complexe représenté par le déterminant des quantités

$$\begin{array}{cccc} (\alpha)_0 & (\alpha)_1 & \ldots & (\alpha)_{m-1}, \\ q_0 & q_1 & \ldots & q_{m-1}, \\ r_0 & r_1 & \ldots & r_{m-1}, \\ \ldots & \ldots & \ldots & \ldots, \\ s_0 & s_1 & \ldots & s_{m-1}, \end{array}$$

aura pour norme l'unité.

J'ai trouvé aussi : *qu'il suffisait d'obtenir le système des substitutions propres à réduire la forme Φ dans un intervalle fini des quantités* A *et* K, *les substitutions correspondant à toutes les autres valeurs de ces mêmes quantités se déduisant de celles-là.*

De là on déduit que toutes les solutions de l'équation

$$\text{Norme } \varphi(\alpha) = 1$$

peuvent s'obtenir par un nombre *limité* d'entre elles, convenablement choisies, mais d'autres considérations mènent à la même conséquence. Je vais les indiquer en restant dans le cas particulier qui me les a fait découvrir.

Désignons par α la racine réelle, et par β et γ les deux racines imaginaires de l'équation du troisième degré à coefficients entiers

$$x^3 + Ax^2 + Bx + C = 0.$$

Soient aussi φ et ψ deux unités complexes de la forme

$$x + \alpha y + \alpha^2 z,$$

je dis *que de ces deux unités en résulte une troisième dont elles sont l'une et l'autre des puissances entières.*

Posons, en effet,

$$\Phi = \varphi^m \psi^n, \qquad \Psi = \varphi^{m_0} \psi^{n_0},$$

m, n, m_0, n_0 étant quatre nombres entiers tels que

$$mn_0 - nm_0 = 1,$$

on aura réciproquement

$$\varphi = \Phi^{n_0} \Psi^{-n}, \qquad \psi = \Psi^m \Phi^{-m_0}.$$

De deux choses l'une : ou l'on pourra faire par exemple $\Phi = 1$, et le théorème est démontré : ou bien au moins $\Phi = \psi^{\frac{\varepsilon}{n}}$, ε étant

moindre que l'unité et n pouvant prendre une infinité de valeurs différentes. Or, ayant toujours norme $\Phi = 1$, on conclurait qu'il existe une infinité de solutions de cette équation dans lesquelles la valeur de l'unité complexe réelle et celle du module analytique des deux unités conjuguées imaginaires seraient aussi voisines du nombre 1 qu'on le voudrait, ce qui est absurde.

Une méthode toute semblable m'a conduit à démontrer que, dans le cas des *trois racines réelles,* toutes les unités sont les produits des puissances de *deux* d'entre elles qui ne sont pas réductibles l'une et l'autre aux puissances entières d'une troisième, et il ne me paraît pas difficile d'étendre les mêmes considérations au cas le plus général.

Quatrième Lettre.

La dernière Lettre que j'ai eu l'honneur de vous écrire était à peine partie que j'ai eu communication, par M. Liouville, d'une Note tirée des *Comptes rendus* de votre Académie, et dans laquelle vous traitez de la réduction des formes quadratiques, à coefficients entiers, sous un point de vue qui ne se serait jamais présenté à mon esprit et qui m'a vivement intéressé. Le résultat plein d'élégance auquel vous arrivez par une méthode si simple m'a fait rechercher si, dans ce nouveau type de formes réduites, il y avait encore possibilité d'obtenir *des limitations des coefficients, fonctions seulement du déterminant.*

En particulier, j'ai considéré les formes définies ternaires

$$f = ax^2 + a'y^2 + a''z^2 + 2byz + 2b'xz + 2b''xy,$$

dans lesquelles, d'après le principe de votre méthode, il faut faire par exemple

$$x = \frac{b}{\omega}\xi + \beta\eta, \qquad y = -\frac{b'}{\omega}\xi + \beta'\eta,$$

ω désignant le plus grand commun diviseur de b et b', déterminé par l'équation

$$\omega = b\beta' + b'\beta.$$

On obtient ainsi la transformée

$$\mathfrak{A}\xi^2 + \mathfrak{A}'\eta^2 + a''z^2 + 2\mathfrak{B}\xi\eta + 2\omega\eta z,$$

où l'un des rectangles des indéterminées a disparu.

Cela posé, *si les coefficients de la forme proposée sont limités, au moyen du déterminant* D, *il en sera de même des coefficients de la transformée*. En particulier, $\mathfrak{A}$ peut s'écrire

$$\mathfrak{A} = \frac{1}{\omega^2}(ab^2 + a'b'^2 - 2bb'b'') = \frac{1}{\omega^2}(aa'a'' - a''b''^2 - \mathrm{D}),$$

donc

$$\mathfrak{A} < \frac{aa'a''}{\omega^2}.$$

Or on peut ensuite supposer

$$2\mathfrak{B} < \mathfrak{A},$$

en déterminant convenablement β et β' dans l'équation

$$\omega = b\beta' + \beta b'$$

ou, ce qui est au fond la même chose, en changeant dans la transformée ξ en $\xi + m\eta$. Quant à la limite du dernier coefficient $\mathfrak{A}'$, elle se tire de l'équation

$$\mathfrak{A}\mathfrak{A}' - \mathfrak{B}^2 = aa' - b''^2.$$

En revenant aux premières considérations qui m'avaient fait entrevoir, il y a longtemps, l'importance de la recherche du minimum des formes à un nombre quelconque de variables, j'ai été conduit à présenter de la manière suivante les idées que vous avez le premier émises sur l'impossibilité de certaines fonctions périodiques.

Soient, pour les fonctions d'une seule variable,

$$a + b\sqrt{-1}, \qquad a' + b'\sqrt{-1}, \qquad a'' + b''\sqrt{-1}$$

trois indices quelconques de périodicité, je considère la forme définie ternaire

$$f = (ax + a'y + a''z)^2 + (bx + b'y + b''z)^2 + \frac{z^2}{\Delta^2},$$

dont le déterminant

$$\mathrm{D} = \left(\frac{ab' - ba'}{\Delta}\right)^2.$$

Si $ab' - ba'$ n'est pas nul, et que les deux équations

$$ax + a'y + a''z = 0, \qquad bx + b'y + b''z = 0$$

ne puissent être vérifiées pour des valeurs entières de x, y et z, la fonction sera impossible. Car pouvant faire, pour toute valeur de Δ,

$$f < \sqrt[3]{2\mathrm{D}}$$

et, *a fortiori*,

$$(ax + a'y + a''z)^2 + (bx + b'y + b''z)^2 < \sqrt[3]{2\mathrm{D}},$$

on déduirait des indices proposés une période dont le module serait infiniment petit. Mais cette conclusion n'a plus lieu si $ab' - ba' = 0$. Alors je considère la forme binaire

$$f = (ax + a'y)^2 + (bx + b'y)^2 + \frac{y^2}{\Delta^2},$$

dont le déterminant, dans l'hypothèse admise, se trouve être

$$\mathrm{D} = \frac{a^2 + b^2}{\Delta^2}.$$

Or il est maintenant facile de prouver *que lorsque* $ab' - ba' = 0$ l'on ne peut même admettre les deux périodes

$$a + b\sqrt{-1} \quad \text{et} \quad a' + b'\sqrt{-1},$$

si on les suppose irréductibles, c'est-à-dire si les équations

$$ax + a'y = 0, \qquad bx + b'y = 0$$

ne peuvent avoir lieu en nombres entiers. On peut faire, en effet, pour toute valeur de Δ,

$$f < \sqrt{\tfrac{4}{3}\mathrm{D}},$$

et, *a fortiori*,

$$(ax + a'y)^2 + (bx + b'y)^2 < \sqrt{\tfrac{4}{3}\mathrm{D}},$$

ce qui conduit de nouveau à une période infiniment petite.

