{A}$ est unimodulaire, ce qui n'a en général pas lieu. Mais on sait que

$$\mathfrak{A} = \mathfrak{U}\mathfrak{A}_\nu .$$

Considérons alors le système $\ddot{S}$ transformé de $\dot{S}$ par $\mathfrak{A}_\nu^{-1}$, c'est-à-dire le système des matrices

$$\ddot{\mathfrak{S}}^{(k)} = \dot{\mathfrak{S}}^{(k)}[\mathfrak{A}_\nu^{(k)-1}] = \mathfrak{S}^{(k)}[\mathfrak{U}^{(k)}] \qquad k = 1, \ldots, \gamma .$$

Ce système $\ddot{S}$ est équivalent au système primitif S. On l'appellera *le système réduit de* S. Pour un S donné, $\ddot{S}$ dépend de la manière dont les $\mathfrak{A}_1, \ldots, \mathfrak{A}_N$ ont été choisies dans leur classes d'associées.

Les coordonnées de $\ddot{S}$ vérifient une infinité d'inégalités que l'on obtient en remplaçant $\dot{\mathfrak{S}}^{(k)}$ par $\ddot{\mathfrak{S}}^{(k)}[\mathfrak{A}_\nu^{(k)}]$ dans (I) et (II). Il est inutile de les écrire; elles sont, d'après la remarque faite à la fin du § précédent, linéaires et homogènes en les parties réelles et imaginaires des $\ddot{s}_{ij}^{(k)}$. Pour chaque $\mathfrak{A}_\nu$ on obtient ainsi un domaine que nous désignerons par R_ν, et qui sera le $\nu^{\text{ième}}$ domaine réduit, relatif à la matrice $\mathfrak{A}_\nu$, défini comme le lieu des systèmes de matrices $\ddot{\mathfrak{S}}^{(k)} = \dot{\mathfrak{S}}^{(k)}[\mathfrak{A}_\nu^{(k)-1}]$ lorsque le système des $\dot{\mathfrak{S}}^{(k)}$ parcourt tout le domaine $R(\mathfrak{A}_\nu)$.

Comme on l'a vu à la fin du § 4, $R(\mathfrak{A}_\nu)$ ne dépend pas des représentantes choisies pour les $\mathfrak{A}_\nu$; mais R_ν en dépend, à une équivalence près. De même que $R(\mathfrak{A}_\nu)$, R_ν *est convexe, fermé, limité par des hyperplans.*

Soit P l'espace des systèmes S. Comme il est facile de le voir, P est un domaine ouvert dans l'espace cartésien dont les coordonnées sont les parties réelles et imaginaires des $s_{ij}^{(k)}$.

Désignons par R la portion située dans P de la réunion des domaines R_ν: $R = P \frown \sum_{\nu=1}^{N} R_\nu$ (le signe $\frown$ signifie intersection). R est par définition *le domaine réduit des systèmes* S.

Théorème 3. Le domaine R précédemment défini constitue un domaine fondamental pour les systèmes S relativement aux transformations unimodulaires dans K.

Il s'agit de démontrer 2 choses:

1° *A tout système S de matrices positives $\mathfrak{S}^{(k)}$ correspond un système S_1 équivalent dans R:*

$$S_1 \sim S \quad , \qquad S_1 \quad \text{dans} \quad R \, .$$

C'est évident par définition de R. Reprenons la notation abrégée introduite au § 2. En transformant le système S par sa matrice auxiliaire $\mathfrak{A}$, on obtient le système $\dot{S}$ défini par $\dot{S} = S[A]$. On sait que la matrice $\mathfrak{A}$ se met sous la forme $\mathfrak{A} = \mathfrak{U}\mathfrak{A}_\nu$, $\mathfrak{U}$ unimodulaire dans K. Alors $\ddot{S} = \dot{S}[A_\nu^{-1}] = S[U]$ est le système réduit équivalent à S; $\ddot{S}$ est dans R_ν puisque S est dans $R(\mathfrak{A}_\nu)$. Donc $\ddot{S}$ est bien situé dans R.

2° *Deux systèmes S et T de R ne peuvent être équivalents que s'ils sont situés sur la frontière de R.*

Soient S et T deux systèmes réduits et équivalents:

$$S \text{ et } T \text{ dans } R;\ S = T[U]\ ; \qquad \mathfrak{U} \neq \omega\mathfrak{E}\ .$$

On a pour certains indices μ et ν:

$$S = \dot{S}[A_\mu^{-1}] \qquad \dot{S} \text{ dans } R(\mathfrak{A}_\mu)$$

$$T = \dot{T}[A_\nu^{-1}] \qquad \dot{T} \text{ dans } R(\mathfrak{A}_\nu)$$

Par conséquent $\dot{S} = \dot{T}[A_\nu^{-1} U A_\mu] = \dot{T}[V]$ avec $V = A_\nu^{-1} U A_\mu$. Les matrices $\mathfrak{A}_\nu\mathfrak{V} = \mathfrak{U}\mathfrak{A}_\mu$ et $\mathfrak{A}_\mu\mathfrak{V}^{-1} = \mathfrak{U}^{-1}\mathfrak{A}_\nu$ sont entières dans K. Montrons que $\dot{S}$ et $\dot{T}$ sont sur la frontière des domaines respectifs $R(\mathfrak{A}_\mu)$ et $R(\mathfrak{A}_\nu)$; alors S et T seront évidemment systèmes frontières de R_μ et R_ν, puisque le passage de $R(\mathfrak{A}_\nu)$ à R_ν se fait par la transformation $\dot{\mathfrak{S}} = \mathfrak{S}[\mathfrak{A}_\nu]$ qui est topologique. Distinguons 2 cas, selon que $\mathfrak{V}$ est diagonale ou non.

1er cas. $\mathfrak{V}$ *est diagonale:* $\mathfrak{V} = \mathfrak{D}\ (v_1, \ldots, v_n)$.

Alors $\mathfrak{V} \neq \omega\mathfrak{E}$, car $\mathfrak{U} \neq \omega\mathfrak{E}$ et $\mathfrak{A}_\nu\mathfrak{V} = \mathfrak{U}\mathfrak{A}_\mu$. Les éléments de $\dot{\mathfrak{S}}^{(k)} = (\dot{s}_{ij}^{(k)})$ et de $\dot{\mathfrak{T}}^{(k)} = (\dot{t}_{ij}^{(k)})$ sont liés par les relations $\dot{\mathfrak{S}}^{(k)} = \dot{\mathfrak{T}}^{(k)}[\mathfrak{V}^{(k)}]$, c.-à-d.: $\dot{s}_{ij}^{(k)} = \dot{t}_{ij}^{(k)}\, v_i^{(k)}\, \bar{v}_j^{(k)}$. Considérons les colonnes $\mathfrak{v}_i = \begin{pmatrix} 0 \\ v_i \\ 0 \end{pmatrix}$ de $\mathfrak{V} = (\mathfrak{v}_1, \ldots, \mathfrak{v}_n)$. Comme $\mathfrak{A}_\nu\mathfrak{V}$ est entière, la colonne $\mathfrak{A}_\nu\mathfrak{v}_i$ est entière, et l'on peut appliquer (I) aux matrices $\dot{\mathfrak{T}}^{(k)}$ avec $\mathfrak{y} = \mathfrak{v}_i$, $l = i$:

$$\tau(\dot{s}_i) = \tau(\dot{\mathfrak{T}}[\mathfrak{v}_i]) \geqslant \tau(t_i)\ .$$

La matrice $\mathfrak{A}_\mu\mathfrak{V}^{-1}$ est aussi entière; si $\mathfrak{V}^{-1} = (\mathfrak{v}_1^*, \ldots, \mathfrak{v}_n^*)$, la colonne $\mathfrak{A}_\mu\mathfrak{v}_i^*$ est entière, et l'on peut appliquer (I) à $\dot{S}$ avec $\mathfrak{y} = \mathfrak{v}_i^*$, $l = i$:

$$\tau(\dot{t}_i) = \tau(\dot{\mathfrak{S}}[\mathfrak{v}_i^*]) \geqslant \tau(\dot{s}_i)\ .$$

On voit donc que $\tau(\dot{s}_i) = \tau(\dot{t}_i)$, et le système $\dot{T}$ vérifie la relation

$$\tau(\dot{\mathfrak{T}}[\mathfrak{v}_i]) = \tau(\dot{t}_i)\ .$$

Si tous les v_i, $i = 1, \ldots, n$, ne sont pas des racines de l'unité, soit $v_l \neq \omega$, on en déduit que $\dot{T}$ est bien sur la frontière de $R(\mathfrak{A})$ puisque $\dot{T}$ est dans $R(\mathfrak{A})$ et vérifie:

$$\tau(\dot{\mathfrak{T}}[\mathfrak{v}_l]) = \tau(\dot{t}_l)$$

relation non identiquement satisfaite, car $v_l \neq \omega$, obtenue en prenant le signe $=$ dans l'une des inégalités définissant $R(\mathfrak{A}_\nu)$. Il en est de même de $\dot{S}$.

Si tous les v_i sont des racines de l'unité, ils ne peuvent être tous égaux. Soit donc $v_i = \omega_i$; il existe un l pour lequel $\omega_1 \neq \omega_l$. Alors $\dot{\mathfrak{T}}^{(k)}[\mathfrak{V}^{(k)}] = \dot{\mathfrak{S}}^{(k)}$ montre que:

$$\dot{s}_{1l}^{(k)} = \dot{t}_{1l}^{(k)}\, \omega_1^{(k)}\, \overline{\omega}_l^{(k)} \ , \quad \omega_1 \overline{\omega}_l = \omega \neq 1 \ .$$

En particulier pour l'indice supérieur $k = 1$ on a

$$\dot{s}_{1l}^{(1)} = \dot{t}_{1l}^{(1)}\, \omega^{(1)} \ , \quad \omega^{(1)} \neq 1 \ , \quad \omega^w = 1 \ .$$

On peut supposer $\dot{s}_{1l}^{(1)} \neq 0$, car si $\dot{s}_{1l}^{(1)} = 0$ il est clair d'après (II′) (§ 4) que $\dot{S}$ et $\dot{T}$ sont frontières.

