

BULLETIN DE LA S. M. F.

J. FAVARD

Sur les formes décomposables et les nombres algébriques

Bulletin de la S. M. F., tome 57 (1929), p. 50-71

http://www.numdam.org/item?id=BSMF_1929__57__50_0

© Bulletin de la S. M. F., 1929, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LES FORMES DÉCOMPOSABLES ET LES NOMBRES ALGÈBRIQUES;

PAR M. J. FAVARD.

Dans les *Disquisitiones arithmeticae* Gauss a posé les problèmes fondamentaux à résoudre pour édifier une théorie arithmétique des formes. Ces problèmes sont les suivants :

1° Réduire une forme donnée, ou encore reconnaître si, étant données deux formes, elles sont équivalentes.

2° Trouver toutes les substitutions automorphes d'une forme ou encore trouver toutes les substitutions permettant de passer d'une forme à une autre équivalente.

3° Trouver les représentations d'un nombre donné par une forme et les représentations d'une forme par une autre.

Un renouveau d'actualité a été donné à ces questions par les belles recherches d'Axel Thue et de ses continuateurs (dans des directions bien différentes) MM. Siegel et Nagell, relatives au troisième problème pour les formes binaires.

Je me suis proposé de résoudre ces problèmes pour les formes décomposables qui me semblent devoir jouer un grand rôle dans la théorie des irrationnelles algébriques. Malheureusement si la résolution des deux premiers problèmes peut être facilement abordée pour ces formes, il n'en est pas de même du troisième pour lequel je n'apporte aucun résultat nouveau et c'est ce problème qui, cependant, a donné lieu à ces recherches.

La méthode employée pour résoudre le premier problème est celle de la réduction continue d'Hermite, rien de nouveau donc : une méthode régulière dont l'application ne présente pas de difficulté et, si je me décide à publier ce travail, c'est à cause de certaines inégalités, rencontrées au cours de ces recherches, et qui, je crois, n'ont pas encore été remarquées. La plus importante et la plus curieuse, à mon avis, peut se déduire sans difficulté des travaux d'Hermite sur les formes binaires et des compléments

importants apportés à cette théorie par M. Julia (¹); cette inégalité est la suivante :

Soient $\xi_1, \xi_2, \dots, \xi_n$, n entiers algébriques conjugués racines d'une même équation irréductible du $n^{\text{ième}}$ degré; parmi ces nombres il y en a un couple au moins (ξ_i, ξ_j) tel que

$$|\xi_i - \xi_j| \geq \sqrt{\frac{3}{2}}.$$

Il est d'abord évident que, parmi ces nombres, il y a un couple tel que $|\xi_i - \xi_j| \geq 1$, car les $\xi_i - \xi_j$ sont des entiers algébriques, mais c'est tout ce que l'on peut dire *a priori* et je n'ai pu trouver de méthode, autre que celle qui va être exposée, pour remplacer 1 par un nombre plus grand (mais inférieur nécessairement à 2 comme le montrent les équations de la division du cercle).

1. — DÉFINITIONS ET PROPOSITIONS PRÉLIMINAIRES.

Dans ce qui va suivre, il s'agira toujours de formes décomposables à coefficients entiers. Soit la forme décomposable de degré m à n indéterminés que nous écrirons

$$\begin{aligned} F(x_1, x_2, \dots, x_n) \\ &= A(\mu_1^{(1)}x_1 + \mu_2^{(1)}x_2 + \dots + \mu_n^{(1)}x_n) \dots (\mu_1^{(m)}x_1 + \dots + \mu_n^{(m)}x_n) \\ &= \sum_{i_1 + i_2 + \dots + i_n = m} A_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = A \mathfrak{M}_1 \mathfrak{M}_2 \dots \mathfrak{M}_m, \end{aligned}$$

la constante A et les facteurs $\mathfrak{M}$ ne sont déterminés qu'à des facteurs près a et t liés par la relation

$$a t_1 t_2 \dots t_m = 1.$$

La forme est dite irréductible dans le domaine de ses coefficients si l'on ne peut la décomposer en un produit de plusieurs autres dont les coefficients sont dans le domaine de rationalité des coefficients de la forme : ici le corps des nombres rationnels; dans le cas contraire la forme est dite réductible.

Nous appellerons les variables $x_1, x_2, \dots, x_n$ variables ou

(¹) JULIA, *Thèse*, Paris, 1917.

décomposable irréductible du $m^{\text{ième}}$ degré a $n > m$ variables apparentes, ces variables ne sont pas essentielles. Dans ce qui va suivre nous supposons donc toujours $n \leq m$ pour les formes irréductibles.

Remarquons aussi qu'en multipliant les $\alpha^{(k)}$ par un même entier du corps $\Omega^{(k)}$, nous pouvons supposer que les facteurs linéaires $\mathcal{N}$ ont pour coefficients des entiers algébriques, le nombre A sera alors rationnel; en posant

$$\mu_1 x_1 + \mu_2 x_2 + \dots + \mu_n x_n = \mu,$$

nous écrirons

$$F(x_1, x_2, \dots, x_n) = A \mathcal{N}(\mu) = A \Pi(\mu_1 x_1 + \dots + \mu_n x_n),$$

où $\mathcal{N}(\mu)$ désigne comme d'habitude la norme de μ .

De même lorsque la forme est réductible on peut faire en sorte que les μ soient des entiers algébriques qui appartiennent à plusieurs corps de degrés inférieurs à m .

Signalons enfin une propriété des formes irréductibles moins évidente que les précédentes :

Les formes représentables par une forme décomposable sont ou bien irréductibles, ou bien, à un facteur constant près, des puissances entières de formes irréductibles.

Une forme est dite représentable par une autre si, en faisant dans la première une substitution de la forme

$$\begin{aligned} x_1 &= a_1 y_1 + a_2 y_2 + \dots + a_p y_p \\ x_2 &= b_1 y_1 + b_2 y_2 + \dots + b_p y_p \\ &\dots\dots\dots \\ x_n &= l_1 y_1 + l_2 y_2 + \dots + l_p y_p, \end{aligned} \quad (p \leq n),$$

on retrouve la deuxième aux notations près.