Les fonctions de plusieurs variables à périodes coexistantes que vous avez introduites le premier dans l'analyse, peuvent être traitées par les mêmes principes.

Soient

$$a_i + b_i\sqrt{-1}, \quad c_i + d_i\sqrt{-1}, \quad \ldots, \quad k_i + l_i\sqrt{-1},$$

n indices simultanés de périodicité correspondant, respectivement, aux variables

$$x, \quad y, \quad \ldots, \quad u,$$

dans une fonction telle que $\mathfrak{f}(x, y, \ldots, u)$, je dis *que si le nombre de ces groupes d'indices, supposés irréductibles, surpasse* $2n$, *la fonction proposée sera impossible, dans ce sens qu'on sera forcé d'admettre un groupe d'indices simultanés infiniment petits.*

Faisons, pour abréger,

$$\begin{aligned}
\mathfrak{A} &= a_1 x_1 + a_2 x_2 + \ldots + a_{2n+1} x_{2n+1},\\
\mathfrak{B} &= b_1 x_1 + b_2 x_2 + \ldots + b_{2n+1} x_{2n+1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\mathfrak{K} &= k_1 x_1 + k_2 x_2 + \ldots + k_{2n+1} x_{2n+1},\\
\mathfrak{L} &= l_1 x_1 + l_2 x_2 + \ldots + l_{2n+1} x_{2n+1},
\end{aligned}$$

le déterminant D de la forme

$$f = \mathfrak{A}^2 + \mathfrak{B}^2 + \ldots + \mathfrak{K}^2 + \mathfrak{L}^2 + \frac{x_{2n+1}^2}{\Delta^2}$$

sera, comme on le trouve aisément,

$$D = \frac{1}{\Delta^2}\,\text{dét.}\begin{pmatrix} a_1 & b_1 & \ldots & k_1 & l_1 \\ a_2 & b_2 & \ldots & k_2 & l_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{2n} & b_{2n} & \ldots & k_{2n} & l_{2n} \end{pmatrix}^2,$$

et la conséquence que je voulais obtenir découle, comme précédemment, de la relation

$$f < \left(\frac{4}{3}\right)^{n} \sqrt[2n+1]{D},$$

à laquelle on peut toujours satisfaire quelque grand que soit Δ.

Si l'on suppose que le déterminant qui entre dans l'expression de D s'évanouisse, la démonstration n'est plus applicable, mais la proposition n'en a pas moins lieu, et l'on obtient ainsi le premier terme d'une série de nouveaux cas d'impossibilité dont voici les conditions analytiques.

Soit, pour abréger,

$$\begin{aligned}
\mathfrak{A}_i &= a_1 x_1 + a_2 x_2 + \ldots + a_{2n+1-i} x_{2n+1-i},\\
\mathfrak{B}_i &= b_1 x_1 + b_2 x_2 + \ldots + b_{2n+1-i} x_{2n+1-i},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\mathfrak{K}_i &= k_1 x_1 + k_2 x_2 + \ldots + k_{2n+1-i} x_{2n+1-i},\\
\mathfrak{L}_i &= l_1 x_1 + l_2 x_2 + \ldots + l_{2n+1-i} x_{2n+1-i},
\end{aligned}$$

et soit D_i le déterminant de la forme

$$f_i = \mathfrak{A}_i^2 + \mathfrak{B}_i^2 + \ldots + \mathfrak{K}_i^2 + \mathfrak{L}_i^2 + \frac{x_{2n+1-i}^2}{\Delta^2}.$$

Si l'on suppose D_{i-1} nul, on trouve que $\Delta^2 D_i$ s'obtient en faisant la somme des carrés de tous les déterminants que fournit le système

$$\begin{matrix}
a_1, & b_1, & \ldots, & k_1, & l_1,\\
a_2, & b_2, & \ldots, & k_2, & l_2,\\
\ldots, & \ldots, & \ldots, & \ldots, & \ldots,\\
a_{2n-i}, & b_{2n-i}, & \ldots, & k_{2n-i}, & l_{2n-i},
\end{matrix}$$

en employant, d'une manière quelconque, $2n - i$ lignes verticales. Or, toute fonction périodique de n variables sera impossible lorsque, ayant $2n - i$ groupes de périodes simultanées irréductibles, savoir :

$$\left\{ a_\mu + b_\mu\sqrt{-1}, \; c_\mu + d_\mu\sqrt{-1}, \; \ldots, \; k_\mu + l_\mu\sqrt{-1} \right\}_{\mu=1}^{\mu=2n-i},$$

le déterminant D_i de la forme f_i, composé avec ces indices, s'annulera. En effet, on arrivera à un système de périodes simultanées infiniment petites, en considérant dans la série des formes

$$f_{i+1}, \quad f_{i+2}, \quad \ldots, \quad f_{2n-1},$$

la première de celles dont le déterminant ne s'évanouit point. La dernière d'ailleurs est dans ce cas, car on trouve aisément

$$D_{2n-1} = \frac{1}{\Delta^2}(a_1^2 + b_1^2 + \ldots + k_1^2 + l_1^2).$$

L'analyse que je viens d'employer s'applique à une question bien différente, *à la théorie des unités complexes les plus générales*, et donne ce théorème :

Soit m' le nombre des racines réelles et des couples de racines imaginaires d'une équation irréductible à coefficients *entiers et dont le premier coefficient est l'unité, si l'on a m' unités complexes quelconques, formées avec les racines de cette équation, elles peuvent toujours s'exprimer par les produits des puissances entières, positives ou négatives, de $m'-1$ autres convenablement choisies* (¹).