$\dot{S}$ et $\dot{T}$ sont dans $R(\mathfrak{A}_u)$ et $R(\mathfrak{A}_\nu)$, donc d'après (II):

$$\begin{aligned} -\frac{\pi}{w} &\leqslant \arg\, \dot{s}_{1l}^{(1)} \leqslant \frac{\pi}{w} \\ -\frac{\pi}{w} &\leqslant \arg\, \dot{t}_{1l}^{(1)} \leqslant \frac{\pi}{w} \ . \end{aligned} \tag{II}$$

En faisant la différence:

$$-\frac{2\pi}{w} \leqslant \arg\, \frac{\dot{s}_{1l}^{(1)}}{\dot{t}_{1l}^{(1)}} \leqslant \frac{2\pi}{w}$$

c'est-à-dire

$$-\frac{2\pi}{w} \leqslant \arg\, \omega^{(1)} \leqslant \frac{2\pi}{w} \ .$$

Cette inégalité entraîne, puisque $\omega^{(1)} = e^{\frac{2\pi m i}{w}} \neq 1$, $\arg \omega^{(1)} = \pm \frac{2\pi}{w}$.

Cela n'est possible que si

$$\begin{cases} \arg\ \dot{s}_{1l}^{(1)} = \ \ \frac{\pi}{w} \\ \arg\ \dot{t}_{1l}^{(1)} = -\frac{\pi}{w} \end{cases} \quad \text{ou bien si} \quad \begin{cases} \arg\ \dot{s}_{1l}^{(1)} = -\frac{\pi}{w} \\ \arg\ \dot{t}_{1l}^{(1)} = \ \ \frac{\pi}{w} \end{cases}$$

Ce qui montre que $\dot{S}$ et $\dot{T}$ sont systèmes frontières de $R(\mathfrak{A}_\mu)$ et $R(\mathfrak{A}_\nu)$ respectivement.

2ème cas. $\mathfrak{V}$ *n'est pas diagonale.*

Soit de nouveau $\mathfrak{V} = (\mathfrak{v}_1, \ldots, \mathfrak{v}_n)$, et soit $\mathfrak{v}_l$ la première colonne différente d'une colonne de matrice diagonale; alors, si $\mathfrak{v}_l = \begin{pmatrix} v_{l1} \\ \vdots \\ v_{ln} \end{pmatrix}$, on a nécessairement $(v_{l1}, \ldots, v_{ln}) \neq 0$, puisque $|\mathfrak{V}| \neq 0$.

$\mathfrak{V}^{-1}$ a la même forme que $\mathfrak{V}$, sa l^e colonne est $\mathfrak{v}_l^* = \begin{pmatrix} v_{l1}^* \\ \vdots \\ v_{ln}^* \end{pmatrix}$ avec $(v_{l1}^*, \ldots, v_{ln}^*) \neq 0$. Comme $\mathfrak{A}_\nu \mathfrak{v}_l$ est entière, on peut appliquer (I) à $\dot{T}$ pour le vecteur $\mathfrak{v}_l$, et l'on trouve:

$$\tau(\dot{s}_l) = \tau(\mathfrak{T}[\mathfrak{v}_l]) \geqslant \tau(\dot{t}_l) .$$

De même, en appliquant (I) à $\dot{S}$ pour $\mathfrak{v}_l^*$, on trouve:

$$\tau(\dot{t}_l) = \tau(\mathfrak{S}[\mathfrak{v}_l^*]) \geqslant \tau(\dot{s}_l) .$$

On en déduit $\tau(\dot{t}_l) = \tau(\dot{s}_l)$, et l'on voit comme précédemment que $\dot{S}$ et T sont frontières de $R(\mathfrak{A}_\mu)$ et $R(\mathfrak{A}_\nu)$, étant respectivement dans ces domaines et vérifiant les égalités non identiques

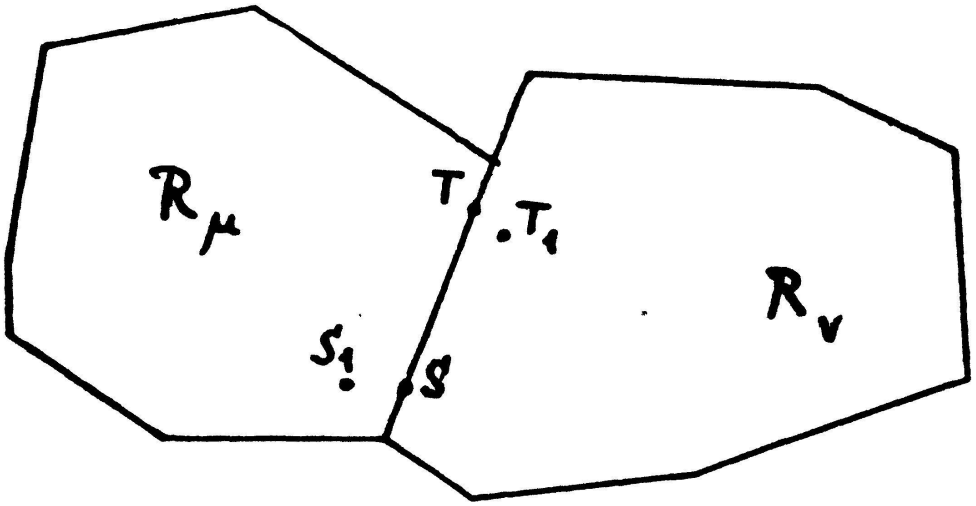
$$\tau(\dot{s}_l) = \tau(\dot{\mathfrak{S}}[\mathfrak{v}_l^*]) \quad \text{et} \quad \tau(\dot{t}_l) = \tau(\dot{\mathfrak{T}}[\mathfrak{v}_l]) .$$

En résumé, les systèmes $\dot{S}$ et $\dot{T}$ sont frontières de $R(\mathfrak{A}_\mu)$ et de $R(\mathfrak{A}_\nu)$, si les systèmes $S = \dot{S}[A_\mu^{-1}]$ et $T = \dot{T}[A_\nu^{-1}]$ sont équivalents. Il s'ensuit que S et T *sont frontières de* R_μ *et* R_ν *respectivement.* Pour en déduire que S et T sont frontières de R, il faudrait être sûr que R_μ et R_ν n'aient pas de région commune. Or il est aisé de voir que *si un système* S *appartient à la fois à* R_μ *et à* R_ν, *il est frontière de ces 2 domaines*; en effet soit $\mathfrak{U}$ une substitution unimodulaire transformant S en un système T différent de S: $T = S[U] \neq S$. S appartient à R_μ et T appartient au domaine R_ν^* transformé de R_ν par $\mathfrak{U}$. Ce domaine R_ν^* peut remplacer R_ν; on l'obtient comme R_ν en partant de $R(\mathfrak{A}_\nu)$, mais en transformant ce dernier domaine par $\mathfrak{A}_\nu^{-1}\mathfrak{U}$ au lieu de $\mathfrak{A}_\nu^{-1}$; cela revient à prendre $\mathfrak{U}^{-1}\mathfrak{A}_\nu$ au lieu de $\mathfrak{A}_\nu$ comme représentante de la classe gauche d'associées de $\mathfrak{A}_\nu$.

Le résultat obtenu, à savoir que S et T sont respectivement frontières de R_μ et R_ν s'ils sont équivalents, est valable quels que soient les représentants $\mathfrak{A}_\mu$ et $\mathfrak{A}_\nu$ choisies dans leurs classes d'associées, on peut donc appliquer ce résultat aux systèmes S et $T = S[U]$ équivalents, l'un S situé dans R_μ, l'autre T dans R_ν^*. Il en résulte que les systèmes S et T sont frontières, l'un de R_μ, l'autre de R_ν^*, et notre assertion est démontrée.

D'après cela la région commune à R_μ et à R_ν ne peut être qu'une portion de la frontière d'un de ces domaines.

Pour achever la démonstration du théorème 3, il reste à faire voir que les deux systèmes S et T ne peuvent se trouver sur une portion de frontière commune à R_μ et R_ν, comme le montre schématiquement la figure. En effet, supposons par absurde qu'il en soit ainsi. Considérons un système S_1 voisin de S, *à l'intérieur de* R_μ. La transformation $T = S[U]$ étant topologique, S_1 est transformé par $\mathfrak{U}$ en un système T_1 voisin de T.



Si S_1 est suffisamment près de S, T_1 sera soit dans R_μ, soit dans R_ν. Or cela est impossible, car il a été démontré que deux systèmes S_1 et T_1 situés tous deux dans R et équivalents, sont *frontières*, l'un de $R_{\mu'}$, l'autre de $R_{\nu'}$.

Il s'agit maintenant de déterminer la nature du domaine R, intersection de P avec la réunion des R_ν. Notre but est de montrer que chacun des domaines R_ν est limité par un nombre *fini* d'hyperplans. C'est la démonstration de ce fait qui présente le plus de difficultés.

§ 6. Théorème préliminaire

Dans le cas où la matrice $\mathfrak{A}$ est égale à la matrice unité $\mathfrak{E}$, les inégalités (I) du § 3 s'écrivent

$$\tau(\mathfrak{S}[\mathfrak{x}]) \geqslant \tau(s_l) \qquad l = 1, \ldots, n \qquad (\mathrm{I}_0)$$

avec $\mathfrak{x}$ entier de K tel que $(\xi_1, \ldots, \xi_n) \neq 0$. Ce sont ces inégalités qui, avec (II), définissent le domaine R_0 contenant tous les domaines $R(\mathfrak{A})$.

Théorème 4. Si un système de γ matrices $\mathfrak{S}^{(k)}$, dont les g_1 premières sont réelles et symétriques, les g_2 suivantes hermitiennes, vérifie les inégalités (I_0), on a pour $k = 1, 2, \ldots, \gamma$:

$$| \mathfrak{S}^{(k)} | \leqslant s_1^{(k)} s_2^{(k)} \ldots s_n^{(k)} \leqslant C | \mathfrak{S}^{(k)} |$$

où C est une constante ne dépendant que de n et du corps K : $C = C(n, K)$.

Montrons d'abord que les inégalités (I_0) à elles seules entraînent qu'aucune des formes de matrices $\mathfrak{S}^{(k)}$ n'est indéfinie; c.-à-d. que l'on a toujours:

$$\mathfrak{S}^{(k)}[\mathfrak{x}] \geqslant 0$$

quel que soit le vecteur $\mathfrak{x}$ (réel si $k \leqslant g_1$).