Les formes représentables par F seront donc de la forme

$$A \cdot \Pi(v_1 y_1 + v_2 y_2 + \dots + v_p y_p);$$

or les nombres $\frac{v_2}{v_1}, \frac{v_3}{v_1}, \dots, \frac{v_n}{v_1}$ étant dans le corps Ω dont ils sont des éléments primitifs ou imprimitifs, le corps qu'ils définissent a donc pour degré m ou un diviseur de m , ce qui démontre le théorème.

2. — RÉDUCTION DES FORMES QUADRATIQUES DÉFINIES.

Je me permettrai de rappeler les résultats de la théorie de la réduction des formes quadratiques définies à n variables, car c'est cette théorie qui est le fondement de la réduction continue que je me propose d'appliquer.

La réduction des formes quadratiques peut être effectuée de plusieurs façons : celle que je vais exposer est indiquée par Hermite dans la troisième de ses lettres à Jacobi sur la théorie des nombres (*Œuvres*, t. I, p. 149).

Soit la forme quadratique définie positive à n variables

$$f = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i x_j \quad (a_{ij} = a_{ji}).$$

Supposons que nous ayons formé l'ensemble (f) de toutes les formes équivalentes à f , c'est-à-dire l'ensemble des formes que l'on déduit de f par une substitution modulaire.

Dans (f) nous allons choisir la réduite de f par le procédé suivant :

1° Prenons dans (f) toutes les formes où a_{11} a la plus petite valeur possible : cela se peut car, comme nous le verrons plus loin, l'ensemble des a_{11} n'est dense nulle part.

2° Parmi ces formes, conservons seulement celles où a_{22} est minimum et continuons ainsi pour $a_{33}, \dots, a_{nn}$, nous arriverons finalement à un ensemble de formes dont les coefficients des carrés seront les mêmes. Ces formes seront d'ailleurs telles que toutes les formes à deux variables que l'on peut en déduire en égalant $n - 2$ quelconques des variables à zéro seront réduites ; car si, par exemple, la forme

$$(a_{ii}, a_{ij}, a_{jj}) = a_{ii}x_i^2 + 2a_{ij}x_ix_j + a_{jj}x_j^2$$

de discriminant

$$\Delta_{ij} = a_{ii}a_{jj} - a_{ij}^2$$

n'était pas réduite, on pourrait diminuer la valeur d'un des coefficients a_{ii} ou a_{ij} sans altérer les autres par une substitution modulaire portant seulement sur x_i et x_j .

Alors, dans le dernier ensemble des formes obtenues, qui ne

comprend qu'un nombre fini de formes comme nous le montrons plus loin, nous extrairons :

1° Les formes où le discriminant Λ_{12} de la formule (a_{11}, a_{12}, a_{22}) est minimum.

2° Parmi les formes restantes nous choisirons celles où Λ_{13} est aussi minimum et ainsi de suite dans l'ordre

$$\begin{array}{cccc} \Lambda_{12}, & \Lambda_{13}, & \dots, & \Lambda_{1n}, \\ & \Lambda_{23}, & \dots, & \Lambda_{2n}, \\ & \dots, & \dots, & \dots, \\ & \Lambda_{j,j+1}, & \dots, & \Lambda_{j,n}, \\ & \dots, & \dots, & \dots, \\ & & & \Lambda_{n-1,n}. \end{array}$$

On arrivera ainsi, peut-être avant la dernière opération indiquée, à un ensemble de formes offrant des valeurs égales pour les Λ_{ij} .

Mais, comme les coefficients des carrés de ces formes sont déjà égaux, il résulte de l'expression de Λ_{ij} que les coefficients des termes rectangles de ces formes ne pourront différer que par le signe; par conséquent le dernier ensemble obtenu ne contiendra qu'un nombre limité de formes.

Dans ce dernier ensemble, il y en a une, si $n > 2$, telle que a_{12} est non négatif, car en changeant x_2 en $-x_2$ et x_3 en $-x_3$, par exemple, on change a_{12} en $-a_{12}$ et a_{13} en $-a_{13}$ sans altérer les autres coefficients. Si donc nous avons obtenu plusieurs formes en dernier lieu (ce qui arrivera nécessairement, si les a_{ij} ne sont pas tous nuls, lorsque $n > 2$), nous choisirons parmi celles-ci, celles où a_{12} est non négatif; puis parmi les formes restantes celles où a_{13} est non négatif si c'est nécessaire et ainsi de suite dans l'ordre ⁽¹⁾

$$\begin{array}{cccc} a_{12}, & a_{13}, & \dots, & a_{1n}, \\ & a_{22}, & \dots, & a_{2n}, \\ & \dots, & \dots, & \dots, \\ & a_{j,j+1}, & \dots, & a_{j,n}, \\ & \dots, & \dots, & \dots, \\ & & & a_{n-1,n} \end{array}$$

(1) La dernière opération ne sera nécessaire que dans le cas où

$$a_{n-1,n-1} = -a_{n-1,n} = a_{n,n}.$$

et l'on aura bien ainsi une réduite unique; par suite, on pourra reconnaître si deux formes données sont équivalentes, en comparant leurs réduites : c'est là le but de la réduction des formes.

Représentation géométrique. — Ce mode de réduction est susceptible d'une représentation géométrique intéressante donnée par Minkowski et déjà utilisée par Lejeune-Dirichlet dans le cas des formes ternaires.