Nommons

$$\alpha_1,\quad \alpha_2,\quad \ldots,\quad \alpha_n$$

les racines réelles de l'équation proposée, et

$$\beta_1,\ \gamma_1;\quad \beta_2,\ \gamma_2;\quad \ldots;\quad \beta_{n'},\ \gamma_{n'}$$

les divers couples de ses racines imaginaires. Soit encore

$$\varphi_i(\alpha) = a_i + \alpha b_i + \alpha^2 c_i + \ldots + \alpha^{m-1} l_i$$

une unité complexe quelconque, et

$$\begin{aligned}
\log \varphi_i^2(\alpha) &= (\alpha)_i,\\
\log \varphi_i(\beta)\,\varphi_i(\gamma) &= (\beta,\gamma)_i,\\
\mathrm{F}(\alpha) &= x_1(\alpha)_1 + x_2(\alpha)_2 + \ldots + x_{m'}(\alpha)_{m'},\\
\mathrm{F}(\beta,\gamma) &= x_1(\beta,\gamma)_1 + x_2(\beta,\gamma)_2 + \ldots + x_{m'}(\beta,\gamma)_{m'};
\end{aligned}$$

je dis qu'il est toujours possible de déterminer, pour $x_1, x_2, \ldots, x_{m'}$, un système de valeurs entières, positives ou négatives, telles qu'on ait

$$(1)\qquad \mathrm{F}(\alpha) = 0 \quad \text{ou} \quad \varphi_1^{2x_1}(\alpha)\,\varphi_2^{2x_2}(\alpha)\ldots\varphi_{m'}^{2x_{m'}}(\alpha) = 1.$$

Cette condition d'ailleurs aura nécessairement lieu à la fois pour toutes les racines, réelles ou imaginaires, puisqu'elles appartiennent, par hypothèse, à une équation irréductible.

Supposons, en effet, l'équation (1) impossible, et voyons quelles conséquences vont s'ensuivre.

(¹) Le théorème complet, savoir : *Qu'il y a effectivement, dans tous les cas, $m'-1$ unités complexes indépendantes par les produits des puissances desquelles on peut représenter toutes les autres*, est un des plus importants, mais aussi un des plus épineux de la Science des nombres. La démonstration rigoureuse de ce théorème a été donnée par M. Lejeune-Dirichlet dans les *Comptes rendus mensuels de l'Académie de Berlin* du 30 mars 1846. *Voir* aussi ceux d'octobre 1841 et d'avril 1842, et une Lettre du même auteur à M. Liouville. (*Journal de Mathématiques*, t. V; 1840.) JACOBI.

En premier lieu, deux systèmes distincts de valeurs entières des indéterminées, $x_1, x_2, \ldots, x_{m'}$, ne donneront jamais la même valeur de $\mathrm{F}(\alpha)$. Car, ayant, par exemple,

$$x_1(\alpha)_1 + x_2(\alpha)_2 + \ldots + x_{m'}(\alpha)_{m'} = y_1(\alpha)_1 + y_2(\alpha)_2 + \ldots + y_{m'}(\alpha)_{m'},$$

on en déduirait

$$(x_1 - y_1)(\alpha)_1 + (x_2 - y_2)(\alpha)_2 + \ldots + (x_{m'} - y_{m'})(\alpha)_{m'} = 0,$$

c'est-à-dire une solution de l'équation (1), ce qui est contre l'hypothèse admise.

Cela posé, je considère la forme quadratique

$$\begin{aligned}
\mathbf{F} = {}& \mathrm{F}^2(\beta_1,\gamma_1) + \mathrm{F}^2(\beta_2,\gamma_2) + \ldots + \mathrm{F}^2(\beta_{n'},\ {}_{n'})\\
&+ \mathrm{F}^2(\alpha_1) + \mathrm{F}^2(\alpha_2) + \ldots + \mathrm{F}^2(\alpha_{n-1}) + \frac{x_{m'}^2}{\Delta^2},
\end{aligned}$$

dont le déterminant est

$$\mathrm{D} = \frac{1}{\Delta^2}\,\text{dét.}\begin{pmatrix}
(\alpha_1)_1 & (\alpha_1)_2 & \ldots & (\alpha_1)_{m'-1}\\
(\alpha_2)_1 & (\alpha_2)_2 & \ldots & (\alpha_2)_{m'-1}\\
\ldots & \ldots & \ldots & \ldots\\
(\alpha_{n-1})_1 & (\alpha_{n-1})_2 & \ldots & (\alpha_{n-1})_{m'-1}\\
(\beta_1,\gamma_1)_1 & (\beta_1,\gamma_1)_2 & \ldots & (\beta_1,\gamma_1)_{m'-1}\\
(\beta_2,\gamma_2)_1 & (\beta_2,\gamma_2)_2 & \ldots & (\beta_2,\gamma_2)_{m'-1}\\
\ldots & \ldots & \ldots & \ldots\\
(\beta_{n'},\gamma_{n'})_1 & (\beta_{n'},\gamma_{n'})_2 & \ldots & (\beta_{n'},\gamma_{n'})_{m'-1}
\end{pmatrix}^2$$

et je le supposerai d'abord différent de zéro.

Dans ce cas, si je cherche les minima de la forme $\mathbf{F}$, pour des valeurs indéfiniment croissantes de Δ, il est clair qu'en posant

$$\mathrm{F}(\alpha) = \log \Phi^2(\alpha)$$

et, par suite,

$$\mathrm{F}(\beta,\gamma) = \log \Phi(\beta)\,\Phi(\gamma),$$

j'obtiendrai une infinité d'unités complexes, $\Phi(\alpha)$, toutes différentes, d'après la remarque précédemment faite, et dont les valeurs absolues réelles, ainsi que les modules des valeurs imaginaires, seront aussi voisins de l'unité qu'on voudra. Or on aurait de la sorte m' fonctions linéaires et homogènes, à m' indéterminées entières, qui seraient susceptibles de prendre une infinité de valeurs numériques inégales et comprises dans un intervalle limité, ce qui est absurde.

Lorsque le déterminant D sera différent de zéro, on peut donc satisfaire par des nombres entiers à l'équation

$$x_1(\alpha)_1 + x_2(\alpha)_2 + \ldots + x_{m'}(\alpha)_{m'} = 0.$$

Cela posé, je fais

$$\begin{aligned} y_1(\alpha)_1 + y_2(\alpha)_2 + \ldots + y_{m'}(\alpha)_{m'} &= \log Y(\alpha), \\ z_1(\alpha)_1 + z_2(\alpha)_2 + \ldots + z_{m'}(\alpha)_{m'} &= \log Z(\alpha), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots &\ldots\ldots\ldots, \\ v_1(\alpha)_1 + v_2(\alpha)_2 + \ldots + v_{m'}(\alpha)_{m'} &= \log V(\alpha), \end{aligned}$$

les nombres entiers $y, z, \ldots, v$ étant pris de manière que le déterminant relatif à ces équations linéaires et à la précédente soit l'unité. Il est clair qu'on pourra tirer de là les valeurs des m' unités $\varphi_i(\alpha)$, exprimées par les produits des puissances entières de $Y(\alpha)$, $Z(\alpha), \ldots, V(\alpha)$, qui représentent d'autres unités complexes, au nombre seulement de $m' - 1$.