Supposons par absurde que pour un certain indice ϱ on ait:

$$a_0 = \mathfrak{S}^{(\varrho)}[\mathfrak{x}_0] < 0 , \qquad (\mathfrak{x}_0 \text{ réel si } \varrho \leqslant g_1) .$$

$\mathfrak{x}_0$ n'est pas nécessairement un vecteur entier du corps $K^{(\varrho)}$. Mais la fonction $\mathfrak{S}^{(\varrho)}[\mathfrak{x}]$ des $\xi_1, \ldots, \xi_n$ étant continue, on peut déterminer un nombre réel $r > 0$ tel que, pour tout $\mathfrak{x}$ satisfaisant à $|\mathfrak{x} - \mathfrak{x}_0| \leqslant r$, on ait:

$$| \mathfrak{S}^{(\varrho)}[\mathfrak{x}] - a_0 | \leqslant \frac{|a_0|}{2}$$

donc aussi

$$\mathfrak{S}^{(\varrho)}[\mathfrak{x}] \leqslant \frac{a_0}{2} .$$

Or il existe une infinité de vecteurs $\mathfrak{x}$ du corps $K^{(\varrho)}$ tels que $|\mathfrak{x}^{(\varrho)} - \mathfrak{x}_0| \leqslant r$; prenons-en un quelconque, et soit $q \neq 0$ un entier rationnel tel que $q\mathfrak{x} =$ entier. Désignant ce vecteur entier $q\mathfrak{x}$ par $\mathfrak{x}$, on aura

$$\mathfrak{S}^{(\varrho)}[\mathfrak{x}^{(k)}] \leqslant \frac{q^2 a_0}{2} = b_0 < 0 .$$

Il existe donc un vecteur entier $\mathfrak{x}$ de K pour lequel la forme hermitienne de matrice $\mathfrak{S}^{(\varrho)}$ prend une valeur négative.

Supposons alors $\gamma > 1$. Pour les autres conjugués de cet $\mathfrak{x}$, soient $a_k = \mathfrak{S}^{(k)}[\mathfrak{x}^{(k)}]$ les valeurs des autres formes, $k \neq \varrho$. Soit $a = \max |a_k|$. Il existe une unité ε du corps K pour laquelle

$$|\varepsilon^{(\varrho)}| > 1, \quad |\varepsilon^{(k)}| < 1 \qquad \text{si } k \neq \varrho .$$

Pour une certaine puissance de cette unité, puissance que nous désignerons de nouveau par ε, on aura:

$$\left| \varepsilon^{(\varrho)} \right| \geqslant \left| \frac{a}{b_0} \right| \gamma .$$

Il est alors visible que, si $\mathfrak{y} = \varepsilon \mathfrak{x}$, la trace $\tau(\mathfrak{S}[\mathfrak{y}])$ est négative; en effet:

$$\tau(\mathfrak{S}[\mathfrak{y}]) = \mathfrak{S}^{(\varrho)}[\mathfrak{y}^{(\varrho)}] + \sum_{k \neq \varrho} \mathfrak{S}^{(k)}[\mathfrak{y}^{(k)}] =$$

$$= |\varepsilon^{(\varrho)}|^2 \, \mathfrak{S}^{(\varrho)}[\mathfrak{x}^{(\varrho)}] + \sum_{k \neq \varrho} |\varepsilon^{(k)}|^2 \, \mathfrak{S}^{(k)}[\mathfrak{x}^{(k)}] \leqslant$$

$$\leqslant \left| \frac{a}{b_0} \right| \gamma \cdot b_0 + (\gamma - 1)\, a = -a < 0 \; .$$

Cette conclusion est vraie aussi avec $\mathfrak{y} = \mathfrak{x}$ dans le cas où $\gamma = 1$, car alors $\tau(\mathfrak{S}[\mathfrak{y}]) = \mathfrak{S}^{(1)}[\mathfrak{x}^{(1)}] < 0$.

Pour un multiple entier rationnel assez grand de $\mathfrak{y}$, on pourrait rendre $\tau(\mathfrak{S}[\mathfrak{y}])$ négatif et aussi grand qu'on le voudrait, ce qui est impossible, en vertu de (I_0):

$$\tau(\mathfrak{S}[\mathfrak{x}]) \geqslant \tau(s_1) \quad \text{si} \quad \mathfrak{x} \text{ entier } \neq 0 \; .$$

Il suit de là que les inégalités:

$$s_l^{(k)} \geqslant 0 \; , \quad 2\,|\,s_{ij}^{(k)}\,| \leqslant s_i^{(k)} + s_j^{(k)}$$

sont des conséquences de (I_0) (voir § 4).

Montrons ensuite que les $s_l^{(k)}$, $k = 1, \ldots, \gamma$, sont du même ordre de grandeur, c'est-à-dire que:

$$s_l^{(\lambda)} \leqslant c_1 \, s_l^{(\mu)} \qquad \text{quels que soient } \lambda, \mu \, , \tag{4}$$

la constante c_1 ne dépendant que de K. Pour la démonstration, on peut supposer $\gamma > 1$, car si $\gamma = 1$, l'affirmation (4) est évidente. Ordonnons les conjugués de K de manière à ce que l'on ait:

$$0 \leqslant s_l^{(1)} \leqslant s_l^{(2)} \leqslant \cdots \leqslant s_l^{(\gamma)} \; .$$

Appliquons (I_0) au vecteur $\mathfrak{x} = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ avec $\begin{cases} \xi_i = 0 \text{ si } i \neq l \; . \\ \xi_l = \varepsilon = \text{unité de } K. \end{cases}$

On obtient:

$$\sum_{k=1}^{\gamma} s_l^{(k)} \leqslant \sum_{k=1}^{\gamma} s_l^{(k)} \, |\, \varepsilon^{(k)} \,|^2 \; .$$

Or il existe une unité de K telle que:

$$|\varepsilon^{(1)}| > 1, \quad |\varepsilon^{(k)}| < 1 \qquad \text{si} \qquad k \neq 1 \; .$$

L'inégalité obtenue s'écrit:

$$s_l^{(1)}\left(|\,\varepsilon^{(1)}\,|^2-1\right)+\sum_{k=2}^{\gamma-1} s_l^{(k)}\left(|\,\varepsilon^{(k)}\,|^2-1\right)\geqslant s_l^{(\gamma)}\left(1-|\,\varepsilon^{(\gamma)}\,|^2\right)$$

d'où a fortiori, les $s_l^{(k)}$ étant non négatifs:

$$s_l^{(1)}\left(|\,\varepsilon^{(1)}\,|^2-1\right)\geqslant s_l^{(\gamma)}\left(1-|\,\varepsilon^{(\gamma)}\,|^2\right)\ .$$

Donc

$$s_l^{(\gamma)}\leqslant\frac{|\,\varepsilon^{(1)}\,|^2-1}{1-|\,\varepsilon^{(\gamma)}\,|^2}\,s_l^{(1)}\leqslant c_1 s_l^{(1)}$$

avec

$$c_1=\max.\ \frac{|\,\varepsilon^{(1)}|^2-1}{1-|\,\varepsilon^{(\gamma)}\,|^2}\quad\text{(max. pour toutes les ordonnances possibles des conjugués)}\ .$$

Comme $0\leqslant s_l^{(1)}\leqslant\cdots\leqslant s_l^{(\gamma)}$, on voit que

$$s_l^{(\lambda)}\leqslant s_l^{(\gamma)}\leqslant c_1 s_l^{(1)}\leqslant c_1 s_l^{(\mu)}\ \text{(c. q. f. d.)}\ .$$

Les inégalités (3) du § 4 sont des conséquences de (I_0):

$$\tau(s_1)\leqslant\tau(s_2)\leqslant\cdots\leqslant\tau(s_n)\ . \tag{3}$$

Il en est de même des inégalités suivantes, que l'on déduit facilement de (3) et (4):

$$s_i^{(\lambda)}\leqslant c_1^2 s_j^{(\mu)}\qquad\text{si}\quad i\leqslant j\ . \tag{5}$$

Pour démontrer le théorème 4, envisageons d'abord le cas où aucune des $\mathfrak{S}$ n'est semi-positive: $\mathfrak{S}^{(k)}>0$ pour tout k. On procède par induction sur n. Le théorème est vrai pour $n=1$, avec $C=1$. Supposons le vrai pour les systèmes S de formes quadratiques à $n-1$ variables.

On se sert de l'identité:

$$\mathfrak{S}=\begin{pmatrix}\mathfrak{S}_1 & \bar{\mathfrak{s}}\\ \mathfrak{s}' & s_n\end{pmatrix}=\begin{pmatrix}\mathfrak{S}_1 & 0\\ 0 & h\end{pmatrix}\begin{bmatrix}\mathfrak{E} & \overline{\mathfrak{S}}_1^{-1}\mathfrak{s}\\ 0 & 1\end{bmatrix} \tag{6}$$

où $h+\mathfrak{S}_1^{-1}[\mathfrak{s}]=s_n$, et où $\mathfrak{S}_1$ est la matrice obtenue en supprimant dans $\mathfrak{S}$ la dernière ligne et la dernière colonne. $|\,\mathfrak{S}_1|$ est différent de zéro, car la matrice $\mathfrak{S}$ est positive.

Si S vérifie (I_0), le système S_1 des $\mathfrak{S}_1^{(k)}$ vérifie aussi (I_0) pour les vecteurs $\mathfrak{x}$ à $n-1$ composantes. On le voit immédiatement en particularisant $\mathfrak{x}$ de sorte que $\xi_n=0$.

Par hypothèse d'induction on a:

$$1 \leqslant \frac{s_1^{(k)} \dots s_{n-1}^{(k)}}{|\mathfrak{S}_1^{(k)}|} \leqslant c \qquad c = C(n-1, K) \ .$$

Comme $|\mathfrak{S}^{(k)}| = |\mathfrak{S}_1^{(k)}| h^{(k)}$, il suffira de démontrer que l'on a:

$$1 \leqslant \frac{s_n^{(k)}}{h^{(k)}} \leqslant c_0 \ , \quad \text{avec } c_0(n, K) \ .$$

La partie de gauche de ces inégalités est évidente d'après $h + \mathfrak{S}_1^{-1}[\mathfrak{s}] = s_n$, car la matrice $\mathfrak{S}_1^{-1} = \mathfrak{S}_1[\overline{\mathfrak{S}}_1^{-1}]$ est comme $\mathfrak{S}_1$ positive, donc $h \leqslant s_n$. Il reste à démontrer que

$$\frac{s_n^{(k)}}{h^{(k)}} \leqslant c_0 \ .$$

Posons

$$\mathfrak{x} = \begin{pmatrix} \mathfrak{x}_1 \\ \\ \xi_n \end{pmatrix} , \quad \text{où} \quad \mathfrak{x}_1 = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_{n-1} \end{pmatrix} .$$

Au moyen de ces variables l'identité (6) s'écrit

$$\mathfrak{S}[\mathfrak{x}] = \mathfrak{S}_1[\mathfrak{x}_1 + \mathfrak{r}\, \xi_n] + h|\xi_n|^2$$

avec $\mathfrak{r} = \overline{\mathfrak{S}}_1^{-1}\, \mathfrak{s}$.

