Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 23 (1949)

Artikel: Réduction de formes quadratiques dans un corps algébrique fini.
Autor: Humbert, Pierre
DOI: https://doi.org/10.5169/seals-19752

Réduction de formes quadratiques dans un corps algébrique fini

Par Pierre Humbert (†), Lausanne

Introduction

Auf Wunsch der Redaktion möchte ich dieser nachgelassenen Untersuchung von Pierre Humbert zwei erklärende Bemerkungen anfügen:

1. In meiner 1940 in den Abhandlungen des Hamburger Mathematischen Seminars erschienenen Arbeit wird die Reduktionstheorie der indefiniten quadratischen Formen von m Variablen mit ganzen rationalen Koeffizienten in folgender Weise auf die Minkowskische Reduktionstheorie der positiven definiten quadratischen Formen derselben Variablenzahl zurückgeführt. Es sei $\mathfrak{S}$ die Matrix der gegebenen indefiniten Form F und $\mathfrak{H}$ die Matrix einer positiven definiten Form mit reellen Koeffizienten, welche der Bedingung $\mathfrak{S}\mathfrak{H}^{-1}\mathfrak{S} = \mathfrak{H}$ genügt. Wenn F die Signatur $n, m-n$ hat, d. h. reell in eine Summe von n positiven und $m-n$ negativen Quadraten transformierbar ist, so erfüllen jene $\mathfrak{H}$ einen $n(m-n)$-dimensionalen Unterraum H im $\frac{1}{2}m(m+1)$-dimensionalen Raume P der positiven symmetrischen Matrizen $\mathfrak{P}$. Der Minkowskische reduzierte Raum R ist eine gewisse konvexe Pyramide in P, deren Bilder bei Ausführung der sämtlichen verschiedenen unimodularen Transformationen $\mathfrak{P} \to \mathfrak{P}[\mathfrak{U}] = \mathfrak{U}'\mathfrak{P}\mathfrak{U}$ eine lückenlose einfache Überdeckung von P ergeben. Man nennt F reduziert, wenn der Durchschnitt von H mit R nicht leer ist, mit andern Worten, wenn die Gleichung $\mathfrak{S}\mathfrak{H}^{-1}\mathfrak{S} = \mathfrak{H}$ eine Lösung $\mathfrak{H}$ in R besitzt. Da aus dieser Gleichung für $\mathfrak{S}_1 = \mathfrak{S}[\mathfrak{U}]$, $\mathfrak{H}_1 = \mathfrak{H}[\mathfrak{U}]$ die analoge Beziehung $\mathfrak{S}_1\mathfrak{H}_1^{-1}\mathfrak{S}_1 = \mathfrak{H}_1$ folgt, so gibt es zu F mindestens eine äquivalente reduzierte Form. Aus den Eigenschaften von R folgt, daß die Anzahl der reduzierten indefiniten quadratischen Formen von m Variablen mit ganzzahligen Koeffizienten von gegebener Determinante endlich ist; hieraus ersieht man, daß einerseits die Klassenzahl der indefiniten Formen gegebener Determinante und Variablenzahl endlich ist, anderseits zu jeder indefiniten Form nur endlich viele äquivalente reduzierte Formen existieren. Aus letzterer Aussage ergibt sich schließlich, daß die Gruppe $\Gamma(\mathfrak{S})$ der Einheiten von $\mathfrak{S}$, d. h. der ganzzahligen Transformationen von F in sich, aus endlich vielen ihrer Elemente erzeugbar ist.

Diese Resultate werden in der vorliegenden Abhandlung von Pierre Humbert weitgehend verallgemeinert, indem statt des Körpers der rationalen Zahlen ein beliebiger algebraischer Zahlkörper K von endlichem Grade zugrunde gelegt wird. An die Stelle der Minkowskischen Reduktionstheorie tritt dann ihre schöne und wichtige Übertragung auf algebraische Zahlkörper, die Humbert bereits in seiner Thèse durchgeführt hatte. Sind r_1 von den Konjugierten von K reell, $2r_2$ komplex und hat F in den reellen Konjugierten die Signatur $n_k, m-n_k$ $(k = 1, \ldots, r_1)$, so hat man für H das direkte Produkt von r_1 Räumen der Dimensionen $n_k(m-n_k)$ und r_2 Räumen der Dimensionen $\frac{1}{2}m(m-1)$ zu nehmen. Zugleich werden auch die analogen Probleme für hermitische Formen behandelt.

2. Der Raum H geht bei der Abbildung $\mathfrak{H} \to \mathfrak{H}[\mathfrak{V}]$ in sich über, wenn $\mathfrak{V}$ die Matrix einer beliebigen reellen Transformation von F in sich bedeutet. Auf diese Weise erhält man eine Darstellung der „Drehgruppe" $\Omega(\mathfrak{S})$ im Raume H von $n(m-n)$ Dimensionen, in wel-

chem die Einheitengruppe $\Gamma(\mathfrak{S})$ diskontinuierlich ist. Auf H läßt sich ein bei $\Omega(\mathfrak{S})$ invariantes Volumenelement einführen. Sind $\mathfrak{U}_1, \ldots, \mathfrak{U}_g$ die Matrizen von unimodularen Substitutionen, welche die sämtlichen zu F äquivalenten reduzierten Formen $F_1, \ldots, F_g$ in F überführen, und geht bei den entsprechenden Transformationen $\mathfrak{P} \to \mathfrak{P}[\mathfrak{U}]$ der reduzierte Raum R in die Bilder $R_1, \ldots, R_g$ über, so ist der Durchschnitt von H mit $R_1 + \cdots + R_g$ ein Fundamentalbereich von $\Gamma(\mathfrak{S})$ auf H. In meiner erwähnten Arbeit wurde gezeigt, daß das Volumen $v(\mathfrak{S})$ des Fundamentalbereiches endlich ist, wenn von dem trivialen Ausnahmefall einer rational zerlegbaren binären quadratischen Form abgesehen wird. Aus einem Satze, den ich 1943 in den Annals of Mathematics veröffentlicht habe, ergibt sich übrigens, daß H der kleinstdimensionale Wirkungsraum der Drehgruppe ist, in welchem die Einheitengruppe noch diskontinuierlich ist. Das Gruppenmaß $v(\mathfrak{S})$ und einige weitere damit zusammenhängende Folgerungen der Reduktionstheorie sind für die tiefere Untersuchung der analytisch-arithmetischen Eigenschaften indefiniter quadratischer Formen von Bedeutung; man vergleiche etwa meine Arbeit „On the theory of indefinite quadratic forms" in den Annals of Mathematics vom Jahre 1944.