Il me reste à examiner le cas où le déterminant de la forme F est supposé s'évanouir. Soit alors

$$\begin{aligned} F_i(\alpha) &= x_1(\alpha)_1 + x_2(\alpha)_2 + \ldots + x_{m'-i}(\alpha)_{m'-i}, \\ F_i(\beta, \gamma) &= x_1(\beta, \gamma)_1 + x_2(\beta, \gamma)_2 + \ldots + x_{m'-i}(\beta, \gamma)_{m'-i}, \end{aligned}$$

et soit D_i le déterminant de la forme

$$\begin{aligned} \mathbf{F}_i = {} & F_i^2(\beta_1, \gamma_1) + F_i^2(\beta_2, \gamma_2) + \ldots + F_i^2(\beta_{n'}, \gamma_{n'}) \\ & + F_i^2(\alpha_1) + F_i^2(\alpha_2) + \ldots + F_i^2(\alpha_{n-1}) + \frac{x_{m'-i}^2}{\Delta^2}, \end{aligned}$$

Si l'on suppose D_{i-1} nul, on trouve, tout à fait comme précédemment, que $\Delta^2 D_i$ s'obtient en faisant la somme des carrés des divers déterminants que fournit le système

$$\begin{array}{cccccccc} (\alpha_1)_1 & (\alpha_2)_1 & \ldots & (\alpha_{n-1})_1 & (\beta_1, \gamma_1)_1 & (\beta_2, \gamma_2)_1 & \ldots & (\beta_{n'}, \gamma_{n'})_1 \\ (\alpha_1)_2 & (\alpha_2)_2 & \ldots & (\alpha_{n-1})_2 & (\beta_1, \gamma_1)_2 & (\beta_2, \gamma_2)_2 & \ldots & (\beta_{n'}, \gamma_{n'})_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ (\alpha_1)_{m'-1-i} & (\alpha_2)_{m'-1-i} & \ldots & (\alpha_{n-1})_{m'-1-i} & (\beta_1, \gamma_1)_{m'-1-i} & (\beta_2, \gamma_2)_{m'-1-i} & \ldots & (\beta_{n'}, \gamma_{n'})_{m'-1-i} \end{array}$$

en employant $m' - 1 - i$ lignes verticales. Considérant donc dans la série des formes

$$\mathbf{F}_1, \quad \mathbf{F}_2, \quad \ldots, \quad \mathbf{F}_{m'-2},$$

la première de celles dont le déterminant ne s'évanouit point [et la dernière est toujours dans ce cas (¹)], on obtiendra absolument les mêmes résultats que ceux auxquels nous sommes parvenus tout à l'heure, puisque le déterminant D_i devient d'une petitesse arbitraire pour des valeurs suffisamment grandes de Δ.

Je ne sais, Monsieur, si ces résultats et la méthode que j'ai employée sont connus, et nommément s'ils se trouvent déjà dans les travaux de M. Kummer, que vous avez eu la bonté de m'indiquer. M. Liouville sans doute les publierait de suite dans son Journal, si nous pouvions trouver un traducteur, et ce serait pour moi en particulier un grand plaisir de prendre connaissance de ces recherches d'après ce que vous m'en avez écrit. L'introduction du nombre complexe, auquel M. Kummer donne le nom *d'idéal*, m'intéresserait surtout au plus haut degré.

P. S. L'expression des unités complexes au moyen d'un nombre déterminé d'entre elles donne lieu à une remarque essentielle et que j'ai omise, lorsque les racines qui entrent dans leur composition sont toutes imaginaires. L'analyse que j'ai employée conduit alors de nouveau à isoler celle de ces unités dont le module analytique est *un*, si toutefois il en existe. C'est au reste le même résultat auquel je suis parvenu par une tout autre voie dans ma dernière Lettre.

(¹) Il faudrait excepter le cas où les unités complexes considérées auraient leurs modules analytiques égaux à l'unité. E. P.

SUR L'INTRODUCTION

DES

VARIABLES CONTINUES

DANS LA THÉORIE DES NOMBRES.

Journal de Crelle, tome 41.

I.

Amené depuis longtemps, par des recherches sur la théorie des fonctions elliptiques et abéliennes, à diverses questions d'Arithmétique transcendante, je viens offrir aux Lecteurs de ce Recueil quelques-uns des résultats auxquels je suis parvenu, et les principes de la méthode que j'ai suivie. Ces résultats sont relatifs surtout aux nombres complexes, considérés en général, ou plutôt à la théorie de certaines formes décomposables en facteurs linéaires et dont on verra plus bas la définition. Pour la méthode, son principal caractère consiste dans l'introduction, par un procédé général et très simple, de variables continues, qui font dépendre les questions relatives aux nombres entiers des principes analytiques les plus élémentaires. C'est là surtout ce que je me suis proposé de faire ressortir avec évidence, en revenant même sur une des théories exposées avec tant de profondeur et d'élégance dans les *Disquisitiones arithmeticæ* (la distribution en périodes des formes de déterminant positif), pour la présenter sous un nouveau point de vue. Quant aux questions nouvelles que j'ai essayé de traiter, je suis loin de les avoir approfondies autant que je l'aurais souhaité; aussi je demande l'indulgence du Lecteur pour ce que mon travail aura d'incomplet, espérant par la suite y revenir et le perfectionner.

II.

On connaît toute l'importance du problème général, dont l'objet est de distinguer si deux formes sont équivalentes ou non, et de trouver dans le premier cas toutes les transformations de l'une dans l'autre. Je m'occuperai, sous ce point de vue, des formes quadratiques définies, à un nombre quelconque de variables, et des formes binaires de degré quelconque, pour présenter d'une manière nouvelle ce que j'ai déjà dit dans le *Journal de Crelle,* tome 46. J'essayerai ensuite de fonder la théorie des nombres complexes, sur l'étude d'une série particulière de formes, que je définis de la manière suivante :

Soient

$$f(u) = u^n + \mathrm{A}u^{n-1} + \mathrm{B}u^{n-2} + \ldots + \mathrm{K}u + \mathrm{L} = 0$$

une équation irréductible à coefficients entiers, et

$$\varphi_i(u) = m_i u^{n-1} + p_i u^{n-2} + \ldots + r_i u + s_i$$

une fonction entière de u, à coefficients entiers : l'expression

$$\text{Norme}\,[\mathrm{X}\varphi_1(u) + \mathrm{Y}\varphi_2(u) + \ldots + \mathrm{V}\varphi_n(u)]$$

sera évidemment une fonction homogène et à coefficients entiers des n variables, X, Y, ..., V. Je nomme encore Δ le déterminant du système

$$\begin{vmatrix} m_1 & p_1 & \ldots & r_1 & s_1 \\ m_2 & p_2 & \ldots & r_2 & s_2 \\ .. & .. & \ldots & .. & .. \\ m_n & p_n & \ldots & r_n & s_n \end{vmatrix}.$$

Cela étant, j'assimilerai à l'ensemble des formes quadratiques de même déterminant toutes les expressions

$$\Phi = \frac{1}{\Delta}\,\text{Norme}\,[\mathrm{X}\varphi_1(u) + \mathrm{Y}\varphi_2(u) + \ldots + \mathrm{V}\varphi_n(u)],$$

dont les coefficients se réduiront à des nombres entiers. Ainsi il faut concevoir que la fonction $f(u)$ ne changeant point, on attribue à Δ la série indéfinie des valeurs entières, puis qu'on prenne, pour chaque valeur de Δ, tous les systèmes de nombres entiers m, $p, \ldots, s$, qui donnent à la norme le facteur Δ. Distribuer en classes distinctes toutes les expressions Φ, obtenues de la sorte, sera la question fondamentale d'une théorie analogue à celle des formes quadratiques binaires à facteurs réels, et qui indique sous quel point de vue j'envisage l'étude des nombres complexes.