En posant $\mathfrak{y} = \mathfrak{x}_1 + \mathfrak{r}\, \xi_n = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_{n-1} \end{pmatrix}$ on aura

$$\mathfrak{S}[\mathfrak{x}] = \mathfrak{S}_1[\mathfrak{y}] + h|\xi_n|^2 \ . \tag{6'}$$

Nous allons appliquer (I_0) à un vecteur $\mathfrak{x}$ particulier que nous déterminons à l'aide du théorème de Minkowski déjà utilisé. Considérons les gn formes linéaires $\eta_i^{(k)}$ et $\xi_n^{(k)}$ en les variables u_{ik}:

$$\eta_i^{(k)} = \sum_{\sigma=1}^{g} u_{i\sigma}\, \omega_\sigma^{(k)} + r_i^{(k)} \sum_{\sigma=1}^{g} u_{n\sigma}\, \omega_\sigma^{(k)} \qquad \begin{cases} i = 1, \dots, n-1 \ , \\ k = 1, \dots, \gamma \ , \end{cases}$$

ainsi que pour chaque i les g_2 formes conjuguées de celles qui sont complexes; et

$$\xi_n^{(k)} = \sum_{\sigma=1}^{g} u_{n\sigma}\, \omega_\sigma^{(k)} \qquad k = 1, \dots, g \ .$$

Les $r_i^{(k)}$ sont les composantes des vecteurs $\mathfrak{r}^{(k)} = \overline{\mathfrak{S}}_1^{(k)-1}\, \mathfrak{s}^{(k)}$. Les ω_σ sont les g entiers d'une base de K. Le déterminant de ce système de formes

linéaires est $|\Omega|^n = \sqrt{d^n}$. En outre à toute forme correspond sa conjuguée complexe. On peut donc appliquer le théorème de Minkowski sous la forme énoncée au § 4.

Mais nous allons auparavant multiplier chacune de ces formes linéaires par un facteur convenable, sans que le déterminant ne change. Nous prendrons ce facteur égal à H (nombre positif qui sera fixé plus tard), cela pour toutes les formes η, ainsi que pour les $\xi_n^{(k)}$ si $k \neq \varrho$ fixe. Quant à la forme $\xi_n^{(\varrho)}$ (si $\varrho \leqslant g_1$) ou aux deux formes conjuguées $\xi_n^{(\varrho)}$ et $\xi_n^{(\varrho+g_2)}$ (si $g_1 + 1 \leqslant \varrho \leqslant \gamma$), il faudra la ou les multiplier par le facteur H^{-q}, avec $q = gn - 1$ ou $q = \frac{1}{2}gn - 1$ suivant les cas.

Il existe donc des $u_{i\sigma}$ entiers rationnels non tous nuls tels que:

$$\left.\begin{array}{ll} |\eta_i^{(k)}| \leqslant \dfrac{\Delta}{H} & \begin{cases} i = 1, \ldots, n-1 \\ k = 1, \ldots, g \end{cases} . \\ |\xi_n^{(k)}| \leqslant \dfrac{\Delta}{H} & k = 1, \ldots, g,\ k \neq \varrho,\ \varrho + g_2 . \\ |\xi_n^{(\varrho)}| \leqslant H^q \cdot \Delta & \Delta = \sqrt[2g]{D} . \end{array}\right.$$

Pour $H > \Delta$, on a certainement $\xi_n \neq 0$; car si $\xi_n = 0$, en vertu de $\mathfrak{y} = \mathfrak{x}_1 + \mathfrak{x}\xi_n$, les η_i seraient des entiers algébriques, de normes < 1, donc nuls, et les η et ξ_n seraient tous nuls, ce qui n'est pas. Supposons donc $H > \Delta$; alors $\xi_n \neq 0$, et l'on peut appliquer (I_0) au vecteur $\mathfrak{x}$ ainsi déterminé, pour $l = n$; on obtient en vertu de (6′):

$$\sum_{k=1}^{\gamma} \mathfrak{S}_1^{(k)}[\mathfrak{y}^{(k)}] + \sum_{k=1}^{\gamma} h^{(k)} |\xi_n^{(k)}|^2 \geqslant \tau(s_n) .$$

Remplaçons les η et ξ_n par les évaluations trouvées; il vient:

$$\frac{\Delta^2}{H^2} \sum_{k=1}^{\gamma} \sum_{i,j=1}^{n-1} |s_{ij}^{(k)}| + \frac{\Delta^2}{H^2} \sum_{k \neq \varrho} h^{(k)} + h^{(\varrho)} \Delta^2 \cdot H^{2q} \geqslant \tau(s_n) .$$

En tenant compte des inégalités:

$$h^{(k)} \leqslant s_n^{(k)} ;\ 2|s_{ij}^{(k)}| \leqslant s_i^{(k)} + s_j^{(k)} ;\ \tau(s_i) \leqslant \tau(s_j) \text{ si } i < j ,$$

on trouve par un calcul analogue à celui du § 4:

$$(n-1)^2 \frac{\Delta^2}{H^2} \tau(s_n) + \frac{\Delta^2}{H^2} \tau(s_n) + h^{(\varrho)} \Delta^2 H^{2q} \geqslant \tau(s_n)$$

d'où

$$\tau(s_n) \left(1 - n^2 \frac{\Delta^2}{H^2}\right) \leqslant h^{(\varrho)} \Delta^2 H^{2q} .$$

Prenons

$$H = \sqrt{2} \cdot n \cdot \Delta > \Delta \ .$$

Des inégalités (4) on déduit aisément:

$$\tau(s_n) \geqslant c_3 \, s_n^{(\varrho)} \qquad \left(c_3 = \frac{\gamma - 1}{c_1} + 1\right) .$$

L'inégalité trouvée devient finalement:

$$s_n^{(\varrho)} \cdot \frac{c_3}{2} \leqslant h^{(\varrho)} \, \Delta^2 \, H^{2q}$$

c'est-à-dire:

$$\frac{s_n^{(\varrho)}}{h^{(\varrho)}} \leqslant \frac{2}{c_3} \cdot \Delta^2 \, H^{2q} = c_0 \ .$$

Le théorème 4 est démontré dans le cas où $|\mathfrak{S}^{(k)}| > 0$ pour $k = 1, \ldots, \gamma$. Le cas où $|\mathfrak{S}^{(k)}| = 0$ pour un ou plusieurs k se ramène au précédent. En effet un système S tel que $|S| = 0$ et vérifiant (I_0) est la limite d'une suite de systèmes S_n avec $|S_n| > 0$ et vérifiant (I_0); celà résulte du fait que le domaine défini par (I_0) est *convexe*. Prenons en effet un système S_0 vérifiant (I_0) et tel que $|S_0| > 0$, et considérons les systèmes $S(\lambda) = (1 - \lambda)S + \lambda S_0$ avec $1 \geqslant \lambda > 0$. Ces systèmes sont formés de matrices toutes positives, comme sommes de matrices positives et semi-positives. Donc $|S(\lambda)| > 0$. Pour $\lambda \to 0$ on a $S(\lambda) \to S$. En outre les systèmes $S(\lambda)$ vérifient (I_0) à cause de la convexité du domaine (I_0). La démonstration du théorème 4 s'applique à ces systèmes $S(\lambda)$, qui vérifient par conséquent les inégalités de ce théorème. En passant à la limite, on voit que ces inégalités sont vraies aussi pour le système S.

Une conséquence. Nous avons vu au début de la démonstration du théorème 4 que le domaine défini par (I_0) est tout entier formé de systèmes de matrices positives ou semi-positives. Comme $R(\mathfrak{A})$ est défini par (I_0) et (II), nous voyons que les systèmes de $R(\mathfrak{A})$ qui ne sont pas dans P sont formés de γ matrices dont l'une au moins est semi-positive; nous les appellerons *systèmes semi-positifs*. On a pour eux $|S| = 0$. Il s'ensuit que *le domaine réduit R s'obtient en excluant les systèmes semi-positifs de la réunion des R_ν.*

§ 7. Systèmes frontières de R

Considérons maintenant les systèmes frontières du domaine réduit R. Ecartons ceux qui sont semi-positifs. Nous avons le

Théorème 5. Si S est un système frontière de R pour lequel $|S| > 0$, il existe une matrice unimodulaire $\mathfrak{U} \neq \omega\mathfrak{E}$ qui transforme S en un système T frontière de R.