Humbert hatte beabsichtigt, auch den Satz von der Endlichkeit des Gruppenmaßes auf quadratische Formen in beliebigen algebraischen Zahlkörpern zu übertragen; daran wurde er dann leider durch seinen vorzeitigen Tod verhindert. In dem hier nicht abgedruckten unvollständigen sechsten Paragraphen seines Manuskriptes zeigt er noch, daß für $m > 1$ das gesamte Volumen von H unendlich wird, wenn nicht zugleich K total-reell und F total-definit ist. In Verbindung mit der Endlichkeit von $v(\mathfrak{S})$ folgt hieraus die Existenz unendlich vieler Einheiten von F, wenn von den genannten Ausnahmefällen abgesehen wird. Dies läßt sich allerdings auch durch eine elementare Überlegung ableiten.

Carl Ludwig Siegel.

Ce travail est la généralisation d'un mémoire de *M. Siegel*[1]), le corps des nombres rationnels étant remplacé par un corps algébrique fini K. Les résultats de M. Siegel s'étendent facilement, si l'on fait encore appel à ceux de ma thèse. Toutefois, le cas où le corps K possède des conjugués imaginaires a besoin d'un complément important et diffère sur bien des points de celui où K est totalement réel. Le résultat est :

Il existe seulement un nombre fini de classes de formes quadratiques à coefficients entiers dans K et dont la norme du déterminant est donnée.

Dans un corps imaginaire K, identique au corps conjugué complexe, on peut considérer des formes hermitiennes. Quand on passe aux conjugués de K, la symétrie hermitienne ne subsiste que si l'automorphisme faisant passer au conjugué complexe est permutable avec les autres automorphismes du groupe de Galois du plus petit surcorps galoisien de K. Les résultats énoncés sont alors valables pour les formes hermitiennes dans K.

---

[1]) Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität, Bd. 13, 1940.

§ 1. Réduction des systèmes de formes quadratiques définies positives dans K. (Pour ce paragraphe, se référer à ma thèse, désignée dans la suite par T [2].)

Pour généraliser la théorie de la réduction des formes quadratiques définies positives au cas où le groupe discontinu est celui des substitutions unimodulaires dans un corps algébrique K, on considère des systèmes de formes définies positives à m variables associées aux différents conjugués de K. Si K possède g_1 conjugués réels et $2g_2$ conjugués imaginaires, chacun de ces systèmes est formé de g_1 formes quadratiques définies positives associées aux g_1 points à l'infini réels de K et de g_2 formes hermitiennes définies positives associées aux g_2 points à l'infini imaginaires de K. Le système transformé par une substitution $\mathfrak{A}$ à coefficients dans K s'obtient en transformant chacune des formes du système par la substitution conjuguée $\mathfrak{A}^{(k)}$ associée. On appelle substitution unimodulaire dans K une substitution à coefficients entiers de K et dont le déterminant est une unité de K. Deux systèmes sont équivalents si l'un est le transformé de l'autre par une substitution unimodulaire dans K.

Dans chaque classe d'équivalence, il existe un système réduit généralement unique, et l'ensemble de ces systèmes réduits constitue un domaine fondamental du groupe unimodulaire dans l'espace P des systèmes. On obtient le système réduit par deux transformations successives: le système donné S est d'abord transformé par une substitution entière dans K, dont la matrice $\mathfrak{A}$ s'obtient par certaines conditions de minimum. Le système $\dot{S}$ ainsi obtenu est situé dans un domaine R_0 de l'espace P, domaine défini par les inégalités I et II de T. On démontre que la matrice $\mathfrak{A}$ est égale à $\mathfrak{U}\mathfrak{A}_v$ où $\mathfrak{A}_v$ appartient à un ensemble fini de matrices ne dépendant que de m et de K. Le système transformé de $\dot{S}$ par $\mathfrak{A}_v^{-1}$ est le système réduit. Nous désignerons le domaine fondamental ainsi obtenu par R.

Remarque. Soit $\mathfrak{S}$ la matrice d'une forme quadratique ou hermitienne *définie positive*. Considérons une décomposition quelconque de $\mathfrak{S}$ partagée suivant les lignes et les colonnes:

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \mathfrak{S}_{12} \cdots \\ \mathfrak{S}_{21} & \mathfrak{S}_2 \cdots \\ \cdots & \cdots \end{pmatrix},$$

les matrices $\mathfrak{S}_1, \mathfrak{S}_2, \ldots$ en suivant la diagonale principale étant toutes quadratiques. Les déterminants des $\mathfrak{S}_k$ vérifient l'inégalité suivante:

---

[2]) Comment. math. helv. vol. 12, p. 263, 1939/40.

$$|\mathfrak{S}| \leq |\mathfrak{S}_1| . |\mathfrak{S}_2| \ldots , \tag{1}$$

inégalité qu'il suffit évidemment de démontrer dans le cas d'une décomposition de $\mathfrak{S}$ en 4 matrices :

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & \mathfrak{S}_{12} \\ \mathfrak{S}_{21} & \mathfrak{S}_2 \end{pmatrix} .$$

On utilise pour cela l'identité :

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1 & 0 \\ 0 & \mathfrak{T} \end{pmatrix} \begin{bmatrix} \mathfrak{E} & \overline{\mathfrak{S}_1^{-1} \mathfrak{S}_{12}} \\ 0 & \mathfrak{E} \end{bmatrix} \quad \text{avec} \quad \mathfrak{S}_2 = \mathfrak{T} + \mathfrak{S}_1^{-1} [\overline{\mathfrak{S}_{12}}] .$$

Comme $|\mathfrak{S}| = |\mathfrak{S}_1| . |\mathfrak{T}|$, il suffit de démontrer que le déterminant de la somme de 2 matrices positives est au moins égal à chacun des déterminants des matrices composantes. Or cela est évident si l'on utilise le fait que deux matrices définies positives peuvent être mises simultanément sous la forme diagonale.