La définition précédente peut être simplifiée en observant que toute forme Φ a une équivalente, dans laquelle le système

$$\begin{vmatrix} m_1 & p_1 & \ldots & r_1 & s_1 \\ m_2 & p_2 & \ldots & r_2 & s_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ m_n & p_n & \ldots & r_n & s_n \end{vmatrix},$$

dont le déterminant a pour valeur Δ, est remplacé par le suivant :

$$\begin{vmatrix} \delta & g & h & \ldots & l \\ 0 & \delta_1 & h' & \ldots & l' \\ 0 & 0 & \delta_2 & \ldots & l'' \\ . & . & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \delta_{n-1} \end{vmatrix}.$$

Les nombres entiers, désignés par les lettres $g, h, \ldots, l$, sont positifs et vérifient toutes les conditions

$$\begin{array}{llll} g < \delta_1, & h < \delta_2, & \ldots & l < \delta_{n-1}, \\ & h' < \delta_2, & \ldots & l' < \delta_{n-1}, \\ & \multicolumn{3}{l}{\ldots\ldots\ldots\ldots\ldots\ldots,} \end{array}$$

et l'on a toujours

$$\delta\delta_1\delta_2\ldots\delta_{n-1} = \Delta.$$

Ainsi, pour chaque valeur de Δ, on voit qu'il n'existe jamais qu'un nombre fini d'expressions Φ, distinctes. Mais je m'occuperai tout d'abord des formes binaires qui offrent, dans des circonstances analytiques plus simples, l'application des mêmes principes.

III.

La théorie connue de la réduction des formes quadratiques de déterminant négatif, étant le point de départ des recherches que je vais exposer, je le résumerai en peu de mots.

1° Toute forme

$$f = ax^2 + 2bxy + cy^2,$$

de déterminant négatif

$$b^2 - ac = -D,$$

a une équivalente

$$F = AX^2 + 2BXY + CY^2,$$

où le coefficient moyen $2B$ est, en valeur absolue, inférieur à A et C. Considérons en effet, l'ensemble des transformées déduites de f par la substitution

$$x = mX + m_0 Y,$$
$$y = nX + n_0 Y,$$

m, n, m_0, n_0 étant des entiers tels que

$$mn_0 - m_0 n = 1;$$

puis réunissons dans un même groupe toutes celles où le coefficient de X^2 est le plus petit possible, et choisissons dans ce groupe la forme où le coefficient de Y^2 est lui-même un minimum : cette transformée remplira les conditions énoncées.

Pour le prouver, il suffit de faire voir qu'on ne peut supposer $\pm 2B > A$, puisque A est évidemment le minimum absolu de f, pour des valeurs entières des indéterminées, et ne peut surpasser C ; or on en conclurait

$$A \mp 2B + C < C,$$

et la substitution

$$X = -X' + Y', \quad Y = -Y'$$

changerait F en

$$\begin{aligned} & A(-X' + Y')^2 \mp 2BY'(-X' + Y') + CY'^2 \\ & = AX'^2 + 2(\pm B - A)X'Y' + (A \mp 2B + C)Y'^2, \end{aligned}$$

transformée équivalente, où un coefficient moindre pour Y^2 est associé avec le même coefficient de X^2.

Les formes obtenues par la méthode qui vient d'être indiquée se nomment *formes réduites*, et il est évident que, pour une classe donnée, on a au plus deux réduites, qui ne diffèrent que par le signe du coefficient moyen.

2° Les conditions

$$\pm 2B < A, \quad \pm 2B < C$$

donnent

$$4B^2 < AC,$$

d'où l'on tire, à cause de $D = AC - B^2$, les limitations suivantes :

$$B^2 < \tfrac{1}{3} D, \qquad AC < \tfrac{4}{3} D.$$

On en déduit immédiatement que les formes à coefficients entiers de même déterminant peuvent être distribuées en un nombre limité de classes, puisqu'elles ne donnent qu'un nombre limité de réduites distinctes.

3° Les conditions

$$\pm 2B < A, \qquad \pm 2B < C$$

sont complètement caractéristiques des formes réduites. En effet, supposons, pour fixer les idées, B positif et prenons

$$F(x, y) = Ax^2 - 2Bxy + Cy^2,$$

les équations identiques

$$F(x-1, y) = F(x, y) - A(x-y) - y(A - 2B) - A(x-1),$$
$$F(x, y-1) = F(x, y) - C(y-x) - x(C - 2B) - C(y-1)$$

montrent qu'on diminue la valeur numérique de la forme en diminuant d'une unité celle des deux indéterminées dont la valeur absolue est la plus grande. On conclut de là que A et C sont les deux premiers minima de F, pour des valeurs entières des indéterminées; le troisième minimum est $A - 2B + C$. Cette démonstration de la proposition énoncée est due à Legendre; je me suis servi de la propriété importante des formes réduites sur laquelle elle se fonde, dans ma recherche du minimum d'une forme ternaire définie, pour des valeurs entières des indéterminées, dont l'une est supposée égale à l'unité.

IV.

Comme première application des résultats précédents, considérons la forme suivante :

$$f = (x - ay)^2 + \frac{y^2}{\Delta^2},$$

dans laquelle a et Δ sont des quantités réelles quelconques; soient

$$F = AX^2 + 2BXY + CY^2$$

sa réduite et

$$x = mX + m_0 Y,$$
$$y = nX + n_0 Y$$

la substitution propre à l'obtenir. La condition $AC < \frac{4}{3} D$ donne, pour le coefficient minimum A, la limite $\sqrt{\frac{4}{3} D}$; on a d'ailleurs

$$D = \frac{1}{\Delta^2}, \qquad A = (m - an)^2 + \frac{n^2}{\Delta^2};$$

donc : *Pour une valeur donnée de Δ, on peut toujours déterminer deux entiers m et n, tels qu'on ait*

$$(m - an)^2 + \frac{n^2}{\Delta^2} < \frac{1}{\Delta} \sqrt{\frac{4}{3}}.$$

Or de là se tirent plusieurs conséquences :

1° Le produit des deux facteurs $(m - an)^2$ et $\frac{n^2}{\Delta^2}$ étant toujours inférieur à son maximum, savoir :

$$\frac{1}{4} \left[(m - an)^2 + \frac{n^2}{\Delta^2} \right]^2,$$

on aura *a fortiori*

$$(m - an)^2 \frac{n^2}{\Delta^2} < \frac{1}{3\Delta^2}$$

ou

$$m - an < \frac{1}{n\sqrt{3}}.$$

On a d'ailleurs à la fois

$$(m - an)^2 < \frac{1}{\Delta} \sqrt{\frac{4}{3}}, \qquad \frac{n^2}{\Delta^2} < \frac{1}{\Delta} \sqrt{\frac{4}{3}} \quad \text{ou} \quad n^2 < \Delta \sqrt{\frac{4}{3}};$$

donc, on peut approcher indéfiniment d'une quantité quelconque a par des fractions $\frac{m}{n}$, de telle sorte que l'erreur $\frac{m}{n} - a$ soit toujours moindre que $\frac{1}{n^2\sqrt{3}}$.