Un système S frontière de R est à la fois limite d'une suite de systèmes réduits S_m et d'une suite de systèmes non réduits Q_m:

$$\begin{aligned} &S_1,\ S_2, \ldots \to S && S_m \text{ dans } R\ . \\ &Q_1,\ Q_2, \ldots \to S && Q_m \text{ non dans } R\ . \end{aligned}$$

On a $|S| > 0$; sans diminuer la généralité, on peut supposer que $N(|\mathfrak{S}|) = \prod_{k=1}^{g} |\mathfrak{S}^{(k)}| = 1$. (Par définition $\mathfrak{S}^{(\gamma+k)} = \overline{\mathfrak{S}}_1^{(g_1+k)}$ pour $k=1,\ldots,g_2$).
La norme N est le produit étendu sur un indice supérieur k omis, de $k = 1$ à $k = g$. Pour les S_m et les Q_m, on peut également supposer que

$$N(|\mathfrak{S}_m|) = N(|\mathfrak{Q}_m|) = 1\ .$$

Soient $\mathfrak{B}_m$ la matrice auxiliaire du système Q_m, $\dot{T}_m$ le système obtenu en effectuant sur Q_m la première transformation, T_m le système réduit équivalent à Q_m. Employant la notation abrégée du § 2, nous avons

$$\begin{aligned} &Q_m[B_m] = \dot{T}_m = T_m[A_{\nu(m)}] && \dot{T}_m \text{ dans } R(\mathfrak{A}_{\nu(m)}) \\ &Q_m[U_m] = T_m && T_m \text{ dans } R\ . \\ &\mathfrak{B}_m = \mathfrak{U}_m \mathfrak{A}_{\nu(m)} \end{aligned}$$

La matrice unimodulaire $\mathfrak{U}_m$ n'est pas une unité générale, puisque Q_m n'est pas réduit:

$$\mathfrak{U}_m \neq \omega\mathfrak{E}\ .$$

Le système S étant positif, il existe une quantité $\mu > 0$ telle que

$$S[x] \geqslant 2\,\mu\, x'\,\bar{x}\ .$$

x est le vecteur formé en superposant γ vecteurs $\mathfrak{x}^{(k)}$ de n variables chacun, $k = 1, \ldots, \gamma$. Puisque $\lim_{m\to\infty} Q_m = S$, on a à partir d'un certain rang

$$|(Q_m - S)[x]| \leqslant \mu\, x'\,\bar{x}\ .$$

Donc

$$Q_m[x] \geqslant \mu\, x'\,\bar{x}\ .$$

Le système $Q_m - \mu E$ est donc positif ou semi-positif. Son transformé P_m par $\mathfrak{B}_m$ l'est également:

$$P_m = \dot{T}_m - \mu B'_m \overline{B}_m \geqslant 0\ .$$

Supprimons pour un instant l'indice m. Posons

$$\dot{\mathfrak{T}} = (\dot{t}_{ij}) \qquad \mathfrak{B} = (\beta_{ij}) \qquad \mathfrak{P} = (p_{ij})$$
$$\dot{t}_{ii} = \dot{t}_i \qquad\qquad p_{ii} = p_i$$

Le système P étant positif ou semi-positif, on a

$$p_i^{(k)} = \dot{t}_i^{(k)} - \mu \sum_{j=1}^{n} | \beta_{ji}^{(k)}|^2 \geqslant 0 \ .$$

D'où

$$\dot{t}_i^{(k)} \geqslant \mu \sum_{j=1}^{n} | \beta_{ji}^{(k)} |^2 \ . \tag{7}$$

Faisant le produit de $k = 1$ à $k = g$:

$$N(\dot{t}_i) \geqslant \mu^g \left(\sum_{j=1}^{n} N(\beta_{ji}^2) + \cdots \right) \ .$$

Les termes non écrits sont positifs ou nuls. Or $|\mathfrak{B}| \neq 0$, donc les éléments β_{ij} ne sont pas tous nuls pour $j = 1, \ldots, n$, et par conséquent, ces β_{ji} étant des entiers de K, on a

$$\sum_{j=1}^{n} N(\beta_{ji}^2) + \cdots \geqslant 1 \ .$$

Il s'ensuit que

$$N(\dot{t}_i) \geqslant \mu^g \ . \tag{8}$$

Le système $\dot{T}$ étant dans $R(\mathfrak{B})$ donc dans R_0, les inégalités (4) et (5) du § 6 ont lieu. Multipliant ces inégalités convenablement membre à membre, on obtient

$$c_4 \, \dot{t}_i^{(\lambda) g} \leqslant N(\dot{t}_i) \tag{9}$$

$$c_5 \, N(\dot{t}_i) \leqslant N(\dot{t}_j) \qquad \text{si} \quad i < j \ . \tag{10}$$

Les c_k désignent des constantes positives ne dépendant que de n et de K.

Le théorème 4 donne

$$\dot{t}_1^{(k)} \ldots \dot{t}_n^{(k)} \leqslant C \, | \dot{\mathfrak{T}}^{(k)} | \ .$$

On en déduit en tenant compte du théorème 1 :

$$N(\dot{t}_1) \ldots N(\dot{t}_n) \leqslant C^g N(|\dot{\mathfrak{T}}|) = C^g N(|\mathfrak{Q}|) N(|\mathfrak{B}|) \leqslant C^g \, c \ .$$

D'après (10) et (8) on a

$$N(\dot{t}_1) \ldots N(\dot{t}_{n-1}) \geqslant c_6 \, N(\dot{t}_1^{n-1}) \geqslant c_6 \, \mu^{g(n-1)} \ .$$

Remplaçant dans l'inégalité précédente, on trouve

$$N(\dot{t}_n) \leqslant \frac{C^g \cdot c}{c_6} \mu^{-g(n-1)} .$$

A cause de (9) (pour $i = n$) on en tire

$$\dot{t}_n^{(\lambda)} \leqslant c_7 \mu^{-(n-1)} .$$

Les $\dot{t}_n^{(\lambda)}$ sont donc bornés, la borne ne dépendant que de S et de K. En vertu de (5) § 6, les $\dot{t}_i^{(\lambda)}$ le sont également, de même que les $\beta_{ij}^{(k)}$ à cause de (7). Comme les β_{ij} sont des entiers de K, il n'y a pour eux qu'un nombre fini de valeurs possibles, et par conséquent aussi pour la matrice $\mathfrak{B} = (\beta_{ij})$. La suite des $\mathfrak{B}_m$ contient donc une infinité de fois la même matrice $\mathfrak{B}_0 = \mathfrak{U}_0 \mathfrak{A}_{\nu_0}$ $(\mathfrak{U}_0 \neq \omega \mathfrak{E})$:

On a $$B_{m_1} = B_{m_2} = \cdots = B_0 = U_0 A_{\nu_0} ,$$

pour une suite d'entiers

$$m_1 < m_2 < \cdots$$

La suite correspondante des Q est telle que

$$Q_m[U_0] = T_m , \qquad T_m \text{ dans } R .$$

En passant à la limite, R étant fermé dans P (voir § 5), on obtient

$$S[U_0] = T \qquad S, T \text{ dans } R , \qquad \mathfrak{U}_0 \neq \omega \mathfrak{E} .$$

Il reste à montrer que T est frontière de R. Deux cas peuvent se présenter: ou bien $T = S$, auquel cas le théorème est vrai puisque par hypothèse S est frontière de R; ou bien $T \neq S$; il suffit alors de recourir au théorème 3 (2ème partie) pour voir que T est frontière de R.

Théorème 6. Si deux systèmes S et T réduits sont équivalents, $\mathfrak{S}^{(k)} = \mathfrak{T}^{(k)}[\mathfrak{U}^{(k)}]$ pour $k = 1, \ldots, \gamma$, $\mathfrak{U}$ appartient à un ensemble fini de matrices unimodulaires $\mathfrak{U}_1, \ldots, \mathfrak{U}_M$.

Pour $k = 1, \ldots, \gamma$ on a par hypothèse

$$\mathfrak{S}^{(k)} = \mathfrak{T}^{(k)}[\mathfrak{U}^{(k)}] \qquad S , \ T \text{ dans } R .$$

Par définition du domaine R cela signifie que

$$\mathfrak{S} = \dot{\mathfrak{S}}\,[\mathfrak{A}_\mu^{-1}] \quad \text{avec} \quad \dot{\mathfrak{S}} \text{ dans } R(\mathfrak{A}_\mu)$$
$$\mathfrak{T} = \dot{\mathfrak{T}}\,[\mathfrak{A}_\nu^{-1}] \quad \text{avec} \quad \dot{\mathfrak{T}} \text{ dans } R(\mathfrak{A}_\nu) .$$

On supprime l'indice supérieur afin d'alléger. Mais il faut se rappeler que les relations écrites doivent avoir lieu pour les valeurs $1, \ldots, \gamma$ de cet indice.

Comme $\mathfrak{S} = \mathfrak{T}[\mathfrak{U}]$, on voit que

$$\dot{\mathfrak{S}} = \dot{\mathfrak{T}}[\mathfrak{A}_\nu^{-1}\,\mathfrak{U}\,\mathfrak{A}_\mu] = \dot{\mathfrak{T}}[\mathfrak{X}] \quad \text{où} \quad \mathfrak{X} = \mathfrak{A}_\nu^{-1}\,\mathfrak{U}\,\mathfrak{A}_\mu\,.$$

La matrice $\mathfrak{X}$ a ses éléments dans K. Elle n'est pas nécessairement entière, mais il existe un entier rationnel a ne dépendant que de n et de K tel que $a\,\mathfrak{X}$ soit entière. Il suffit en effet de prendre a divisible par tous les $|\mathfrak{A}_\nu|$. Nous dirons dans ces conditions que $\mathfrak{X}$ *a ses dénominateurs bornés*. $\mathfrak{X}^{-1}$ a également ses dénominateurs bornés, puisque $\mathfrak{X}^{-1} = \mathfrak{A}_\mu^{-1}\,\mathfrak{U}^{-1}\,\mathfrak{A}_\nu$.

Les domaines $R(\mathfrak{A}_\mu)$ et $R(\mathfrak{A}_\nu)$ étant contenus dans $R_0 = R(\mathfrak{E})$, le théorème 6 est une conséquence du

Théorème 6′. Si deux systèmes S et T sont dans R_0, et si $\mathfrak{S} = \mathfrak{T}[\mathfrak{X}]$, $\mathfrak{X}$ et $\mathfrak{X}^{-1}$ ayant leurs dénominateurs bornés, la matrice $\mathfrak{X}$ est bornée ainsi que ses conjuguées.

En effet de 6′ découle que la matrice $a\mathfrak{X}$ est entière et bornée, ainsi que toutes ses conjuguées. Donc $a\mathfrak{X}$ n'est susceptible que d'un nombre fini de valeurs entières dans K, et par conséquent $\mathfrak{U} = \mathfrak{A}_\nu\mathfrak{X}\,\mathfrak{A}_\mu^{-1}$ également.

Dans ce théorème comme dans la suite, *borné signifie inférieur en valeur absolue à une constante ne dépendant que de n et de K*. Nous désignerons par $c_1, c_2, \ldots$ de telles constantes.

Démonstration du théorème 6′.

1er lemme. Soit S un système positif de R_0. Considérons une décomposition quelconque de $\mathfrak{S}$ en 4 matrices :

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \overline{\mathfrak{S}}_2 \\ \mathfrak{S}_2' & \mathfrak{S}_3 \end{pmatrix}, \quad \mathfrak{S}_1 \text{ quadratique de degré } m\ .$$

Alors la matrice $\overline{\mathfrak{S}}_1^{-1}\,\mathfrak{S}_2$ est bornée.