Construisons dans l'espace euclidien à n dimensions le parallélépipède dont les arêtes ont pour longueur $\sqrt{a_{ii}}$, l'angle des deux arêtes i et j ayant pour cosinus $\pm \frac{a_{ij}}{\sqrt{a_{ii} \times a_{jj}}}$: cela est toujours possible si nous supposons que la forme est à variables essentielles; le parallélépipède ainsi obtenu représentera la forme. Divisons alors l'espace en cellules égales à ce parallélépipède, ce qui se fait en menant des plans parallèles entre eux et aux faces du parallélépipède initial, nous obtenons ainsi une grille de points et le carré de la distance de deux points quelconques de cette grille est un nombre représentable par la forme et réciproquement. Les parallélépipèdes qui représentent les formes équivalentes à celle d'où l'on est parti, ont tous le même volume (égal à la racine carrée du discriminant de la forme) et leurs sommets sont des points de la grille.

La réduction revient à chercher :

- 1° Les parallélépipèdes dont la longueur des arêtes est la moindre.
- 2° A choisir parmi ceux-ci ceux où l'aire du parallélogramme formé par deux arêtes est la moindre.

Cette représentation nous montre d'abord que l'ensemble des coefficients a_{ii} n'est dense nulle part puisque les a_{ii} sont représentables par la forme et qu'après la première suite d'opérations il ne restera plus qu'un nombre fini de formes.

Désignant alors par D le discriminant de la forme et par α_{ij} les coefficients de la réduite, Minkowski a trouvé, en appliquant ses procédés de géométrie des nombres ⁽¹⁾,

$$\alpha_{11} \alpha_{22} \dots \alpha_{nn} \leq \left(\frac{2^n}{\sqrt{V}} \right)^2 D,$$

⁽¹⁾ Pour la démonstration, voir la *Geometrie der Zahlen* de Minkowski ou les *Leçons sur la Théorie des nombres* de M. Châtelet.

où V désigne le volume de l'hypersphère de rayon 1 dans l'espace à n dimensions

$$V = \frac{\Gamma\left(1 + \frac{n}{2}\right)}{\left[\Gamma\left(\frac{1}{2}\right)\right]^n}.$$

Hermite avait trouvé par une autre méthode

$$x_{11} x_{22} \dots x_{nn} \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} D.$$

La valeur de Minkowski est préférable pour les grandes valeurs de n , celle d'Hermite est plus simple et plus petite aussi lorsque $n < 5$.

Nous emploierons tantôt l'une, tantôt l'autre des deux limitations et, lorsque nous ne préciserons pas, nous écrirons

$$x_{11} x_{22} \dots x_{nn} \leq K^n \cdot D.$$

D'ailleurs, pour les formes réduites, on a aussi

$$|2 x_{ij}| \leq x_{ii} \quad \text{et} \quad x_{ji}$$

et

$$x_{11} x_{22} \dots x_{nn} \geq D.$$

3. — RÉDUCTION CONTINUELLE DES FORMES DÉCOMPOSABLES.

Nous pouvons nous borner au cas où le nombre n des indéterminées essentielles ne dépasse pas le degré de la forme et ne considérer que des formes irréductibles car, pour les formes réductibles, il faut d'abord constater l'équivalence des facteurs; d'ailleurs la méthode nous donnera aussi la réduction de certaines formes réductibles.

Le but de ce paragraphe est donc de montrer qu'on peut faire correspondre à chaque *forme irréductible* un nombre fini de formes que nous appellerons les *réduites*.

Écrivons la forme décomposable irréductible à n variables essentielles

$$F(x_1, x_2, \dots, x_n) = A \prod_{i=1}^m (\mu_1^{(i)} x_1 + \mu_2^{(i)} x_2 + \dots + \mu_n^{(i)} x_n) \quad (m \geq n)$$

et avec les quantités réelles T_i supposons que l'on ait formé la forme quadratique définie positive

$$\Phi(x_1, x_2, \dots, x_n) = \sum_{i=1}^m T_i^2 [\mu_1^{(i)} x_1 + \mu_2^{(i)} x_2 + \dots + \mu_n^{(i)} x_n]^2$$

que nous appellerons l'*associée* de la forme F.

Imaginons que l'on donne aux quantités $T_1, T_2, \dots, T_m$ des valeurs déterminées et réduisons dans ce cas la forme Φ , ce qui s'obtiendra en faisant sur elle une substitution modulaire, soit

$$S = \begin{pmatrix} a_1^{(1)} & a_2^{(1)} & \dots & a_n^{(1)} \\ a_1^{(2)} & a_2^{(2)} & \dots & a_n^{(2)} \\ \dots & \dots & \dots & \dots \\ a_1^{(m)} & a_2^{(m)} & \dots & a_n^{(m)} \end{pmatrix},$$

nous ferons sur F la même substitution et nous obtiendrons une forme SF équivalente à F.

Ensuite nous supposons que l'on donne aux (T) tous les systèmes de valeurs possibles et que, pour chacun de ces systèmes, on opère comme nous venons de le dire : on obtiendra ainsi un ensemble de transformées de F que nous désignerons par (F).

Une première étude s'impose donc :

Soit f une forme équivalente à F, quelles seront les propriétés relatives des deux ensembles (f) et (F).

Nous allons montrer que (f) et (F) sont composés des mêmes formes. Soit en effet

$$\Sigma = \begin{pmatrix} x_1^{(1)} & x_2^{(1)} & \dots & x_n^{(1)} \\ x_1^{(2)} & x_2^{(2)} & \dots & x_n^{(2)} \\ \dots & \dots & \dots & \dots \\ x_1^{(m)} & x_2^{(m)} & \dots & x_n^{(m)} \end{pmatrix}$$

une substitution modulaire capable de transformer F en f ; on a alors

$$f = \text{Al}(m_1 x_1 + m_2 x_2 + \dots + m_n x_n)$$

en posant

$$m_i = \mu_1 x_1^{(i)} + \mu_2 x_2^{(i)} + \dots + \mu_n x_n^{(i)}$$

et la forme φ associée de f sera

$$\varphi = \Sigma T_i^2 [m_1 x_1 + m_2 x_2 + \dots + m_n x_n]^2$$

Si dans Φ et φ nous faisons maintenant $T_i = t_i$ on voit que les deux formes Φ et φ sont équivalentes ($\varphi = \Sigma \Phi$) et par suite qu'elles ont la même réduite, donc (f) est contenu dans (F) et l'on montre de la même façon que (f) contient (F) ; donc (f) et (F) sont identiques.