Soient $\mathfrak{S}^{(k)} = (s_{ij}^{(k)})$ les matrices, symétriques pour $k = 1, 2, \ldots, g_1$, hermitiennes pour $k = g_1 + 1, \ldots, g_1 + g_2$, des formes d'un système S du domaine R_0. Les s vérifient les inégalités suivantes, où, pour simplifier, s_i désigne s_{ii} :

$$s_i^{(\lambda)} \leq c_1 s_j^{(\mu)} \qquad \text{pour } i \leq j ; \ \lambda, \mu \text{ quelconques} \tag{2}$$

$$|s_{ik}^{(\lambda)}| \leq c_2 s_i^{(\lambda)} \tag{3}$$

$$s_1^{(\lambda)} s_2^{(\lambda)} \ldots s_m^{(\lambda)} \leq c_3 |\mathfrak{S}^{(\lambda)}| \tag{4}$$

et où les constantes positives c_1, c_2, c_3 ne dépassent pas certaines bornes fixées par m et K. Appelons $R(c_1, c_2, c_3)$ ou plus simplement $R(c)$ la portion de l'espace P définie par les inégalités (2), (3), (4). Le domaine $R(c)$ contient R_0 sitôt que les constantes c dépassent les bornes mentionnées. Désignons le domaine $R(c)$ par $R^m(c)$ si l'on veut marquer sa dépendance du degré m des matrices $\mathfrak{S}^{(k)}$, c'est-à-dire du nombre des variables des formes quadratiques ou hermitiennes envisagées.

Montrons que si le système S des $\mathfrak{S}^{(k)}$ est situé dans $R^m(c)$, le système obtenu en supprimant dans les matrices $\mathfrak{S}^{(k)}$ les lignes et les colonnes à partir de la n-ième est situé dans $R^n(c)$. Il suffit de faire voir que les coefficients du système ainsi tronqué vérifient les inégalités (2), (3), (4). Or les inégalités (2) et (3) sont valables puisque le système des $\mathfrak{S}^{(k)}$ est dans $R^m(c)$. Quant à (4), on a

$$\frac{s_1 \ldots s_n}{|\mathfrak{S}_n|} = \frac{s_1 \ldots s_m}{|\mathfrak{S}_n| s_{n+1} \ldots s_m} \leq \frac{s_1 \ldots s_m}{|\mathfrak{S}|} \leq c_3 ,$$

cela en vertu de (1).

On peut maintenant énoncer un théorème analogue au théorème 6 de T :

Théorème 1. *Soient* $\mathfrak{S}^{(k)}$ *et* $\mathfrak{T}^{(k)}$ $(k = 1, \ldots, g_1 + g_2)$ *deux systèmes du domaine* $R(c)$, $\mathfrak{A}$ *une matrice non dégénérée à coefficients dans* K, *et* a *un entier rationnel tel que* $a\mathfrak{A}$ *et* $a\mathfrak{A}^{-1}$ *soient entières. Si l'on a* $\mathfrak{S}^{(k)} = \mathfrak{T}^{(k)}[\mathfrak{A}^{(k)}]$ *pour* $k = 1, \ldots, g_1 + g_2$, *les matrices* $\mathfrak{A}^{(k)}$ *et* $\mathfrak{A}^{(k)-1}$ *ont toutes leurs éléments bornés, la borne ne dépendant que de* m, *de* K *et de* a.

La démonstration se fait comme celle du théorème 6 de T. En effet les inégalités I et II ne sont utilisées dans T que sous la forme atténuée des inégalités définissant $R(c)$. En outre le raisonnement par induction sur m est valable d'après la remarque faite avant l'énoncé du théorème 1.

Démontrons ensuite le

Théorème 2. *Soit* $\mathfrak{V}$ *la matrice de la substitution* $x_k \to x_{m-k+1}$. *Si le système positif des* $\mathfrak{S}^{(k)}$ *est situé dans le domaine* $R(c)$, *le système transformé par* $\mathfrak{V}$ *du système des* $\mathfrak{S}^{(k)-1}$ *est situé dans un domaine* $R(c')$, *où les* c' *ne dépendent que de* m *et de* K.

Posons, en supprimant les indices supérieurs

$$\mathfrak{S}^{-1} = (\sigma_{ik}) \ .$$

L'élément σ_{ik} de $\mathfrak{S}^{-1}$ s'obtient en divisant par le déterminant $|\mathfrak{S}|$ le mineur de s_{ki}. Or en évaluant grossièrement ce mineur au moyen de (3) on trouve

$$|\sigma_{ik}| \leq \frac{(m-1)!\, c_2^{m-1}\, s_1 \ldots s_m}{s_i\, |\mathfrak{S}|} \ .$$

En vertu de (4) on obtient

$$|\sigma_{ik}| \leq \frac{c_2'}{s_i} \ . \tag{5}$$

L'inégalité (1) donne

$$\sigma_i\, s_i \geq 1 \ . \tag{6}$$

Les inégalités (2) et (3) pour les éléments de $\mathfrak{S}^{-1}[\mathfrak{V}]$ découlent de (2), (5) et (6) ; les nouvelles constantes c_1 et c_2 sont $c_1 c_2'$ et c_2'. L'inégalité (4) se démontre en remarquant que $|(\sigma_{ik})| = |\mathfrak{S}|^{-1}$ et en tenant compte de (5) et de (1) :

$$\frac{\sigma_1 \ldots \sigma_m}{|(\sigma_{ik})|} \leq \frac{c_2'^m\, |\mathfrak{S}|}{s_1 \ldots s_m} \leq c_2'^m \ .$$

Le théorème 2 est établi.