Appliquons les inégalités (I_0) définissant R_0 au vecteur $\mathfrak{x} = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ de composantes $\xi_i = \omega_\nu$, $\xi_j = \pm 1$, i, j fixes, et pour $l = j$. Les $\omega_1, \ldots, \omega_g$ forment une base des entiers du corps K. On obtient ainsi

$$\Big|\ 2 \sum_{k=1}^{\gamma} R(s_{ij}^{(k)}\,\omega_\nu^{(k)})\ \Big| \leqslant \sum_{k=1}^{\gamma} s_i^{(k)}\,|\,\omega_\nu^{(k)}\,|^2\ . \tag{11}$$

Pour $\nu = 1, 2, \ldots, g$ considérons les g équations

$$\sum_{k=1}^{\gamma} R(s_{ij}^{(k)} \omega_\nu^{(k)}) = a_\nu \tag{12}$$

les g inconnues étant $Rs_{ij}^{(k)}$, $k = 1, \ldots, \gamma$ et $Js_{ij}^{(k)}$, $k = g_1 + 1, \ldots, \gamma$. Les a_ν sont des quantités réelles données. La matrice de ce système d'équations linéaires est

$$\Phi = (\omega_\nu^{(k_1)}, R\omega_\nu^{(k_2)}, \ldots J\omega_\nu^{(k_2)})$$

$$k_1 = 1, \ldots, g_1 \quad ; \quad k_2 = g_1 + 1, \ldots, \gamma \quad ; \quad \nu = 1, \ldots, g \ .$$

Le déterminant est facile à calculer; on trouve

$$|\Phi| = (2i)^{-g_2} |\Omega|$$

où Ω est la matrice $\Omega = (\omega_i^{(k)})$. $|\Omega|^2 = d$ est le discriminant de K.

On peut donc résoudre ces équations, et l'on trouve

$$\left.\begin{matrix} Rs_{ij}^{(k)} \\ Js_{ij}^{(k-g_2)} \end{matrix}\right\} = \sum_{\nu=1}^{g} \zeta_{\nu k} a_\nu \quad \left\{\begin{matrix} k = 1, \ldots, \gamma \ . \\ k = \gamma + 1, \ldots, g \ . \end{matrix}\right.$$

où les $\zeta_{\nu k}$ ne dépendent que du corps K.

Comme d'après (11) et (12):

$$|a_\nu| \leqslant \frac{1}{2} \sum_{\lambda=1}^{\gamma} s_i^{(\lambda)} |\omega_\nu^{(\lambda)}|^2 \ ,$$

on voit que les quantités $Rs_{ij}^{(k)}$, $Js_{ij}^{(k)}$ sont en valeur absolue inférieures à des expressions de la forme $\sum_{\lambda=1}^{\gamma} \Theta_{\lambda k} s_i^{(\lambda)}$, où les $\Theta_{\lambda k} \geqslant 0$ ne dépendent que de K. Les $s_i^{(\lambda)}$, $\lambda = 1, \ldots, \gamma$ étant d'après (4) § 6 du même ordre de grandeur, on a finalement

$$|s_{ij}^{(k)}| \leqslant c_8 s_i^{(\lambda)} \quad \text{pour tous les } \lambda, k \ . \tag{13}$$

Cela est vrai pour $j > i$ aussi bien que pour $j \leqslant i$. Pour $j \leqslant i$ cela résulte immédiatement des inégalités (1) et (5) (§ 4 et 6). A cause de la symétrie de $\mathfrak{S}$ on a aussi

$$|s_{ij}^{(k)}| \leqslant c_8 s_j^{(\lambda)} \ . \tag{13'}$$

On démontre alors facilement que les éléments de $\overline{\mathfrak{S}}_1^{-1} \mathfrak{S}_2$ sont bornés. Considérons d'abord $\overline{\mathfrak{S}}_1^{-1} = \frac{1}{|\mathfrak{S}_1|} (h_{ik}) = (t_{ik})$. Les h_{ik} sont les déter-

minants adjoints des éléments de $\mathfrak{S}_1$, et comme chaque terme de $\mathfrak{S}_1$ est d'après (13′) inférieur au terme diagonal de sa colonne multiplié par c_8, on a pour chaque h_{ik}

$$| h_{ik} | \leqslant m!\, c_8^{m-1} \frac{s_1 \dots s_m}{s_k} .$$

Donc

$$| t_{ik} | \leqslant c_9 \frac{s_1 \dots s_m}{| \mathfrak{S}_1 |} \cdot \frac{1}{s_k} . \tag{14}$$

Le système des $\mathfrak{S}^{(k)}$ est dans R_0. Désignons par $R_0^{(n)}$ ce domaine R_0 si l'on veut marquer sa dépendance du degré n des matrices $\mathfrak{S}$. Le système des $\mathfrak{S}_1^{(k)}$ définies par la décomposition $\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \overline{\mathfrak{S}}_2 \\ \mathfrak{S}_2' & \mathfrak{S}_3 \end{pmatrix}$ est alors dans $R_0^{(m)}$; il suffit pour le voir d'annuler les $n - m$ dernières composantes du vecteur $\mathfrak{x}$ figurant dans (I_0) (§ 6). Le théorème 4 est donc applicable à ce système des $\mathfrak{S}_1^{(k)}$, et l'inégalité (14) devient

$$| t_{ik} | \leqslant \frac{c_{10}}{s_k} .$$

Formons alors

$$\overline{\mathfrak{S}}_1^{-1}\, \mathfrak{S}_2 = \Big(\sum_{k=1}^{m} t_{ik} s_{kj} \Big) = (r_{ij}) .$$

D'après

$$| t_{ik} | \leqslant \frac{c_{10}}{s_k} \quad \text{et} \quad | s_{kj} | \leqslant c_8 s_k ,$$

on voit que

$$|r_{ij}| \leqslant m\, c_{10}\, c_8 \leqslant c_{11} , \qquad \text{c. q. f. d.}$$

Reprenons l'identité (6) du § 6:

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S} & \bar{\mathfrak{s}} \\ \mathfrak{s}' & s_n \end{pmatrix} = \begin{pmatrix} \mathfrak{S}_1 & 0 \\ 0 & a_n \end{pmatrix} \begin{bmatrix} \mathfrak{E}_{n-1} & \overline{\mathfrak{S}}_1^{-1} \mathfrak{s} \\ 0 & 1 \end{bmatrix} , \quad a_n + \mathfrak{S}_1^{-1}[\mathfrak{s}] = s_n . \tag{6}$$

D'après le 1er lemme, $\overline{\mathfrak{S}}_1^{-1}\, \mathfrak{s}$ est bornée.

En appliquant la même identité à $\mathfrak{S}_1$, qui est dans $R_0^{(n-1)}$ comme on vient de le voir, et en continuant de la sorte, on obtient finalement

$$\mathfrak{S} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \begin{bmatrix} 1 & & \beta_{ik} \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = \mathfrak{D}_a [\mathfrak{B}]$$

où $\mathfrak{D}_a$ est la matrice diagonale d'éléments $a_1, \dots, a_n$, et où $\mathfrak{B} = (\beta_{ik})$ a ses éléments bornés:

$$\beta_{ik} = 0 \quad \text{si} \quad i > k \; ; \qquad \beta_{ii} = 1 \; ; \qquad |\beta_{ik}| \leqslant c_{12} \; .$$

Quant aux a, on a pour a_n d'après (6):

$$|\mathfrak{S}| = |\mathfrak{S}_1| \, a_n \; ; \qquad a_n \leqslant s_n \; .$$

Or le théorème 4 donne

$$\frac{s_1 \ldots s_n}{|\mathfrak{S}|} \leqslant C \; ; \quad |\mathfrak{S}_1| \leqslant s_1 \ldots s_{n-1} \; .$$

On en déduit que $s_n \leqslant C a_n$.

D'une façon générale on a de même

$$s_k \geqslant a_k \geqslant \frac{1}{C} s_k \; .$$

a_k est du même ordre de grandeur que s_k.

La matrice $\mathfrak{T}$ peut être mise sous une forme analogue à $\mathfrak{S}$:

$$\mathfrak{T} = \begin{pmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{pmatrix} \begin{bmatrix} 1 & & \gamma_{ik} \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = \mathfrak{D}_b[\mathfrak{C}]$$

où $\mathfrak{C}$ est une matrice du même type que $\mathfrak{B}$, et où

$$t_k \geqslant b_k \geqslant \frac{1}{C} t_k \; .$$

En vertu de (5) § 6 on voit alors que

$$\begin{aligned} a_i &\leqslant c_{13} \, a_j \qquad \text{si} \qquad i \leqslant j \; . \\ b_i &\leqslant c_{13} \, b_j \qquad \text{si} \qquad i \leqslant j \; . \end{aligned} \tag{15}$$

2e lemme. Les $a_i^{(k)}$ et $b_i^{(k)}$ précédemment définis sont du même ordre de grandeur, c'est-à-dire qu'il existe une constante c_{17} ne dépendant que de n de K telle que

$$\frac{1}{c_{17}} b_i^{(\mu)} \leqslant a_i^{(\lambda)} \leqslant c_{17} \, b_i^{(\mu)} \qquad \begin{matrix} \lambda, \mu = 1, \ldots, \gamma \; . \\ i = 1, \ldots, n \; . \end{matrix}$$

Pour la démonstration, il est essentiel que $\mathfrak{X}$ soit une matrice à coefficients dans K de dénominateurs bornés, de même que $\mathfrak{X}^{-1}$.