C'est parmi les formes de l'ensemble (F) que nous choisirons une réduite pour représenter toute la classe définie par (F) .

Posons, par exemple,

$$\Phi(x_1, x_2, \dots, x_n) = \sum_{i,j=1}^n \alpha_{ij} x_i x_j \quad (\alpha_{i,j} = \alpha_{j,i}),$$

on a

$$\begin{aligned} \alpha_{ii} &= \sum_j T_j^2 |\mu_i^{(j)}|^2, \\ \alpha_{ij} &= \frac{1}{2} \sum_k T_k^2 (\mu_i^{(k)} \bar{\mu}_j^{(k)} + \bar{\mu}_i^{(k)} \mu_j^{(k)}), \end{aligned}$$

où $\bar{\mu}$ désigne la quantité conjuguée de μ .

Désignons par Δ le déterminant de Φ et remarquons que, puisque la forme est irréductible, aucune des quantités

$$M_i^{(j)} = \mu_1^{(j)} \alpha_i^{(1)} + \dots + \mu_n^{(j)} \alpha_i^{(n)}$$

n'est nulle; après S il vient en désignant par A_{ij} le coefficient de $x_i x_j$

$$A_{ii} = \sum_j T_j^2 |M_i^{(j)}|^2$$

et l'on sait par la théorie des formes quadratiques que l'on a d'abord

$$A_{ii} \leq K \sqrt[n]{\Delta},$$

c'est-à-dire

$$T_1^2 |M_1^{(1)}|^2 + T_2^2 |M_1^{(2)}|^2 + \dots + T_m^2 |M_1^{(m)}|^2 \leq K \sqrt[n]{\Delta}.$$

En écrivant maintenant que la moyenne arithmétique d'un ensemble de nombres positifs n'est pas surpassée par leur moyenne géométrique, on obtient l'inégalité

$$T_1^2 T_2^2 \dots T_m^2 \{\sum \mathcal{U}(M_i)\}^2 \leq \left(\frac{1}{m} K \sqrt[n]{\Delta}\right)^m.$$

Posons pour simplifier

$$(T)^2 = T_1^2 T_2^2 \dots T_m^2,$$

on a

$$\{\mathcal{U}(M_1)\}^2 \leq \frac{\Delta^m}{(T)^2} \left(\frac{K}{m}\right)^m;$$

pour condenser encore la formule nous poserons

$$\Theta = \frac{\Delta^m}{(T)^2},$$

on aura

$$\{\mathcal{U}(M_1)\}^2 \leq \Theta \left(\frac{K}{m}\right)^m.$$

A l'aide de cette limitation nous allons maintenant borner les quantités $\left|\frac{M_k^{(i)}}{M_1^{(i)}}\right|$ par le procédé suivant : en supprimant le terme $T_i^2 |M_1^{(i)}|^2$ dans l'expression de A_{11} , la somme des termes restants est plus petite que A_{11} et leur produit est par suite plus petit que $\left(\frac{A_{11}}{m-1}\right)^{m-1}$, ce qui s'écrit

$$\frac{(T)^2 \{\mathcal{U}(M_1)\}^2}{T_i^2 |M_1^{(i)}|^2} \leq \left(\frac{A_{11}}{m-1}\right)^{m-1};$$

mais d'autre part on a évidemment

$$T_i^2 |M_k^{(i)}|^2 \leq A_{kk},$$

d'où l'on déduit

$$(T)^2 \{\mathcal{U}(M_1)\}^2 \left\{ \left| \frac{M_k^{(i)}}{M_1^{(i)}} \right| \right\}^2 \leq A_{11}^{m-1} A_{kk} \frac{1}{(m-1)^{m-1}}.$$

En remplaçant et en réduisant dans l'inégalité précédente

$$A_{kk} \leq \frac{K^n \Delta}{A_{11}^{n-1}}.$$

Mais, puisque $S\Phi$ est réduite

$$\left| \frac{M_k^{(i)}}{M_1^{(i)}} \right|^2 \leq \Theta K^m \frac{1}{(m-1)^{m-1} \{\mathcal{U}(M_1)\}^2}.$$

En opérant comme précédemment, on trouve aussi

$$\{\mathcal{U}(M_i)\}^2 \leq \frac{(A_{ii})^m}{(T)^2} \frac{1}{m^m},$$

d'où, par multiplication, et en tenant compte de

$$\begin{aligned} \Lambda_{11} \Lambda_{22} \dots \Lambda_{nn} &\leq K^n \Delta, \\ \mathfrak{N}(M_1)^2 \cdot \mathfrak{N}(M_2)^2 \dots \mathfrak{N}(M_n)^2 &\leq \left\{ \Theta \left(\frac{K}{m} \right)^m \right\}^n. \end{aligned}$$

Cette inégalité est à rapprocher de celle que l'on vient d'employer dans le cas d'une forme quadratique réduite.

On pourrait établir un grand nombre d'inégalités de ce genre ⁽¹⁾ mais nous n'irons pas plus loin dans cet ordre d'idées, car ce qui vient d'être fait nous fournit déjà ce résultat important : *Tous les coefficients de la forme sont limités au moyen de la seule fonction Θ , ce qui nous conduit à en faire l'étude.*

Tout d'abord nous avons vu que les formes quadratiques qui correspondent à deux formes équivalentes étaient équivalentes pour des valeurs égales des indéterminées T sous la forme où nous les avons prises; par conséquent pour de telles valeurs des T et pour des formes équivalentes la fonction Θ prend la même valeur.

Ensuite, comme nous nous sommes proposé de définir les réduites, il sera avantageux de prendre pour réduites des formes à coefficients les plus petits possibles : nous chercherons donc s'il peut exister un minimum pour la fonction Θ des variables $T_1, T_2, \dots, T_m$.