2° Les deux entiers m et n donnant, pour une certaine valeur de Δ, le minimum de f, on ne saurait avoir deux autres nombres entiers m', n', tels que n' soit $< n$ et $(m' - an')^2 < (m - an)^2$; donc, $m - an$ représente un minimum absolu de la fonction linéaire $x - ay$, relativement à toute valeur entière de x et à des valeurs entières de y qui ne surpassent pas n. Donc encore $\frac{m}{n}$ approche plus de a que toute autre fraction de dénominateur moindre, car l'hypothèse $n' < n$ entraînant $(m' - an')^2 > (m - an)^2$ on en déduit immédiatement

$$\left(\frac{m'}{n'} - a\right)^2 > \left(\frac{m}{n} - a\right)^2.$$

3° Laissant de côté la recherche complète de tous les minima de la fonction $\frac{x}{y} - a$, ces minima étant relatifs à des valeurs entières de x et à des valeurs entières de y, inférieures à une limite donnée qu'on fait grandir indéfiniment : je considère deux minima consécutifs de f, auxquels correspondent deux systèmes distincts $x = m$, $y = n$, puis $x = m'$, $y = n'$.

On devra concevoir deux valeurs infiniment voisines de Δ, auxquelles appartiennent successivement les deux systèmes, de sorte qu'en désignant par δ une quantité infiniment petite, on ait

$$(m - an)^2 + \frac{n^2}{\Delta^2} < \frac{1}{\Delta}\sqrt{\frac{4}{3}},$$

$$(m' - an')^2 + \frac{n'^2}{(\Delta + \delta)^2} < \frac{1}{\Delta + \delta}\sqrt{\frac{4}{3}},$$

en mettant la seconde inégalité sous la forme

$$(m' - an')^2 + \frac{n'^2}{\Delta^2} < \frac{1}{\Delta}\sqrt{\frac{4}{3}} + \varepsilon,$$

ε étant encore infiniment petit, et multipliant membre à membre, il viendra

$$\left[(m - an)(m' - an') + \frac{nn'}{\Delta^2}\right]^2 + \left(\frac{mn' - nm'}{\Delta}\right)^2 < \frac{4}{3\Delta^2} + \frac{\varepsilon}{\Delta}\sqrt{\frac{4}{3}}.$$

On en conclut, en négligeant ε vis-à-vis des quantités finies,

$$(mn' - nm')^2 < \frac{4}{3},$$

et, par suite,

$$mn' - nm' = \pm 1.$$

Cette relation prouve, entre autres choses, qu'étant données trois fractions consécutives, $\frac{m}{n}$, $\frac{m'}{n'}$, $\frac{m''}{n''}$, on aura cette loi de formation :

$$m'' = km' \pm m, \qquad n'' = kn' \pm n,$$

k étant entier. On peut toujours, en effet, supposer deux inconnues, k, l, définies par les deux équations

$$m'' = km' + lm, \qquad n'' = kn' + ln,$$

lesquelles donnent

$$l = \frac{m''n' - n''m'}{mn' - m'n} = \pm 1,$$

le numérateur ayant, aussi bien que le dénominateur, l'unité pour valeur absolue.

V.

Ce qu'on vient de voir, sur l'approximation des quantités par des fractions rationnelles, était connu par la théorie des fractions continues; en faisant dépendre ces résultats de la seule notion de formes réduites de déterminant négatif, j'ai eu pour but de donner un premier exemple de l'emploi d'une variable continue dans une question relative aux nombres entiers, et aussi de faire voir comment cette longue chaîne de vérités, propres à l'Arithmétique transcendante, se lie dans l'origine aux éléments de l'Algèbre. La recherche complète des conditions d'équivalence de deux formes de déterminant négatif se présenterait, maintenant, comme conséquence des résultats qui viennent d'être obtenus, mais je ne saurais pour cela que reproduire l'Ouvrage même de M. Gauss. Laissant donc de côté les propositions importantes qui se rapportent à l'équivalence propre et impropre, aux formes ambiguës, j'arrive à la théorie des fonctions homogènes, telles que

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_{n-1} x y^{n-1} + a_n y^n.$$

1° Désignons par $x + \alpha y$ les facteurs linéaires réels, et par $x + \beta y$, $x + \gamma y$ les facteurs imaginaires conjugués de la forme proposée, de telle sorte qu'on ait

$$f(x, y) = a_0(x + \alpha_1 y)(x + \alpha_2 y)\ldots$$
$$(x + \alpha_\mu y)(x + \beta_1 y)(x + \gamma_1 y)\ldots(x + \beta_\nu y)(x + \gamma_\nu y)$$

et

$$\mu + 2\nu = n;$$

composons ensuite, avec ces facteurs et avec des quantités réelles,

$t_1, t_2, \ldots, u_1, u_2, \ldots$, la forme quadratique définie

$$\varphi(x, y) = t_1^2(x+\alpha_1 y)^2 + t_2^2(x+\alpha_2 y)^2 + \ldots + t_\mu^2(x+\alpha_\mu y)^2$$
$$+ 2u_1^2(x+\beta_1 y)(x+\gamma_1 y) + \ldots + 2u_\nu^2(x+\beta_\nu y)(x+\gamma_\nu y).$$

Cela étant, on concevra qu'on calcule la suite indéfinie des substitutions propres à réduire φ, lorsque les variables t et u passent par tous les états possibles de grandeur. Chacune de ces substitutions, faite dans f, donnera une certaine transformée; nous désignerons leur ensemble par le symbole (f). Or une première observation consistera en ceci :

f et F étant équivalentes, (f) et (F) seront composés des mêmes formes.