§ 2. Formes positives attachées à une forme indéfinie

La théorie de la réduction s'applique aux formes indéfinies par l'intermédiaire d'une idée de Hermite. Une forme quadratique indéfinie en les variables x_i peut se ramener par une substitution linéaire à coefficients réels à une somme algébrique de carrés $\sum_{i=1}^{m} \pm z_i^2$. Hermite lui attache la forme définie positive $\sum_{i=1}^{m} z_i^2$, considérée en les variables x_i. Soit $\mathfrak{U}$ la substitution unimodulaire qui effectue la réduction de cette dernière forme quadratique. La transformée de la forme indéfinie initiale par $\mathfrak{U}$ est la „réduite" de Hermite. La décomposition d'une forme indéfinie en somme algébrique de carrés étant possible d'une infinité de manières différentes, il existe une infinité de formes positives attachées de la façon indiquée à la forme indéfinie envisagée ; ces formes constituent, dans l'espace des formes positives, une variété que nous allons étudier. Comme nous aurons à considérer des formes quadratiques à coefficients réels aussi bien qu'imaginaires, ainsi que des formes hermitiennes, nous avons trois cas à distinguer.

Premier cas : Variété attachée à une forme quadratique réelle

Soit $\mathfrak{S}$ la matrice symétrique réelle d'une forme quadratique indéfinie, de signature $(n, m-n)$. La décomposition en une somme algébrique de carrés revient à écrire

$$\mathfrak{S} = \mathfrak{A}' \mathfrak{F} \mathfrak{A}$$

où $\mathfrak{F}$ est la matrice diagonale ayant n fois $+1$ et $m-n$ fois -1 dans sa diagonale principale, et où $\mathfrak{A}$ est une matrice réelle. La matrice de la forme positive attachée à $\mathfrak{S}$ suivant Hermite est alors :

$$\mathfrak{H} = \mathfrak{A}' \mathfrak{A} \ .$$

Cette matrice $\mathfrak{H}$ vérifie la relation

$$\mathfrak{H} \mathfrak{S}^{-1} \mathfrak{H} = \mathfrak{S} \tag{7}$$

et l'on démontre, en s'appuyant sur le fait que deux formes quadratiques dont l'une est positive peuvent se mettre simultanément sous forme diagonale, que réciproquement toute $\mathfrak{H}$ positive et solution de (7) est la matrice d'une forme positive attachée à $\mathfrak{S}$. La variété H étudiée est donc celle des solutions $\mathfrak{H}$ positives de (7). Ainsi qu'il est démontré dans le mémoire cité de Siegel, cette variété H est algébrique, irréductible, et admet la représentation paramétrique biunivoque suivante :

$$\mathfrak{H} = 2\mathfrak{Z} - \mathfrak{S} \quad \text{avec} \quad \mathfrak{Z} = \mathfrak{T}^{-1}[\mathfrak{E}, \mathfrak{Y}'] \qquad \mathfrak{T} = \mathfrak{S}^{-1}\begin{bmatrix}\mathfrak{E}\\ \mathfrak{Y}\end{bmatrix} > 0 \ ,$$

$\mathfrak{Y}$ étant une matrice variable à $m - n$ lignes et à n colonnes, assujettie à la seule condition que $\mathfrak{T}$ soit positive.

Le nombre de dimensions de H est $n\,(m - n)$.

Deuxième cas. Variété attachée à une forme hermitienne

Soit $\mathfrak{S}$ une matrice hermitienne indéfinie, de signature $(n, m - n)$. Elle peut se mettre sous la forme

$$\mathfrak{S} = \mathfrak{A}'\,\mathfrak{F}\,\overline{\mathfrak{A}}$$

où $\mathfrak{F}$ à la même signification que précédemment,

$$\mathfrak{F} = \begin{pmatrix}\mathfrak{E}_n & 0\\ 0 & -\mathfrak{E}_{m-n}\end{pmatrix}$$

et où $\mathfrak{A}$ est une matrice complexe. La matrice positive attachée à $\mathfrak{S}$ est hermitienne et définie par

$$\mathfrak{H} = \mathfrak{A}'\,\overline{\mathfrak{A}} \ .$$

Elle vérifie la relation (7) du premier cas :

$$\mathfrak{H}\,\mathfrak{S}^{-1}\,\mathfrak{H} = \mathfrak{S} \ . \tag{7}$$

Réciproquement, toute solution $\mathfrak{H}$ hermitienne positive de (7) est une des matrices attachées à $\mathfrak{S}$; cela se démontre comme dans le premier cas. La variété H attachée à $\mathfrak{S}$ est algébrique, irréductible, à $n(m - n)$ dimensions complexes, et admet la même représentation paramétrique que dans le premier cas, sauf que $\mathfrak{Y}$ est complexe au lieu d'être réelle.

Troisième cas : Variété attachée à une forme quadratique complexe

Soit $\mathfrak{S}$ une matrice symétrique non dégénérée, à coefficients complexes quelconques. Il n'y a ici rien d'analogue à la signature. Mais il est clair que $\mathfrak{S}$ peut se mettre sous la forme

$$\mathfrak{S} = \mathfrak{A}'\,\mathfrak{A}$$

où $\mathfrak{A}$ est une matrice complexe. Par définition, on attache à $\mathfrak{S}$ la matrice hermitienne définie positive

$$\mathfrak{H} = \mathfrak{A}'\,\overline{\mathfrak{A}}$$

qui vérifie la relation

$$\overline{\mathfrak{H}}\,\mathfrak{S}^{-1}\,\mathfrak{H} = \overline{\mathfrak{S}} \ . \tag{8}$$

Réciproquement, nous allons voir que toute matrice hermitienne positive $\mathfrak{H}$ vérifiant (8) est une matrice attachée à $\mathfrak{S}$ dans le sens indiqué. On s'appuie pour cela sur le

Théorème 3. *Soient $\mathfrak{H}$ une matrice hermitienne positive et $\mathfrak{S}$ une matrice symétrique à coefficients complexes ; il existe une matrice complexe $\mathfrak{A}$ telle que*

$$\mathfrak{A}' \mathfrak{H} \bar{\mathfrak{A}} = \mathfrak{E} \quad \text{et} \quad \mathfrak{A}' \mathfrak{S} \mathfrak{A} = \mathfrak{D} = \text{matrice diagonale.}$$

Nous réservons la démonstration de ce théorème à plus tard pour éviter une interruption.