Supposons, pour un instant, l'existence de ce minimum non nul (nous reviendrons tout à l'heure sur cette question), soit D , nombre que nous appellerons le *déterminant* de la forme. Soit Φ les formes quadratiques qui correspondent aux valeurs des T qui donnent le minimum de Θ : avec Hermite nous appellerons ces formes les *correspondantes quadratiques de F* ⁽²⁾. Nous nommerons aussi formes *décomposables* du $m^{\text{ième}}$ degré à n indéterminées de même *déterminant*, l'ensemble des formes pour lesquelles le minimum *absolu* de la fonction Θ aura la même valeur.

Nous sommes maintenant en mesure de définir *la ou les réduites* d'une forme F : ce seront les formes de l'ensemble (F) auxquelles correspond le minimum de la fonction Θ et, d'après ce que

⁽¹⁾ Pour les formes binaires, voir notamment HERMITE, *Sur l'introduction des variables continues dans la théorie des nombres* (*Œuvres*, t. I, p. 171).

⁽²⁾ Il faut remarquer que Θ peut être constant lorsque $m = n$, nous prendrions alors pour correspondante de F une forme Φ quelconque.

l'on vient de voir, deux formes équivalentes auront les mêmes réduites (1).

Puisque nous supposons les formes à coefficients entiers, les coefficients des réduites de même déterminant seront tous (à un facteur près) limités en valeur absolue. Nous arrivons donc au résultat suivant :

Les formes décomposables irréductibles à coefficients entiers et de déterminant donné ou inférieur à une limite donnée se distribuent en un nombre fini de classes.

Venons maintenant à la question que nous avons laissée en suspens : l'existence du minimum de la fonction Θ dont dépend la réduction. Remarquons d'abord que la fonction Θ positive est continue par rapport aux variables T si aucune de celles-ci n'est nulle; puisque la forme est irréductible, elle ne peut représenter zéro (2) alors l'inégalité

$$1 \leq \left| \mathfrak{N}(\mathfrak{M}_1) \right|^{1/m} \leq \Theta \left(\frac{K}{m} \right)^m$$

montre que

$$\Theta \geq \left(\frac{m}{K} \right)^m.$$

Développons d'autre part Δ

$$\Delta = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} \sum_{j=1}^m T_j^2 \{ \alpha_j^j \}^2 & \frac{1}{2} \sum_{j=1}^m T_j^2 (\alpha_1^j \bar{\alpha}_2^j + \bar{\alpha}_1^j \alpha_2^j) & \dots \\ \dots & \dots & \dots \\ \frac{1}{2} \sum_{j=1}^m T_j^2 (\alpha_1^j \bar{\alpha}_n^j + \bar{\alpha}_1^j \alpha_n^j) & \dots & \dots \end{vmatrix},$$

(1) Les raisonnements précédents et ceux qui suivront relativement à l'existence du minimum de Θ ne supposent nullement entiers les coefficients de la forme.

(2) Pour des valeurs non toutes nulles des indéterminées, la méthode de réduction s'appliquera donc aux formes décomposables réductibles qui ne peuvent représenter zéro.

d'où

$$\Delta = \sum_{(i_1, i_2, \dots, i_n)} T_{i_1}^2 T_{i_2}^2 \dots T_{i_n}^2 \Delta(i_1, i_2, \dots, i_n),$$

la sommation étant faite par rapport aux combinaisons des indices $i_1, i_2, \dots, i_n$, chaque indice correspondant à un corps imaginaire pouvant être répété deux fois au plus; quant à la valeur de $\Delta(i_1, i_2, \dots, i_n)$ elle s'obtient en remplaçant par zéro dans Δ tous les T dont l'indice n'est pas égal à l'un des $i_1, \dots, i_n$; en revenant à Φ cela veut dire que l'on prend le déterminant de la forme

$$\Phi(i_1, i_2, \dots, i_n) = \sum_{j=1}^n T_{ij}^2 [\mu_1^{(ij)} x_1 + \mu_2^{(ij)} x_2 + \dots + \mu_n^{(ij)} x_n]^2.$$

d'où

$$\Delta(i_1, i_2, \dots, i_n) = \text{module} \begin{vmatrix} \mu_1^{(i_1)} & \mu_2^{(i_1)} & \dots & \mu_n^{(i_1)} \\ \mu_1^{(i_2)} & \mu_2^{(i_2)} & \dots & \mu_n^{(i_2)} \\ \dots & \dots & \dots & \dots \\ \mu_1^{(i_n)} & \mu_2^{(i_n)} & \dots & \mu_n^{(i_n)} \end{vmatrix}^2.$$

lorsque les μ_i sont réels.

Or on peut évidemment borner inférieurement et supérieurement les Δ puisqu'ils sont en nombre fini, et écrire

$$\alpha^n \leq \Delta(i_1, i_2, \dots, i_n) \leq A^n,$$

il viendra alors

$$\alpha^n \sum_{i_1, \dots, i_n} T_{i_1}^2 T_{i_2}^2 \dots T_{i_n}^2 \leq \Delta \leq A^n \sum_{i_1, i_2, \dots, i_n} T_{i_1}^2 T_{i_2}^2 \dots T_{i_n}^2.$$

où, à gauche, on peut se borner aux combinaisons sans répétition. Si l'on peut prendre $\alpha > 0$, ce qui revient à supposer qu'aucun des déterminants $\Delta(i_1, i_2, \dots, i_n)$ n'est nul ($i_j \neq i_k$), on aura, en remarquant que la moyenne géométrique des termes de la somme est $[(T)^2]^{\frac{n}{m}}$,

$$\Delta \geq \alpha^n C_m^n [(T)^2]^{\frac{n}{m}},$$

d'où

$$\Theta \geq \alpha^m \left\{ \frac{m!}{n! (m-n)!} \right\}^{\frac{m}{n}};$$

dans ce cas aussi on a une limite inférieure pour Θ .