On a $\mathfrak{S} = \mathfrak{T}[\mathfrak{X}]$, d'où $\mathfrak{D}_a = \mathfrak{D}_b[\mathfrak{P}]$ avec $\mathfrak{P} = \mathfrak{C}\mathfrak{X}\mathfrak{B}^{-1}$. Soit

$$\mathfrak{P} = (p_{ij}) \qquad \mathfrak{X} = (\xi_{ij}) \; .$$

La relation $\mathfrak{D}_a = \mathfrak{D}_b[\mathfrak{P}]$ donne

$$a_k = \sum_{i=1}^{n} | p_{ik} |^2 b_i \ .$$

Par conséquent

$$| p_{ik} | \leqslant \sqrt{\frac{a_k}{b_i}} \ . \tag{16}$$

Considérons la relation $\mathfrak{X} = \mathfrak{C}^{-1}\mathfrak{P}\mathfrak{B}$. La matrice $\mathfrak{C}$ étant bornée et $|\mathfrak{C}| = 1$, il s'ensuit que $\mathfrak{C}^{-1} = (\delta_{ij})$ est également bornée; en outre $\mathfrak{C}^{-1}$ a une forme analogue à $\mathfrak{C}$, c'est-à-dire que $\delta_{ij} = 0$ si $i > j$ et $\delta_{ii} = 1$. La relation $\mathfrak{X} = \mathfrak{C}^{-1}\mathfrak{P}\mathfrak{B}$ donne à cause de (15) et (16):

$$| \xi_{ik} | = | \sum_{\substack{r \geq i \\ s \leq k}} \delta_{ir} \gamma_{sk} p_{rs} | \leqslant c_{14} \sqrt{\frac{a_k}{b_i}} \ . \tag{17}$$

Cela est valable pour tous les conjugués des ξ_{ik}, qui sont dans K. Or ces ξ_{ik} ont leurs dénominateurs bornés; il existe un nombre naturel $G = G(n, K)$ tel que $|N(\xi_{ik})| \geqslant G^{-1}$ si $\xi_{ik} \neq 0$. Comme $|\mathfrak{X}| \neq 0$, il y a au moins un terme non nul dans ce déterminant:

$$\xi_{1k_1} \xi_{2k_2} \dots \xi_{nk_n} \neq 0 \ , \quad \xi_{ik_i} \neq 0 \quad \text{pour} \quad i = 1, \dots, n \ .$$

Alors

$$| N(\xi_{ik_i}) | \geqslant G^{-1} \ . \tag{18}$$

Les $s_i^{(k)}$, $k = 1, \dots, \gamma$ étant du même ordre de grandeur, il découle de $s_i^{(k)} \geqslant a_i^{(k)} \geqslant \frac{1}{C} \cdot s_i^{(k)}$ que les $a_i^{(k)}$ sont du même ordre de grandeur, pour $k = 1, \dots, \gamma$; il en est de même des $b_i^{(k)}$. On peut donc écrire à cause de (17):

$$| \xi_{ik}^{(\varrho)} | \leqslant c_{15} \sqrt{\frac{a_k^{(\lambda)}}{b_i^{(\mu)}}} \quad \lambda \ , \ \mu \ , \ \varrho \ \text{quelconques} \ . \tag{19}$$

Prenant la norme, il vient à cause de (18):

$$G^{-1} \leqslant c_{15}^{g} \left(\frac{a_{ki}^{(\lambda)}}{b_i^{(\mu)}} \right)^{\frac{g}{2}} .$$

D'où

$$b_i^{(\mu)} \leqslant c_{16} a_{ki}^{(\lambda)} \qquad i = 1, \dots, n \ . \tag{20}$$

Récrivons (15) en mettant des indices supérieurs:

$$\begin{aligned} a_i^{(\lambda)} &\leqslant c_{13} a_j^{(\lambda)} \qquad \text{si} \quad i \leqslant j \ . \\ b_i^{(\mu)} &\leqslant c_{13} b_j^{(\mu)} \qquad \text{si} \quad i \leqslant j \ . \end{aligned} \tag{21}$$

Or $\begin{pmatrix} 1 & \dots & n \\ k_1 & \dots & k_n \end{pmatrix}$ est une permutation des indices $1, \dots, n$. Soit i_0 un indice fixe. Les k_i avec $i \geqslant i_0$ sont tous différents, donc l'un au moins est $\leqslant i_0$; soit par exemple

$$k_j \leqslant i_0 \qquad , \qquad j \geqslant i_0 \ .$$

Alors on a en vertu de (20) et (21):

$$b_{i_0}^{(\mu)} \leqslant c_{13}\, b_j^{(\mu)} \leqslant c_{13}\, c_{16}\, a_{k_j}^{(\lambda)} \leqslant c_{16}\, c_{13}^2\, a_{i_0}^{(\lambda)} \ .$$

Donc

$$b_{i_0}^{(\mu)} \leqslant c_{17}\, a_{i_0}^{(\lambda)} \ .$$

Cela a lieu pour $i_0 = 1, 2, \dots, n$.

Par analogie (on utilise ici le fait que $\mathfrak{X}^{-1}$ a ses dénominateurs bornés) on a évidemment

$$a_i^{(\lambda)} \leqslant c_{17}\, b_i^{(\mu)} \ .$$

Le 2ème lemme est donc démontré.

Pour la suite, nous poserons

$$a_i = a_i^{(1)} \qquad b_i = b_i^{(1)} \ .$$

En tenant compte du 2ème lemme, on peut écrire les inégalités (19) sous la forme

$$| \xi_{ik}^{(\varrho)} | \leqslant c_{18} \sqrt{\frac{a_k}{a_i}} \ . \tag{22}$$

La démonstration du théorème 6′ procède alors par induction sur n de la manière suivante: ce théorème est vrai pour $n = 1$, ce qui résulte par exemple de (22). Supposons qu'il soit vrai pour tous les $t \leqslant n - 1$.

On a d'après (15)

$$a_i \leqslant c_{13}\, a_k \qquad \text{si} \qquad i \leqslant k \ . \tag{23}$$

Soit

$$c_{19} = c_{13}\, c_{18} \sqrt[g]{G} \ .$$

Considérons les quotients $\sqrt{\dfrac{a_i}{a_{i-1}}}$, $i = 2, \dots, n$.

Supposons que

$$\sqrt{\frac{a_n}{a_{n-1}}} \leqslant c_{19} \ , \qquad \sqrt{\frac{a_{n-1}}{a_{n-2}}} \leqslant c_{19} \ , \dots , \qquad \sqrt{\frac{a_{t+2}}{a_{t+1}}} \leqslant c_{19}$$

mais que

$$\sqrt{\frac{a_{t+1}}{a_t}} > c_{19} \ .$$

Cela a certainement lieu pour un $t \leqslant n - 1$.

On a alors pour $i > t$, $j \leqslant t$, d'après (22) et (23):

$$| \xi_{ij}^{(k)} | \leqslant c_{18} \sqrt{\frac{a_j}{a_i}} \leqslant c_{18} \sqrt{\frac{c_{13}^2 a_t}{a_{t+1}}} < \frac{c_{18} c_{13}}{c_{19}} = \frac{1}{\sqrt[g]{G}} .$$

Prenant la norme:

$$| N(\xi_{ij}) | < \frac{1}{G} .$$

Par conséquent

$$\xi_{ij} = 0 \qquad \text{si} \quad i > t, \quad j \leqslant t .$$

La matrice $\mathfrak{X}$ se décompose alors en 4 parties:

$$\mathfrak{X} = \begin{pmatrix} \mathfrak{X}_1 & \mathfrak{X}_2 \\ 0 & \mathfrak{X}_4 \end{pmatrix} \quad \text{où} \quad \mathfrak{X}_1 \text{ est de degré } t .$$

Toutes les conjuguées de la matrice $\mathfrak{X}_4$ sont bornées, car pour $i > t$, $j > t$, on a

$$| \xi_{ij}^{(k)} | \leqslant c_{18} \sqrt{\frac{a_j}{a_i}} \leqslant c_{18} \sqrt{\frac{c_{13}^2 a_n}{a_{t+1}}} \leqslant c_{18} c_{13} c_{19}^{n-t-1} .$$

Il reste à montrer que $\mathfrak{X}_1$ et $\mathfrak{X}_2$ sont bornées. Pour cela décomposons $\mathfrak{S}$ et $\mathfrak{T}$ d'une façon analogue à $\mathfrak{X}$:

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \overline{\mathfrak{S}}_2 \\ \mathfrak{S}_2' & \mathfrak{S}_3 \end{pmatrix} \qquad \mathfrak{T} = \begin{pmatrix} \mathfrak{T}_1 & \overline{\mathfrak{T}}_2 \\ \mathfrak{T}_2' & \mathfrak{T}_3 \end{pmatrix} .$$

A cause de $\mathfrak{S} = \mathfrak{T}[\mathfrak{X}]$, on a

$$\begin{aligned} \mathfrak{S}_1 &= \mathfrak{T}_1[\mathfrak{X}_1] \\ \mathfrak{S}_2 &= \overline{\mathfrak{X}}_1' \mathfrak{T}_1' \mathfrak{X}_2 + \overline{\mathfrak{X}}_1' \mathfrak{T}_2 \mathfrak{X}_4 . \end{aligned} \tag{24}$$

Le théorème 6′ étant par induction supposé vrai pour les systèmes de formes à moins de n variables, on peut l'appliquer aux systèmes des $\mathfrak{S}_1$ et $\mathfrak{T}_1$ liés par $\mathfrak{S}_1 = \mathfrak{T}_1[\mathfrak{X}_1]$, car ces systèmes sont dans $R_0^{(t)}$ comme on l'a vu et $\mathfrak{X}_1$, $\mathfrak{X}_1^{-1}$ ont de même que $\mathfrak{X}$, $\mathfrak{X}^{-1}$ leurs dénominateurs bornés, puisque

$$\mathfrak{X} = \begin{pmatrix} \mathfrak{X}_1 & \mathfrak{X}_2 \\ 0 & \mathfrak{X}_4 \end{pmatrix} \qquad \mathfrak{X}^{-1} = \begin{pmatrix} \mathfrak{X}_1^{-1} & * \\ 0 & \mathfrak{X}_4^{-1} \end{pmatrix} .$$

Les $\mathfrak{X}_1^{(k)}$ sont donc bornées par hypothèse d'induction. On calcule alors $\mathfrak{X}_2$ au moyen de (24):

$$\mathfrak{X}_2 = \mathfrak{T}_1'^{-1}\ \overline{\mathfrak{X}}_1'^{-1}\ (\mathfrak{S}_2 - \overline{\mathfrak{X}}_1'\ \mathfrak{T}_2\ \mathfrak{X}_4) =$$
$$= \mathfrak{X}_1\,\overline{\mathfrak{S}}_1^{-1}\,\mathfrak{S}_2 \qquad - \overline{\mathfrak{T}}_1^{-1}\,\mathfrak{T}_2\ \mathfrak{X}_4\ .$$

On voit que $\mathfrak{X}_2$ est bornée, puisque $\mathfrak{X}_1$ et $\mathfrak{X}_4$ le sont, ainsi que $\overline{\mathfrak{S}}_1^{-1}\,\mathfrak{S}_2$ et $\overline{\mathfrak{T}}_1^{-1}\,\mathfrak{T}_2$, cela en vertu du 1er lemme.