Soit donc $\mathfrak{H}$ une matrice hermitienne positive vérifiant (8) ; on peut écrire, d'après le théorème 3 :

$$\mathfrak{H} = \mathfrak{A}' \bar{\mathfrak{A}} , \qquad \mathfrak{S} = \mathfrak{A}' \mathfrak{D} \mathfrak{A} .$$

$\mathfrak{D}$ étant une matrice diagonale complexe, et $|\mathfrak{A}| \neq 0$ puisque $\mathfrak{S}$ n'est pas dégénérée. La relation (8) donne

$$\mathfrak{D}^{-1} = \bar{\mathfrak{D}} .$$

Soit $\mathfrak{D}_1$ la matrice dont les éléments sont les racines carrées de ceux de $\mathfrak{D}$, et soit $\mathfrak{B}$ la matrice $\mathfrak{B} = \mathfrak{D}_1 \mathfrak{A}$; on a

$$\mathfrak{H} = \mathfrak{B}' \bar{\mathfrak{B}} \qquad \mathfrak{S} = \mathfrak{B}' \mathfrak{B} \qquad \text{c. q. f. d.}$$

La variété des $\mathfrak{H}$ hermitienne positives attachées à $\mathfrak{S}$ peut donc aussi être définie par l'équation (8).

On peut donner de cette variété la représentation paramétrique suivante : Soit $\mathfrak{A}_0$ une matrice particulière telle que

$$\mathfrak{S} = \mathfrak{A}_0' \mathfrak{A}_0 .$$

Si $\mathfrak{X}$ est une matrice imaginaire vérifiant les conditions de symétrie

$$\mathfrak{X}' = \bar{\mathfrak{X}} = - \mathfrak{X} ,$$

on voit que la matrice

$$\mathfrak{H} = \mathfrak{A}_0' \frac{\mathfrak{E} - \mathfrak{X}}{\mathfrak{E} + \mathfrak{X}} \bar{\mathfrak{A}}_0 \tag{9}$$

est hermitienne et vérifie la relation (8) ; $\mathfrak{H}$ est positive pour un certain domaine D de l'espace des $\mathfrak{X}$. Réciproquement, toute $\mathfrak{H}$ hermitienne positive et vérifiant (8) peut se mettre sous la forme (9), car on tire de (9)

$$\mathfrak{X} = \frac{\mathfrak{E} - \mathfrak{K}}{\mathfrak{E} + \mathfrak{K}} \qquad \text{avec} \qquad \mathfrak{K} = \mathfrak{H} [\mathfrak{A}_0^{-1}]$$

et l'on vérifie que $\mathfrak{X}' = \bar{\mathfrak{X}} = - \mathfrak{X}$.

Remarque. *Le domaine D des* $\mathfrak{X}$ *pour lequel* $\mathfrak{H}$ *est positive peut aussi être défini par la condition que* $\mathfrak{E} + \mathfrak{X}$ *soit positive.*

En effet, supposons tout d'abord $\mathfrak{H}$ positive; alors d'après (9) $(\mathfrak{E} - \mathfrak{X})(\mathfrak{E} + \mathfrak{X})^{-1}$ l'est aussi; soit $\mathfrak{E} + \mathfrak{X} = \mathfrak{Z}$, d'où $\mathfrak{E} - \mathfrak{X} = \mathfrak{Z}'$. On en tire $2\mathfrak{E} = \mathfrak{Z} + \mathfrak{Z}'$. En multipliant par $\mathfrak{Z}^{-1}$, on voit que

$$2\,\mathfrak{Z}^{-1} = \mathfrak{E} + \mathfrak{Z}'\,\mathfrak{Z}^{-1}$$

est positive comme somme de deux matrices positives. $\mathfrak{Z}^{-1}$ étant positive, $\mathfrak{Z}$ et $\mathfrak{Z}'$ le sont aussi.

Supposons maintenant que $\mathfrak{Z} = \mathfrak{E} + \mathfrak{X}$ soit positive; alors $\mathfrak{Z}' = \mathfrak{E} - \mathfrak{X}$ l'est aussi. La matrice

$$\mathfrak{Z}'\,\mathfrak{Z}^{-1} = (\mathfrak{E} - \mathfrak{X})\,(\mathfrak{E} + \mathfrak{X})^{-1}$$

est hermitienne, en vertu des conditions de symétrie que vérifie $\mathfrak{X}$. Or *si deux matrices hermitiennes positives* $\mathfrak{S}$ *et* $\mathfrak{T}$, telles que $\mathfrak{E} - \mathfrak{X}$ et $(\mathfrak{E} + \mathfrak{X})^{-1}$ par exemple, *ont pour produit une matrice hermitienne, cette matrice est positive.* En effet, la condition de symétrie hermitienne s'exprime par

$$\mathfrak{S}\,\mathfrak{T} = \mathfrak{T}\,\mathfrak{S}\ ,$$

on peut transformer $\mathfrak{S}$ et $\mathfrak{T}$ simultanément sous forme diagonale : $\mathfrak{S} = \mathfrak{A}'\,\overline{\mathfrak{A}}$, $\mathfrak{T} = \mathfrak{A}'\,\mathfrak{D}\,\overline{\mathfrak{A}}$; on voit alors que $\mathfrak{D}$ est permutable avec la matrice $\overline{\mathfrak{A}}\,\mathfrak{A}' = \mathfrak{K}$ et que $\mathfrak{S}\,\mathfrak{T}$ a la même signature que $\mathfrak{K}\,\mathfrak{D} = \mathfrak{D}\,\mathfrak{K}$; il suffit donc de montrer que $\mathfrak{K}\,\mathfrak{D}$ est positive. La matrice $\mathfrak{D}$ est diagonale et a ses éléments positifs; on peut supposer qu'ils sont ordonnés par grandeurs croissantes. Décomposons $\mathfrak{K}$ de façon analogue :

$$\mathfrak{K} = \begin{pmatrix} \mathfrak{K}_{11} & \mathfrak{K}_{12} \dots \\ \mathfrak{K}_{21} & \mathfrak{K}_{22} \dots \\ \dots\dots\dots\dots \end{pmatrix}.$$

L'égalité $\mathfrak{K}\,\mathfrak{D} = \mathfrak{D}\,\mathfrak{K}$ donne alors

$$\mathfrak{K}_{ik} = 0 \qquad \text{si } i \neq k\ .$$

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

$$\mathfrak{K} = \begin{pmatrix} \mathfrak{K}_1 & 0 \dots \\ 0 & \mathfrak{K}_2 \dots \\ \dots\dots\dots \end{pmatrix}.$$

Les matrices $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$ sont positives puisque $\mathfrak{K} = \bar{\mathfrak{A}}\,\mathfrak{A}'$ est positive. On en déduit que la matrice

$$\mathfrak{D}\,\mathfrak{K} = \begin{pmatrix} d_1\,\mathfrak{K}_1 & 0 & \ldots \\ 0 & d_2\,\mathfrak{K}_2 \ldots \\ \ldots\ldots\ldots\ldots \end{pmatrix}$$

est aussi positive, c. q. f. d.