D'autre part, comme Θ est une fonction continue des T et qu'on peut la borner par l'un ou l'autre des procédés que nous venons d'employer, elle atteint nécessairement son minimum pour des valeurs des T que l'on pourra calculer dans chaque cas particulier; d'ailleurs Θ devient infinie, comme on le voit facilement, si quelques-uns des T tendent vers zéro, les autres restant finis. Pour trouver ce minimum on pourra, par exemple, poser $(T)^2 = 1$ et l'on n'aura à faire que des calculs algébriques. Le minimum D de Θ sera donc un nombre algébrique et, si l'on suppose que le coefficient de la plus haute puissance de l'équation qui le définit est l'unité, on voit que les coefficients de cette équation seront des invariants de la forme F puisque deux formes équivalentes ont les mêmes réduites et par suite la même équation en D .

4. — UNE INÉGALITÉ RELATIVE AUX NOMBRES ALGÈBRIQUES.

Si l'on cherche, comme on a le droit de le faire, le minimum de la fonction $\Theta (= D)$ en supposant $(T)^2 = 1$, on est ramené à chercher le minimum de Δ sous cette même condition; or ce minimum ne peut dépasser la valeur que prend Δ lorsque tous les T sont égaux à 1. Dans ce cas une borne supérieure de Δ est facile à trouver pour $n = 2$ ou 3; en général nous décomposerons Δ en la somme de $(2m)^n$ déterminants dont je n'écris que l'un d'eux :

$$\begin{vmatrix} \frac{1}{2} \mu_1^{(i_1)} \overline{\mu_1^{(i_1)}} & \frac{1}{2} \mu_2^{(i_1)} \overline{\mu_1^{(i_1)}} & \dots & \frac{1}{2} \mu_n^{(i_1)} \overline{\mu_1^{(i_1)}} \\ \frac{1}{2} \mu_1^{(i_2)} \overline{\mu_2^{(i_2)}} & \frac{1}{2} \mu_2^{(i_2)} \overline{\mu_2^{(i_2)}} & \dots & \frac{1}{2} \mu_n^{(i_2)} \overline{\mu_2^{(i_2)}} \\ \dots & \dots & \dots & \dots \\ \frac{1}{2} \mu_1^{(i_n)} \overline{\mu_n^{(i_n)}} & \frac{1}{2} \mu_2^{(i_n)} \overline{\mu_n^{(i_n)}} & \dots & \frac{1}{2} \mu_n^{(i_n)} \overline{\mu_n^{(i_n)}} \end{vmatrix} \\ = \frac{1}{2^n} \overline{\mu_1^{(i_1)} \mu_2^{(i_2)} \dots \mu_n^{(i_n)}} \begin{vmatrix} \mu_1^{(i_1)} & \mu_2^{(i_1)} & \dots & \mu_n^{(i_1)} \\ \mu_1^{(i_2)} & \mu_2^{(i_2)} & \dots & \mu_n^{(i_2)} \\ \dots & \dots & \dots & \dots \\ \mu_1^{(i_n)} & \mu_2^{(i_n)} & \dots & \mu_n^{(i_n)} \end{vmatrix}.$$

Tous les déterminants qui contiennent le dernier déterminant écrit au facteur sont au nombre de $n!$ et leur somme est visiblement égale au carré du module du dernier déterminant; d'ailleurs

certaines sont nuls. Désignant, à partir de maintenant, par A^n le maximum des modules des carrés de ces différents déterminants on a

$$\min_{[(T)^2=1]} \Delta \leq A^n \frac{m^n}{n!},$$

donc

$$D \leq A^m \cdot \frac{m^m}{(n!)^n};$$

d'autre part, pour la forme réduite,

$$|\mathcal{U}(M_1)|^2 \leq D \left(\frac{K}{m} \right)^m,$$

et comme la forme ne peut représenter zéro $|\mathcal{U}(M_1)| > 1$, donc on a

$$A \geq \frac{m}{K} \cdot \frac{(n!)^n}{m}$$

ou encore

$$A^n \geq \frac{n!}{K^n},$$

inégalité qui exprime une propriété des nombres algébriques et de leurs conjugués :

Soient $\mu_1^{(i)}, \mu_2^{(i)}, \dots, \mu_n^{(i)}$, n entiers algébriques linéairement indépendants d'un corps algébrique de degré m et de ses conjugués : il existe un minimum indépendant de m pour

$$\max_{(i_1, i_2, \dots, i_n = 1, 2, \dots, m)} \Delta(i_1, i_2, \dots, i_n) = \text{module} \begin{vmatrix} \mu_1^{(i_1)} & \mu_2^{(i_1)} & \dots & \mu_n^{(i_1)} \\ \mu_1^{(i_2)} & \mu_2^{(i_2)} & \dots & \mu_n^{(i_2)} \\ \dots & \dots & \dots & \dots \\ \mu_1^{(i_n)} & \mu_2^{(i_n)} & \dots & \mu_n^{(i_n)} \end{vmatrix}^2,$$

ce minimum croît d'ailleurs avec n .

Le cas $m = n$ est fort connu, il contient le théorème de Hermite : le nombre des corps dont le module du discriminant ne dépasse pas une limite donnée est fini.