Le théorème 6′ est ainsi démontré, et l'on a vu que le théorème 6 s'en suit.

Conséquence. Soit D un domaine quelconque de l'espace des S. Appelons domaine équivalent à D tout domaine transformé de D par une substitution unimodulaire $\mathfrak{U}$. Nous désignerons par $R_\nu^{(i)}$ les domaines équivalents à R_ν. Il résulte du théorème 6 que:

Les $R_\nu^{(i)}$ touchant un R_μ suivant une portion intérieure à P de sa frontière sont en nombre fini. (P désigne l'espace des systèmes *positifs*.)

§ 8. Forme des domaines R_μ

Théorème 7. Chacun des domaines R_μ, $\mu = 1, \ldots, N$, est l'intérieur d'un angle solide convexe limité par un nombre fini d'hyperplans passant par l'origine de l'espace des S. La portion de la frontière de R_μ située sur la multiplicité $|S| = 0$ a une dimension d'au moins $gn - g_2$ unités inférieure à celle de R_μ.

Nous ne considérons dans ce théorème que les R_μ ayant la dimension $d = \frac{n}{2}\,(ng + g_1)$ de l'espace des S. Les éventuels R_μ de dimension inférieure à d peuvent être laissés de côté, car ils sont équivalents à des portions de frontière de R_ν de dimension d.

Examinons d'abord les points frontières semi-positifs de R_μ. On peut raisonner sur $R(\mathfrak{A}_\mu)$ au lieu de R_μ, car la transformation qui change R_μ en $R(\mathfrak{A}_\mu)$ est linéaire et laisse la multiplicité $|S| = 0$ invariante.

Soit donc S un système frontière de $R(\mathfrak{A}_\mu)$ tel que $|S| = 0$. Le théorème 4 et les inégalités (5) donnent

$$s_1^{(k)^n} \leqslant C^* \mid \mathfrak{S}^{(k)} \mid$$

la constante C^* ne dépendant que de n et de K. Comme $|S| = |\mathfrak{S}^{(1)}| \ldots |\mathfrak{S}^{(\gamma)}| = 0$, il existe un k pour lequel $|\mathfrak{S}^{(k)}| = 0$, d'où $s_1^{(k)} = 0$. D'après (4) § 6 on en déduit que

$$s_1^{(\lambda)} = 0 \quad \text{pour tout} \quad \lambda\ ,$$

et d'après (13) § 7 que

$$s_{1j}^{(\lambda)} = 0 \quad \text{pour tous} \quad j\ ,\ \lambda\ .$$

Ce sont là $ng - g_2$ relations indépendantes entre les coefficients de S. La 2ème partie du théorème 7 est démontrée.

Pour ce qui concerne la 1ère partie, nous savons déjà que R_μ est convexe et limité par des hyperplans passant par l'origine (voir § 5). Il reste à montrer que ces hyperplans sont en nombre fini. Soit H un de ces hyperplans. On peut supposer que la portion de H frontière de R_μ contient des systèmes positifs, car $ng - g_2 \geqslant 2$ (sauf dans le cas banal $n = \gamma = 1$ que nous excluons ici).

L'hyperplan H divise l'espace P des systèmes positifs en 2 régions, dans l'une desquelles R_μ est situé. L'autre de ces régions contient au moins un $R_\nu^{(i)}$ qui touche R_μ suivant H. Les domaines R_μ et $R_\nu^{(i)}$ étant convexes ne peuvent se toucher que suivant l'hyperplan H. Donc l'existence d'une infinité de H serait en contradiction avec la conséquence du théorème 6 énoncée à la fin du § 7.

Remarques

1. *Si $n > 1$, les systèmes semi-positifs de R_μ admettent chacun une infinité de transformations unimodulaires en eux-mêmes.*

En effet, pour un S de $R(\mathfrak{A}_\mu)$ tel que $|S| = 0$ on a $s_{1k}^{(\lambda)} = 0$. Il s'ensuit que toute matrice de la forme $\mathfrak{B} = \begin{pmatrix} 1 & \mathfrak{b}' \\ 0 & \mathfrak{E} \end{pmatrix}$ transforme S en lui-même. Le système T correspondant à S dans R_μ est alors transformé en lui-même par la matrice

$$\mathfrak{C} = \mathfrak{A}_\mu \mathfrak{B} \mathfrak{A}_\mu^{-1} .$$

Il suffit de choisir les composantes de $\mathfrak{b}'$ dans K et divisibles par le déterminant $|\mathfrak{A}_\mu|$ pour que $\mathfrak{C}$ soit unimodulaire dans K. On voit qu'il y a bien une infinité de $\mathfrak{C}$ unimodulaires laissant T invariant.

2. *Le domaine R peut être rendu connexe par un choix convenable des $\mathfrak{A}_\nu$.* En effet, l'espace P des systèmes S positifs est connexe. Or en transformant R par un ensemble complet de représentantes $\mathfrak{U}$ du groupe quotient $\mathfrak{U}|\mathfrak{F}$ (voir § 2) on obtient une infinité de domaines équivalents à R et recouvrant exactement P. Supposons alors que R se compose de deux parties R' et R'' n'ayant aucun point commun, en dehors de 0. Effectuant sur R' et R'' toutes les substitutions de $\mathfrak{U}|\mathfrak{F}$, on obtient des domaines P', P'' qui forment P par leur réunion et qui ont à cause de la connexité de P d'autres points communs que 0; soit S un de ces points, S_1 et S_2 ses équivalents dans R' et R''. On a

$$S = S_1[U_1] = S_2[U_2] \qquad \begin{matrix} S_1 \text{ dans } R', \\ S_2 \text{ dans } R''. \end{matrix}$$

En transformant R'' par $\mathfrak{U}_2 \mathfrak{U}_1^{-1}$, on obtient un domaine équivalent R''' qui a avec R' le point S_1 en commun. En continuant de la sorte, on obtient finalement un domaine R connexe.

§ 9. Application

Les résultats obtenus permettent de démontrer facilement un théorème de Hurwitz sur la structure du groupe unimodulaire dans K:

Théorème. Le groupe unimodulaire de degré n dans K possède un nombre fini d'éléments générateurs, pour lesquels on peut prendre les $\mathfrak{U}_m$ du théorème 6 et les $\omega\mathfrak{E}$.

Soit $\mathfrak{U}$ une substitution unimodulaire dans K. Choisissons un système réduit S_1, et soit S_2 son transformé par $\mathfrak{U}$. Dans l'espace P des S, le segment de droite S_1S_2 rencontre, comme nous le verrons, un nombre *fini* seulement de domaines équivalents à R; soient $R^{(0)} = R$, $R^{(1)}, \ldots, R^{(q)}$ ces domaines dans l'ordre où le segment S_1S_2 les rencontre, et soit $\mathfrak{V}_i$ la substitution unimodulaire transformant R en $R^{(i)}$, $\mathfrak{V}_0 = \mathfrak{E}$, $\mathfrak{V}_q = \mathfrak{U}$.

Les domaines $R^{(i)}$ et $R^{(i+1)}$ se touchent; leurs transformés par $\mathfrak{V}_i^{-1}$ se touchent également: ce sont R et son transformé par $\mathfrak{V}_{i+1}\mathfrak{V}_i^{-1}$. Il s'ensuit que la substitution $\mathfrak{V}_{i+1}\mathfrak{V}_i^{-1}$ appartient dans le groupe quotient $\mathfrak{U}/\mathfrak{F}$ à la même classe que l'une des $\mathfrak{U}_i$ du théorème 6:

$$\mathfrak{V}_{i+1} \equiv \mathfrak{U}_{m_i}\mathfrak{V}_i \pmod{\mathfrak{F}}.$$

De ces relations pour $i = 0, 1, \ldots, q-1$ on déduit que

$$\mathfrak{U} = \mathfrak{V}_q \equiv \mathfrak{U}_{m_{q-1}} \ldots . \mathfrak{U}_{m_1}\mathfrak{U}_{m_0} \pmod{\mathfrak{F}}$$

ce qui démontre le théorème.

Il reste à voir que le segment S_1S_2 rencontre un nombre fini de domaines $R^{(i)}$ équivalents à R. Supposons par absurde que S_1S_2 rencontre une infinité de $R^{(i)}$. Prenons un point du segment S_1S_2 dans chacun de ces $R^{(i)}$. Ces points en nombre infini auraient un point d'accumulation S:

$$S = \lambda S_1 + (1-\lambda) S_2, \quad 0 \leqslant \lambda < 1, \quad |S| > 0.$$

Dans tout voisinage de S il y aurait des points d'une infinité de domaines équivalents à R, ce qui est en contradiction avec le

Lemme: Soit un système S positif, $|S| > 0$. Il existe un voisinage de S ne contenant qu'un nombre fini de portions de domaines équivalents au domaine réduit R.

Distinguons 3 cas pour la démonstration de ce lemme.

I^er cas. *S est intérieur à l'un des R_ν.*

Le domaine R_ν est convexe et limité par un nombre fini d'hyperplans. Soit $r > 0$ la plus petite des distances de S à ces hyperplans. Le voisinage formé par l'intérieur de la sphère $\Sigma(S, r)$ de centre S et de rayon r ne contient que des points de R.

2^ème cas. *S est sur la frontière d'un R_ν.*

D'après le théorème 6 il existe un nombre fini seulement de domaines équivalents à R se touchant en S; les domaines $R_{\nu_i}^{(i)}$ équivalents aux R_ν et sur la frontière desquels S est situé sont donc aussi en nombre fini. Soit $r > 0$ la plus petite des distances de S aux hyperplans en nombre fini limitant ces $R_{\nu_i}^{(i)}$, les hyperplans passant par S exceptés. La sphère $\Sigma(S, r)$ est un voisinage de S convenable.

3^ème cas. *S n'est pas dans R.*

Soit S_1 le système réduit équivalent à S, $\mathfrak{U}$ la substitution unimodulaire transformant S_1 en S. S_1 rentre dans l'un des deux premiers cas. Si V_1 est un voisinage de S_1 ne contenant à son intérieur qu'un nombre fini de portions de domaines équivalents à R, le voisinage V transformé de V_1 par $\mathfrak{U}$ jouira de la même propriété.