Pour le démontrer, soit

$$x = mX + m_0 Y, \qquad y = nX + n_0 Y$$

la substitution qui change f en

$$F = A_0 X^n + A_1 X^{n-1} Y + \ldots + A_{n-1} X Y^{n-1} + A_n Y^n;$$

posons

$$a = \frac{m_0 + \alpha n_0}{m + \alpha n}, \qquad b = \frac{m_0 + \beta n_0}{m + \beta n}. \qquad c = \frac{m_0 + \gamma n_0}{m + \gamma n};$$

on aura

$$F = A_0(X + a_1 Y)\ldots(X + a_\mu Y)(X + b_1 Y)(X + c_1 Y)\ldots$$
$$(X + b_\nu Y)(X + c_\nu Y),$$

et la forme quadratique Φ composée avec F, comme φ avec f, sera

$$\Phi = T_1^2(X + a_1 Y)^2 + \ldots + T_\mu^2(X + a_\mu Y)^2$$
$$+ 2U_1^2(X + b_1 Y)(X + c_1 Y) + \ldots + 2U_\nu^2(X + b_\nu Y)(X + c_\nu Y).$$

Cela posé, si l'une des formes de (f) a été obtenue en faisant dans f la substitution propre à réduire φ, lorsqu'on y suppose, en général,

$$t = \tau, \qquad u = \upsilon;$$

je dis que la même forme se trouvera dans (F) et aura été obtenue en réduisant Φ dans l'hypothèse

$$T^2 = \tau^2(m + \alpha n)^2, \qquad U^2 = \upsilon^2(m + \beta n)(m + \gamma n).$$

Soient, pour abréger, P la substitution qui transforme f en F

et Q la substitution propre à réduire φ; on vérifiera d'abord immédiatement que, par la substitution P, φ devient Φ : donc, réciproquement, par la substitution inverse P^{-1}, Φ devient φ, de telle sorte enfin que φ et Φ se changent en une seule et même forme réduite par les substitutions Q et $P^{-1}Q$.

Maintenant ces deux substitutions, faites respectivement dans f et F, donnent une même forme, la substitution inverse P^{-1} ramenant tout d'abord F à f.

Il est ainsi prouvé que toutes les formes de (f) sont dans (F); la réciproque est évidente, car on peut raisonner de F à f absolument comme on l'a fait de f à F; (f) et (F) sont donc identiques.

2° C'est parmi les formes dont l'ensemble a été désigné par (f) que nous choisirons une réduite pour représenter la classe entière à laquelle appartient f; dans ce but, nous allons établir quelques résultats préliminaires.

Soit, pour un système déterminé de valeurs de t et u,

$$x = mX + m_0 Y, \qquad y = nX + n_0 Y$$

la substitution propre à réduire φ; en conservant les notations précédentes la transformée réduite Φ sera

$$\Phi = T_1^2(X + a_1 Y)^2 + \ldots + T_\mu^2(X + a_\mu Y)^2$$
$$+ 2U_1^2(X + b_1 Y)(X + c_1 Y) + \ldots + 2U_\nu^2(X + b_\nu Y)(X + c_\nu Y),$$

les quantités T et U ayant pour valeurs

$$T^2 = t^2(m + \alpha n)^2, \qquad U^2 = u^2(m + \beta n)(m + \gamma n).$$

La transformée déduite de f, par la même substitution, sera également représentée par

$$F = A_0 X^n + A_1 X^{n-1} Y + \ldots + A_{n-1} X Y^{n-1} + A_n Y^n$$
$$= A_0(X + a_1 Y)\ldots(X + a_\mu Y)(X + b_1 Y)(X + c_1 Y)\ldots(X + b_\nu Y)(X + c_\nu Y).$$

Soit encore, pour abréger,

$$\Phi = PX^2 + 2QXY + RY^2,$$

de sorte que

$$T_1^2 + \ldots + T_\mu + 2U_1^2 + \ldots + 2U_\nu^2 = P,$$
$$a_1^2 T_1^2 + \ldots + a_\mu^2 T_\mu^2 + 2b_1 c_1 U_1^2 + \ldots + 2b_\nu c_\nu U_\nu^2 = R.$$

On pourra faire, en général,

$$\mathrm{T} = \omega\sqrt{\mathrm{P}}, \qquad \mathrm{U} = \varpi\sqrt{\mathrm{P}},$$
$$\mathrm{a}\mathrm{T} = \varphi\sqrt{\mathrm{R}}, \qquad \sqrt{(\mathrm{bc})}\,\mathrm{U} = \psi\sqrt{\mathrm{R}};$$

les quantités ω, ϖ d'une part, φ, ψ de l'autre, donnent les équations correspondantes

$$\omega_1^2 + \ldots + \omega_\mu^2 + 2\varpi_1^2 + \ldots + 2\varpi_\nu^2 = 1,$$
$$\varphi_1^2 + \ldots + \varphi_\mu^2 + 2\psi_1^2 + \ldots + 2\psi_\nu^2 = 1.$$

Enfin, nous remplacerons l'équation unique

$$\sqrt{(\mathrm{bc})}\,\mathrm{U} = \psi\sqrt{\mathrm{R}},$$

par les deux suivantes

$$\mathrm{b}\mathrm{U} = \psi\sqrt{\mathrm{R}}\,e^{i\lambda}, \qquad \mathrm{c}\mathrm{U} = \psi\sqrt{\mathrm{R}}\,e^{-i\lambda},$$

λ étant l'argument de l'imaginaire b. Cela posé, nous transformerons comme il suit l'expression en facteurs linéaires de F. Multiplions les facteurs réels $\mathrm{X} + \mathrm{a}\mathrm{Y}$ par T, et chacun des facteurs imaginaires conjugués $\mathrm{X} + \mathrm{b}\mathrm{Y}$, $\mathrm{X} + \mathrm{c}\mathrm{Y}$ par U; on aura d'abord

$$\mathrm{T}_1\mathrm{T}_2\ldots\mathrm{T}_\mu\mathrm{U}_1^2\mathrm{U}_2^2\ldots\mathrm{U}_\nu^2\mathrm{F} = \mathrm{A}_0\ldots(\mathrm{TX} + \mathrm{a}\mathrm{TY})(\mathrm{UX} + \mathrm{b}\mathrm{UY})(\mathrm{UX} + \mathrm{c}\mathrm{UY})\ldots;$$

puis, en introduisant les quantités ω, ϖ, φ, ψ, et représentant, pour abréger, $\mathrm{T}_1\mathrm{T}_2\ldots\mathrm{T}_\mu\mathrm{U}_1^2\mathrm{U}_2^2\ldots\mathrm{U}_\nu^2$ par (TU),

$$\mathrm{F} = \frac{\mathrm{A}_0}{(\mathrm{TU})}\ldots(\omega\sqrt{\mathrm{P}}\mathrm{X} + \varphi\sqrt{\mathrm{R}}\mathrm{Y})(\varpi\sqrt{\mathrm{P}}\mathrm{X} + e^{i\lambda}\psi\sqrt{\mathrm{R}}\mathrm{Y})(\varpi\sqrt{\mathrm{P}}\mathrm{X} + e^{-i\lambda}\psi\sqrt{\mathrm{R}}\mathrm{Y})\ldots$$

Or telle est l'expression de F à laquelle nous voulions arriver; par une simple raison d'homogénéité on en déduit cette conséquence importante, savoir :

Le produit de deux coefficients de F, *également éloignés des extrêmes, s'exprime de la manière suivante :*

$$\mathrm{A}_i\mathrm{A}_{n-i} = \frac{\mathrm{A}_0^2(\mathrm{PR})^{\frac{1}{2}n}}{(\mathrm{TU})^2}\,(i),$$

la quantité désignée par (i) *dépendant seulement de* ω, ϖ, φ, ψ *et* λ.