Prenons le cas où $n = 2$ et prenons alors $K_{(1)}^2 = \frac{4}{3}$, il vient

$$A \geq \sqrt{\frac{3}{2}}.$$

Un cas particulier extrêmement intéressant est celui où l'on fait $\mu_1 = 1$, $\mu_2 = \zeta$, nombre algébrique entier quelconque; on en déduit :

Étant donnés m entiers algébriques conjugués : $\xi_1, \xi_2, \dots, \xi_m$, il y en a une paire au moins (ξ_i, ξ_j) telle que

$$|\xi_i - \xi_j| \geq \sqrt{\frac{3}{2}}.$$

Faisons maintenant $n = 3$, prenons $K_3 = \left(\frac{4}{3}\right)^3$ et faisons $\mu_1 = 1$, $\mu_2 = \zeta$, $\mu_3 = \zeta^2$, on a le résultat suivant :

Parmi m entiers algébriques conjugués $\xi_1, \xi_2, \dots, \xi_m$ ($m \geq 3$) on peut en trouver trois au moins : ξ_i, ξ_j, ξ_k tels que

$$(\xi_i - \xi_j)(\xi_j - \xi_k)(\xi_k - \xi_i) \geq \frac{9}{8} \sqrt{2}.$$

Le théorème général nous permet aussi de définir une *base canonique* pour un corps ou un idéal, un anneau, ou plus généralement pour tout module de nombres algébriques. Soit par exemple Ω un corps de degré m , nous désignerons par

$$\Omega^{(i)} \quad (i = 1, 2, \dots, m)$$

le corps et ses conjugués, soit $\omega_1^{(i)}, \omega_2^{(i)}, \dots, \omega_m^{(i)}$ une base du corps. Pour premier nombre fondamental du corps nous prendrons l'unité, et le deuxième sera choisi parmi ceux qui sont définis de la façon suivante : soit μ un entier quelconque du corps, différent d'un entier naturel, posons

$$M(\mu) = \max |\mu^{(i)} - \mu^{(j)}| \quad (i, j = 1, 2, \dots, m)$$

et aussi

$$M_2(\Omega) = \min M(\mu) \quad (> 0).$$

Soit μ_1 le nombre choisi, nous prendrons le nombre μ_2 , non compris dans le module $(1, \mu_1)$, tel que μ désignant un nombre quelconque du corps non compris dans ce module en posant

$$M(1, \mu_1, \mu) = \max \text{ module } \begin{vmatrix} 1 & 1 & 1 \\ \mu_1^{(i)} & \mu_1^{(j)} & \mu_1^{(k)} \\ \mu^{(i)} & \mu^{(j)} & \mu^{(k)} \end{vmatrix} \quad (i, j, k = 1, 2, \dots, m),$$

ou ait

$$\min M(1, \mu_1, \mu) = M(1, \mu_1, \mu_2) = M_3(\Omega)$$

et l'on continuera de la sorte en définissant successivement $M_1(\Omega) \dots M_{m-1}(\Omega)$. On vérifie facilement que les bases des corps quadratiques et des corps de la division du cercle que l'on prend habituellement jouissent des propriétés qui viennent d'être indiquées.

Prenons maintenant le cas le plus simple : celui où $n = 2$.

Soit E_m une équation irréductible du $m^{\text{ième}}$ degré à coefficients entiers dont le coefficient de la plus haute puissance de x est l'unité : cette équation définit m entiers algébriques conjugués $\xi_1, \xi_2, \dots, \xi_m$, posons

$$M(E_m) = \max \xi_i - \xi_j \quad (i, j = 1, 2, \dots, m).$$

puis, parmi les équations E_m , choisissons celles qui rendent minimum le nombre $M(E_m)$ et posons

$$M(m) = \min M(E_m).$$

D'après ce que nous venons de voir on a

$$M(m) \geq \sqrt{\frac{3}{2}}.$$

Les équations de la division du cercle montrent d'autre part qu'il existe une infinité de valeurs de m pour lesquelles on a

$$M(m) < 2.$$

Il y aurait, je crois, intérêt à montrer que cette inégalité est vraie pour toute valeur de m ⁽¹⁾ mais je n'ai pas réussi à le faire; on aurait alors une limite supérieure du minimum des modules des discriminants des corps de degré m en résolvant le problème suivant :

(1) L'équation

$$(E_m) \quad x^m - 2 = 0$$

est irréductible et montre que

$$M(m) \leq M(E_m) < 2 \sqrt[m]{2}.$$

La différente de ce nombre a d'ailleurs pour valeur absolue $\frac{(2m)^m}{2}$, ce qui enlève toute valeur à la remarque faite dans ma Note aux *Comptes rendus* relative-ment aux discriminants des corps de degré m (t. 186, 1928, p. 1181).

Étant donnés n points dans un plan dont les distances respectives sont plus petites que 2, trouver le maximum du produit des carrés de leurs distances respectives.

Considérons maintenant les équations irréductibles de degré m qui possèdent r racines réelles et $2s$ racines imaginaires

$$(m = r + 2s),$$

on pourra se proposer de déterminer le nombre $M(m = r + 2s)$; dans le cas où s est nul, ce nombre croît sans doute avec m .

D'après l'inégalité de Minkowski (meilleure que celle que notre méthode peut donner) relative au discriminant d'un corps de cette sorte, on a

$$11(\xi_i - \xi_j)^2 > \frac{m^{2m}}{(m!)^2}.$$

En l'appliquant on trouve, après quelques calculs simples,

$$M(3 = 3 + 0) > \sqrt[3]{18} = 2,620\dots,$$

$$M(4 = 4 + 0) > \sqrt[4]{\frac{12 \sqrt{32.10^6}}{9}} \approx 2,901\dots$$

Déterminons les nombres dont nous venons de parler pour $m = 2$ et 3.

Pour $m = 2$ on trouve facilement que

$$M(2) = M(2 = 0 + 2) = \sqrt{3}$$

et que les équations qui fournissent le minimum se déduisent de l'équation

$$x^2 + x + 1 = 0$$

en changeant x en $\pm x + \alpha$ où α désigne un entier naturel.

De même

$$M(2 = 2 + 0) \approx \sqrt{5}$$

et les équations correspondantes se déduisent de

$$x^2 + x - 1 = 0$$

par les mêmes substitutions.

Pour $m = 3$ nous avons déjà trouvé que $M(3 = 3 + 0) > 2$, nous rechercherons donc parmi les équations E_3 à une seule racine réelle s'il en est dont le nombre M est inférieur à 2.