La matrice $\mathfrak{X}$ dépend de $\frac{m(m-1)}{2}$ paramètres réels ; ce nombre est la dimension de la variété H attachée à une forme quadratique à coefficients imaginaires. H est donc dans ce cas une variété algébrique irréductible à $\frac{m(m-1)}{2}$ dimensions.

Démonstration du théorème 3. Soit $\mathfrak{H}$ une matrice hermitienne positive et $\mathfrak{S}$ une matrice symétrique non dégénérée à coefficients complexes. On peut transformer $\mathfrak{H}$ en la forme unité au moyen d'une substitution de matrice $\mathfrak{C}$: $\mathfrak{C}'\,\mathfrak{H}\,\bar{\mathfrak{C}} = \mathfrak{E}$. Posons $\mathfrak{C}'\,\mathfrak{S}\,\mathfrak{C} = \mathfrak{T}$. Si $\mathfrak{U}$ est une matrice unitaire, définie par $\mathfrak{U}'\,\bar{\mathfrak{U}} = \mathfrak{E}$, on aura, en posant $\mathfrak{A} = \mathfrak{C}\,\mathfrak{U}$:

$$\mathfrak{A}'\,\mathfrak{H}\,\bar{\mathfrak{A}} = \mathfrak{E} \qquad \mathfrak{A}'\,\mathfrak{S}\,\mathfrak{A} = \mathfrak{U}'\,\mathfrak{T}\,\mathfrak{U}\ .$$

Il suffit donc de démontrer que *l'on peut mettre une matrice symétrique donnée* $\mathfrak{T}$ *sous la forme diagonale au moyen d'une transformation par une matrice unitaire :*

$$\mathfrak{U}'\,\mathfrak{T}\,\mathfrak{U} = \mathfrak{D}\ .$$

Pour cela considérons la matrice hermitienne positive $\bar{\mathfrak{T}}\,\mathfrak{T} = \mathfrak{R}$. On peut la mettre sous forme diagonale au moyen d'une transformation unitaire :

$$\bar{\mathfrak{U}}'\,\mathfrak{R}\,\mathfrak{U} = \mathfrak{D}_1\ .$$

$\mathfrak{D}_1$ est réelle et a ses éléments positifs puisque $\mathfrak{R}$ est positive. On a aussi

$$\mathfrak{U}'\,\bar{\mathfrak{R}}\,\bar{\mathfrak{U}} = \mathfrak{D}_1\ .$$

Formons la matrice

$$\mathfrak{A} = \mathfrak{U}'\,\mathfrak{T}\,\mathfrak{U}\ . \tag{10}$$

On a

$$\mathfrak{A}\,\mathfrak{D}_1 = \mathfrak{D}_1\,\mathfrak{A}\ .$$

La matrice $\mathfrak{A}$ étant permutable avec $\mathfrak{D}_1$, il s'ensuit que $\mathfrak{A}$ est diagonale, pourvu que les éléments de $\mathfrak{D}_1$ soient tous inégaux. Dans ce cas le théorème est démontré en vertu de (10).

Si les éléments de $\mathfrak{D}_1$ ne sont pas tous inégaux, on applique le résultat précédent à la matrice $\mathfrak{T}_\varepsilon = \mathfrak{T} + \varepsilon\,\mathfrak{T}_0$ au lieu de $\mathfrak{T}$; $\mathfrak{T}_0$ est symétrique, et ε réel positif. Soit $\mathfrak{R}_\varepsilon = \overline{\mathfrak{T}}_\varepsilon\,\mathfrak{T}_\varepsilon$. La matrice diagonale obtenue en transformant $\mathfrak{R}_\varepsilon$ par une matrice unitaire $\mathfrak{U}_\varepsilon$ convenable, $\mathfrak{D}_\varepsilon = \overline{\mathfrak{U}}'_\varepsilon\,\mathfrak{R}_\varepsilon\,\mathfrak{U}_\varepsilon$, a ses éléments tous inégaux pour un choix convenable de $\mathfrak{T}_0$, lorsque $\varepsilon \to 0$. En effet, les éléments de $\mathfrak{D}_\varepsilon$ sont les racines caractéristiques de $\mathfrak{R}_\varepsilon$; or le discriminant de l'équation caractéristique $|\,\mathfrak{R}_\varepsilon - x\,\mathfrak{E}\,| = 0$ n'est pas nul quel que soit $\mathfrak{T}_0$, car pour $\mathfrak{T}_0 = \varepsilon^{-1}(\mathfrak{D}^{\frac{1}{2}} - \mathfrak{T})$, où $\mathfrak{D}$ est une matrice diagonale d'éléments positifs tous différents, l'équation caractéristique est $|\,\mathfrak{D} - x\,\mathfrak{E}\,| = 0$. Soit donc $\mathfrak{T}_0$ une matrice pour laquelle le discriminant de $|\,\mathfrak{R}_\varepsilon - x\,\mathfrak{E}\,| = 0$ est non nul quel que soit ε positif assez petit. Comme on l'a vu, on peut alors mettre $\mathfrak{T}_\varepsilon$ sous forme diagonale au moyen d'une matrice unitaire :

$$\mathfrak{U}'_\varepsilon\,\mathfrak{T}_\varepsilon\,\mathfrak{U}_\varepsilon = \mathfrak{D}_\varepsilon\ . \tag{11}$$

Ce résultat ne cesse d'être valable lorsque ε tend vers 0. Dans ces conditions $\mathfrak{T}_\varepsilon$ tend vers $\mathfrak{T}$. D'autre part $\mathfrak{U}_\varepsilon$ qui est unitaire, donc bornée, tend vers une matrice unitaire $\mathfrak{U}$, cela pour une certaine suite dénombrable d'ε. Quant à $\mathfrak{D}_\varepsilon$, elle tend à cause de (11) vers une matrice diagonale $\mathfrak{D}$, et l'on a à la limite $\mathfrak{U}'\mathfrak{T}\mathfrak{U} = \mathfrak{D}$, c. q. f. d.