D'abord il est clair qu'en changeant x en $\pm x + a$ on peut ramener les équations à être de l'une des deux formes

$$(I) \quad x^2 + px + q = 0,$$

$$(II) \quad x^3 + x^2 + px + q = 0.$$

Soient alors A, B, C les points représentatifs des racines dans le plan complexe (A sur l'axe réel), le triangle ABC est isocèle ($AB = AC$) et l'on trouve facilement en désignant par x_1 la racine réelle

$$BC^2 = 4p + 3x_1^2, \quad AB^2 = AC^2 = p + 3x_1^2 \quad (\text{type I}),$$

$$BC^2 = 4p - 1 + 3x_1^2 + 2x_1, \quad AB^2 = AC^2 = p + 3x_1^2 + 2x_1 \quad (\text{type II});$$

donc

$$BC^2 - AB^2 = 3p \quad (\text{type I}),$$

$$BC^2 - AB^2 = 3p - 1 \quad (\text{type II}).$$

Si nous voulons que le plus grand côté du triangle ABC soit plus petit que 2, il faudra d'abord

$$p = -1, 0, 1 \quad (\text{type I}),$$

$$p = 0, 1 \quad (\text{type II}).$$

De plus nous conserverons seulement les équations pour lesquelles

$$AB^2 \cdot BC^2 \cdot CA^2 < 64,$$

soit

$$4p^3 + 27q^2 < 64, \quad q = \pm 1 \quad (\text{type I}),$$

$$\left. \begin{aligned} 4\left(p - \frac{1}{3}\right)^2 + 27\left(\frac{2}{27} - \frac{p}{3} + q\right)^2 &< 64 \\ p = 0, \quad q = \pm 1 \\ p = 1, \quad q = -1 \end{aligned} \right\} \quad (\text{type II}).$$

Nous n'avons plus qu'un très petit nombre d'équations à essayer; dans le groupe (I) $p = 0$ ne convient pas car on tombe sur une équation réductible; on peut d'autre part supposer $q < 0$.

L'équation

$$x^2 + x - 1 = 0$$

ne convient pas car

$$BC^2 = 4 + 3x_1^2 > 4;$$

de même pour

$$x^3 + x^2 + x + 1 = 0,$$

on a

$$BC^2 = 3 + 3x_1^2 + 2x_1 > 4,$$

car

$$x_1 > \frac{1}{3}.$$

Il reste donc

$$x^3 - x - 1 = 0,$$

$$x^3 + x^2 + 1 = 0,$$

$$x^3 + x^2 - 1 = 0.$$

Pour décider entre les deux dernières équations, considérons la courbe $y = x^3 + x^2$, elle est symétrique par rapport aux points $x = -\frac{1}{3}$, $y = \frac{2}{27}$ et pour ces deux équations la quantité qui nous intéresse est

$$\Delta B^2 = 3x_1^2 + 2x_1 = y'(x_1)$$

et la symétrique de la droite $y = 1$ par rapport au centre de symétrie de la courbe est la droite $y = -\frac{23}{27} (> -1)$: nous éliminons donc la deuxième équation.

Il reste à comparer la première et la dernière ; soit α la racine réelle de la première, celle de la troisième est $\frac{1}{\alpha}$; nous allons vérifier que le M de la première est supérieur à celui de la troisième, c'est-à-dire que

$$3\alpha^2 - 1 > \frac{1}{\alpha^2} + \frac{2}{\alpha}$$

ou

$$2\alpha^2 + \alpha - 3 > 0,$$

ce qui a effectivement lieu car $\alpha > 1$.

On a donc

$$M(3) = \sqrt{\frac{3}{\alpha^2} + \frac{2}{\alpha}} \approx 1,79(\dots)$$

et les équations correspondantes se déduisent toutes de

$$x^3 + x^2 - 1 = 0$$

par les substitutions $(x, \pm x + a)$.

Pour terminer, recherchons parmi les équations du troisième degré à trois racines réelles celles qui fournissent le minimum de $M(3 = 3 + 0)$; on montre facilement que $M(3 = 3 + 0) > 3$: nous rechercherons donc les équations E_3 pour lesquelles $M(E_3) < 4$.

Si l'équation est du type

$$(E_3) \quad x^3 = px + q \quad (p, q > 0)$$

en posant $D = 4p^3 - 27q^2$, le nombre $M(E'_3)$ est la racine positive de l'équation

$$u^3 = 3pu + \sqrt{D};$$

écrivant que cette racine est plus petite que 4, on aura

$$64 > 12p + \sqrt{D},$$

ce qui donne seulement les trois équations

$$(1) \quad x^3 - 3x - 1 = 0, \quad D = 81,$$

$$(2) \quad x^3 - 4x - 1 = 0, \quad D = 229,$$

$$(3) \quad x^3 - 4x - 2 = 0, \quad D = 148.$$

Si l'équation est du type

$$(E''_3) \quad x^3 + x^2 - px + q = 0 \quad (p > 0),$$

le nombre $M(E''_3)$ est la racine positive de l'équation

$$u^3 = (3p + 1)u + \sqrt{D}$$

avec

$$D = 4p^3 - p^2 - 27q^2 - 18pq - 4q$$

et nous écrirons que

$$60 > 12p + \sqrt{D},$$

ce qui donne, en éliminant les équations réductibles

$$(4) \quad x^3 + x^2 - 2x - 1 = 0, \quad D = 41,$$

$$(5) \quad x^3 + x^2 - 3x - 1 = 0, \quad D = 130,$$

$$(6) \quad x^3 + x^2 - 4x + 1 = 0, \quad D = 137.$$

Pour choisir entre ces six équations, nous n'avons qu'à remarquer que si u_1 et u_2 sont les racines positives de

$$u_1^3 = A u_1 + B, \quad A, B > 0,$$

$$u_2^3 = A' u_1 + B', \quad A', B' > 0$$

avec $A > A', B > B'$ on a

$$u_1 > u_2.$$

L'équation qui nous fournira le minimum de $M(3 = 3 + 0)$ est donc l'équation (4) qui est abélienne et l'on a

$$M(3 = 3 + 0) = 3,048 \dots$$