§ 3. Formes indéfinies dans K et variétés attachées

1. *Cas d'une forme quadratique*

Reprenons le corps K ayant g_1 conjugués réels et $2g_2$ conjugués imaginaires. Soit $\mathfrak{S}$ la matrice symétrique d'une forme quadratique non dégénérée dans K, et soient

$$\mathfrak{S}^{(1)}, \ldots, \mathfrak{S}^{(g)}$$

les g conjugués de $\mathfrak{S}$, qui sont également des matrices symétriques non dégénérées, les $2g_2$ dernières étant en général complexes. Supposons-les numérotées de façon que $\mathfrak{S}^{(k)}$ et $\mathfrak{S}^{(k+g_2)}$ soient imaginaires conjuguées, pour $g_1 < k \leq g_1 + g_2$. A chacune des $\mathfrak{S}^{(k)}$ faisons correspondre la variété des matrices positives $H^{(k)}$ qui lui est attachée, variété qui peut éventuellement se réduire à un seul point si $\mathfrak{S}^{(k)}$ est définie positive ou négative. Le produit direct des $g_1 + g_2$ variétés $H^{(k)}$, $k \leq g_1 + g_2$, est la variété H que nous attacherons à la matrice symétrique $\mathfrak{S}$. Cette variété H doit être considérée comme située dans l'espace P des systèmes positifs, espace qui est le produit direct des espaces des k-ièmes composantes des systèmes. Sa dimension d est la somme des dimensions des variétés $H^{(k)}$, soit

$$d = \sum_{k=1}^{g_1} n_k (m - n_k) + g_2 \frac{m(m-1)}{2}$$

où $(n_k, m - n_k)$ est la signature de $\mathfrak{S}^{(k)}$. La variété H se réduit à un point si $\mathfrak{S}$ est totalement définie, c'est-à-dire si toutes les conjuguées de $\mathfrak{S}$ sont définies positives ou négatives. Cela ne peut toutefois avoir lieu que si le corps K n'a pas de conjugués imaginaires $(g_2 = 0)$.

2. *Cas d'une forme hermitienne*

Si l'on veut considérer des formes hermitiennes dans K, il faut que le corps K soit imaginaire et coïncide avec l'imaginaire conjugué. Dans le passage à un corps conjugué de K, une forme hermitienne $\mathfrak{S} = (s_{ij})$ ne conserve pas nécessairement la symétrie hermitienne caractérisée par la condition $s_{ij} = \bar{s}_{ji}$. Dans quels cas cette symétrie est-elle conservée? Pour le voir envisageons le plus petit corps galoisien $\bar{K}$ surcorps de K. Désignons par $\varkappa$ l'automorphisme de $\bar{K}$ faisant correspondre à chaque nombre de $\bar{K}$ son conjugué complexe. La symétrie hermitienne de la matrice s'exprime par

$$s_{ji} = \varkappa s_{ij} \ .$$

Si $\mathfrak{S}$ doit rester hermitienne dans un corps conjugué σK de K, cela implique

$$\sigma s_{ji} = \varkappa \sigma s_{ij} \ ,$$

c'est-à-dire

$$\sigma \varkappa s_{ij} = \varkappa \sigma s_{ij} \ .$$

Donc: *Si l'automorphisme faisant passer au conjugué complexe est permutable avec les autres automorphismes de $\bar{K}$, les conjuguées d'une matrice hermitienne $\mathfrak{S}$ de K sont aussi hermitiennes.*

Nous supposons qu'il en sera toujours ainsi lorsqu'il s'agira de formes hermitiennes dans un corps K. Dans ce cas le corps K est totalement imaginaire, $g_1 = 0$, et son degré vaut $2g_2$. Soient

$$\mathfrak{S}^{(1)}, \ldots, \mathfrak{S}^{(g_2)}$$

les g_2 premières conjuguées d'une matrice hermitienne $\mathfrak{S}$ dans K, les g_2 autres conjuguées étant les conjuguées complexes de celle-là. Associons à chacune des $\mathfrak{S}^{(k)}$ la variété $H^{(k)}$ qui lui est attachée suivant le § 2, deuxième cas. Le produit direct de ces $H^{(k)}$, $k = 1, \ldots, g_2$, est la variété H attachée à $\mathfrak{S}$. La dimension de H est $\sum_{k=1}^{g_2} 2n_k(m - n_k)$, $(n_k, m - n_k)$ étant la signature de $\mathfrak{S}^{(k)}$. H se réduit à un point si toutes les $\mathfrak{S}^{(k)}$ sont définies.

§ 4. Réduction des formes indéfinies dans K

Soit $\mathfrak{S}$ la matrice d'une forme quadratique ou hermitienne non dégénérée à coefficients dans K. Considérons l'un des systèmes positifs S attachés à $\mathfrak{S}$. Effectuons la réduction de ce système S comme il a été indiqué au § 1, réduction opérée par la substitution unimodulaire $\mathfrak{U}$ de K. La transformation de $\mathfrak{S}$ par $\mathfrak{U}$ donne par définition une *réduite* de $\mathfrak{S}$. En partant d'un autre système S attaché à $\mathfrak{S}$, on peut obtenir une autre réduite. Toutefois le nombre des réduites équivalentes à $\mathfrak{S}$ est fini, en vertu du théorème suivant :

Théorème 4. *Le nombre des formes quadratiques ou hermitiennes à coefficients entiers de K, à m variables, dont la norme du déterminant est donnée et qui sont réduites est fini.*

En effet, soit $\mathfrak{S}$ la matrice de l'une de ces réduites. Il existe un système réduit attaché à $\mathfrak{S}$; soient $\mathfrak{H}^{(k)}$, $k = 1, \ldots, g_1 + g_2$, les matrices de ce système. D'après le § 2 on a les relations

$$\overline{\mathfrak{H}}^{(k)}\, \mathfrak{S}^{(k)-1}\, \mathfrak{H}^{(k)} = \overline{\mathfrak{S}}^{(k)} \quad \text{ou} \quad \mathfrak{H}^{(k)}\, \mathfrak{S}^{(k)-1}\, \mathfrak{H}^{(k)} = \mathfrak{S}^{(k)}$$

suivant les cas. Soit $\mathfrak{A}_v$ la matrice auxiliaire correspondant au système des $\mathfrak{H}^{(k)}$. En transformant $\mathfrak{S}$ et les $\mathfrak{H}$ par $\mathfrak{A}_v^{-1}$, on obtient des matrices $\dot{\mathfrak{S}}$, $\dot{\mathfrak{H}}$ qui vérifient encore les relations écrites, relations qui se mettent aussi sous la forme :

$$\overline{\dot{\mathfrak{H}}}^{-1}[\dot{\mathfrak{S}}] = \dot{\mathfrak{H}} \quad \text{ou} \quad \dot{\mathfrak{H}}^{-1}[\dot{\mathfrak{S}}] = \dot{\mathfrak{H}} \,.$$

D'autre part, le système des $\dot{\mathfrak{H}}$ est situé dans le domaine $R(c)$, et d'après le théorème 2 du § 1 le système des $\dot{\mathfrak{H}}^{-1}$ ou des $\overline{\dot{\mathfrak{H}}}^{-1}$ transformés par $\mathfrak{V}$ est situé dans un domaine $R(c')$. On peut alors appliquer le théorème 1 du § 1, car les domaines $R(c)$ et $R(c')$ sont tous deux contenus dans le domaine $R(c'')$ où $c_i'' = \max(c_i, c_i')$, $i = 1, 2, 3$. Comme $\mathfrak{S} = \dot{\mathfrak{S}}[\mathfrak{A}_v]$ est une matrice entière dans K par hypothèse, on peut prendre pour l'entier rationnel a du théorème 1 le nombre $A^2 N(|\,\mathfrak{S}\,|)$ où A est le plus petit entier rationnel divisible par tous les $|\,\mathfrak{A}_v\,|$. D'après T, théorème 1, l'entier A ne dépend que de m et de K. Les $\dot{\mathfrak{S}}^{(k)}$ possibles étant bornées en vertu du théorème 1 de ce travail, et $A^2\dot{\mathfrak{S}}$ étant entière dans K, les $\dot{\mathfrak{S}}$ sont en nombre fini, et il en est de même des $\mathfrak{S}$. C. q. f. d.

Du théorème 4 découle sans autre le résultat important contenu dans le

Théorème 5. *Le nombre des classes de formes quadratiques définies ou indéfinies, à coefficients entiers dans K, dont la norme du déterminant est donnée et non nulle, est fini. Il en est de même du nombre des classes de formes*

hermitiennes entières dans K, pourvu que la symétrie hermitienne subsiste dans le passage aux corps conjugués.

§ 5. Unités des formes indéfinies dans K

On appelle *unité* d'une forme quadratique ou hermitienne une substitution unimodulaire qui laisse cette forme invariante. Il est clair qu'une forme totalement définie dans K ne possède qu'un nombre fini d'unités. Les unités d'une forme constituent un groupe multiplicatif que nous désignerons par $\Gamma(\mathfrak{S})$.

Considérons une forme quadratique ou hermitienne $\mathfrak{S}$ dans K et sa variété attachée H définie au § 3. La variété attachée à la transformée de $\mathfrak{S}$ par une substitution non dégénérée quelconque $\mathfrak{A}$ est précisément la variété obtenue en transformant H par $\mathfrak{A}$. Il s'ensuit que les unités de $\mathfrak{S}$ transforment la variété H en elle-même. Le groupe $\Gamma(\mathfrak{S})$ des unités de $\mathfrak{S}$ est discontinu dans H ; il y admet un domaine fondamental F que nous allons construire.

Aux réduites de $\mathfrak{S}$ correspondent des variétés équivalentes à H et coupant le domaine réduit R. D'après le théorème 4 il n'y a qu'un nombre fini de pareilles variétés. Soient $\mathfrak{S}_1 = \mathfrak{S}$, $\mathfrak{S}_2 = \mathfrak{S}[\mathfrak{U}_2], \ldots, \mathfrak{S}_t = \mathfrak{S}[\mathfrak{U}_t]$ les différentes réduites de $\mathfrak{S}$, et $H_1, H_2, \ldots, H_t$ les variétés attachées. Désignons par $G_1, G_2, \ldots, G_t$ les domaines communs à R et à $H_1, \ldots, H_t$ respectivement. En transformant ces domaines G_k par les substitutions $\mathfrak{U}_k^{-1}$ correspondantes, on obtient dans la variété H des domaines $D_1 = G_1, D_2, \ldots, D_t$ qui, par leur réunion, constituent un domaine D. Il est facile de voir que tout système S de H possède dans D un système équivalent par une unité de $\mathfrak{S}$. Le domaine D est donc un domaine fondamental pour $\Gamma(\mathfrak{S})$ si deux points *intérieurs* à D dans H ne peuvent être équivalents par une substitution de $\Gamma(\mathfrak{S})$; cela a certainement lieu si la frontière des domaines D_k dans H coïncide avec les portions des D_k obtenues au moyen de la frontière de R. Cela est en général vrai, mais nous n'y insisterons pas. Il nous suffit que le domaine D contienne un domaine fondamental F de $\Gamma(\mathfrak{S})$ dans H.

On peut obtenir les unités d'une forme $\mathfrak{S}$ dans K au moyen des substitutions unimodulaires qui effectuent la réduction de $\mathfrak{S}$. Soient en effet $\mathfrak{U}$ et $\mathfrak{U}^*$ deux substitutions unimodulaires transformant $\mathfrak{S}$ en la même forme réduite $\mathfrak{S}_k$; il est clair que $\mathfrak{U}^* \mathfrak{U}^{-1}$ est une unité de $\mathfrak{S}$. Réciproquement, toute unité peut s'obtenir de cette façon : Le groupe des unités de $\mathfrak{S}$ admet, comme le groupe unimodulaire dans K, un nombre fini d'éléments générateurs.

(Reçu le 9 août 1948.)