On a, par exemple,

$$\mathrm{A}_0\mathrm{A}_n = \frac{\mathrm{A}_0^2(\mathrm{PR})^{\frac{1}{2}n}}{(\mathrm{TU})^2}\,\omega_1\ldots\omega_\mu\varphi_1\ldots\varphi_\mu\varpi_1^2\ldots\varpi_\nu^2\psi_1^2\ldots\psi_\nu^2.$$

3° Cette quantité (i), qui est évidemment réelle, a une valeur numérique essentiellement limitée, et dont le maximum s'obtient, quel que soit i, en annulant les arguments λ, et, en faisant

$$\omega = \varpi = \varphi = \psi = \frac{1}{\sqrt{n}},$$

on obtient ainsi la limite

$$(i) < \frac{1}{n^n}\left(\frac{n.n-1\ldots n-i+1}{1.2\ldots i}\right)^2.$$

Je pense pouvoir supprimer la démonstration, qu'on trouvera sans peine.

4° Il n'a point été introduit jusqu'ici que la forme quadratique Φ fût réduite. Or cette condition donne, en représentant par D le déterminant $\mathrm{PR} - \mathrm{Q}^2$,

$$\mathrm{PR} < \tfrac{4}{3}\mathrm{D},$$

d'où l'on déduit la limitation

$$\mathrm{A}_i\mathrm{A}_{n-i} < \left(\frac{4}{3}\right)^{\frac{1}{2}n}(i)\,\frac{\mathrm{A}_0^2\mathrm{D}^{\frac{1}{2}n}}{(\mathrm{TU})^2}.$$

On est ainsi conduit à étudier avec attention l'expression

$$\theta = \frac{\mathrm{A}_0^2\mathrm{D}^{\frac{1}{2}n}}{(\mathrm{TU})^2},$$

et, en premier lieu, à chercher comment elle dépend des variables t, u restées entièrement arbitraires. J'observe à cet effet qu'on a

$$\mathrm{A}_0 = f(m,n) = a_0(m + \alpha_1 n)\ldots(m + \alpha_\mu n)(m + \beta_1 n)(m + \gamma_1 n)\ldots(m + \beta_\nu n)(m + \gamma_\nu n).$$

On a posé d'ailleurs

$$\mathrm{T}^2 = t^2(m + \alpha n)^2, \qquad \mathrm{U}^2 = u^2(m + \beta n)(m + \gamma n),$$

et l'on en déduit immédiatement que

$$\frac{\mathrm{A}_0^2}{(\mathrm{TU})^2} = \frac{a_0^2}{(tu)^2}.$$

En second lieu, le déterminant $PR - Q^2$ de Φ peut être remplacé par le déterminant de φ, où n'entrent que les variables t et u; on a ainsi

$$\theta = \frac{a_0^2\, D^{\frac{1}{2}n}}{(tu)^2}.$$

Telle est donc la fonction de t, u et des qualités propres seulement à la forme f, et qui sert à limiter les coefficients de toutes les formes contenues dans (f).

5° Il importe de bien voir comment cette fonction θ est liée analytiquement à la classe entière des formes équivalentes à f. A cet effet, considérons une transformée quelconque F, déduite de f par la substitution

$$x = mX + m_0 Y, \qquad y = nX + n_0 Y.$$

La fonction Θ, relative à F, s'obtiendra en remplaçant dans θ les quantités

$$a_0, \quad \alpha, \quad \beta, \quad \gamma$$

respectivement par

$$A_0, \quad a, \quad b, \quad c.$$

Mettons encore à la place des variables t et u, de θ, d'autres lettres T et U; cela fait, je dis que θ et Θ coïncideront en prenant

$$T^2 = t^2(m + \alpha n)^2, \qquad U^2 = u^2(m + \alpha n)(m + \beta n).$$

Effectivement, on trouvera comme tout à l'heure

$$\frac{A_0^2}{(TU)^2} = \frac{a_0^2}{(tu)^2}.$$

D'autre part, ainsi qu'on l'a établi précédemment, la forme quadratique Φ, composée avec F, de même que φ avec f, savoir :

$$\Phi = T_1^2(X + a_1 Y)^2 + \ldots + T_\mu^2(X + a_\mu Y)^2 + 2U_1^2(X + b_1 Y)(X + c_1 Y) + \ldots$$

ou bien, dans l'hypothèse admise,

$$\Phi = t_1^2(m + \alpha_1 n)^2(X + a_1 Y)^2 + \ldots + t_\mu^2(m + \alpha_\mu n)^2(X + a_\mu Y)^2 + \ldots$$

se déduira de φ par la substitution

$$x = mX + m_0 Y, \qquad y = nX + n_0 Y;$$

donc les déterminants de ces deux formes seront les mêmes; donc

le rapport établi entre les variables de Θ et celles de θ rend ces deux fonctions identiques.

De là se tirent deux conséquences importantes.

Premièrement : Les fonctions θ et Θ, relatives à deux formes équivalentes f et F, prennent les mêmes valeurs lorsque les variables passent par tous les états de grandeur, et ont même minimum. Ce minimum sera pour nous la définition du déterminant de la forme binaire de degré quelconque.

Secondement : Les formes quadratiques φ et Φ, déduites de deux formes différentes f et F, avec les valeurs de t et u d'une part, T et U de l'autre, qui donnent le minimum des fonctions θ et Θ, deviendront équivalentes en même temps que f et F. Ainsi, Φ se déduira de φ, par la même substitution que F de f. Pour rappeler cette propriété, nous appellerons, dorénavant, la forme quadratique φ *la correspondante de f.*

VI.

Les considérations précédentes nous conduisent à nommer *formes binaires de même déterminant* l'ensemble des fonctions homogènes de même degré, pour lesquelles le minimum absolu de la fonction θ aura une même valeur. Nous donnerons aussi le nom de *réduites* d'une forme f à la forme unique, ou aux formes de l'ensemble (f), qui correspondent à ce minimum de θ. Cela étant, on établira facilement ces propositions :

1° *Les formes équivalentes ont les mêmes réduites.*

Supposons que le minimum de la fonction θ, relative à f, s'obtienne pour les valeurs

$$t = \tau, \qquad u = \upsilon;$$

le même minimum de la fonction Θ, relative à une transformée équivalente F, déduite de f, en faisant

$$x = mX + m_0 Y, \qquad y = nX + n_0 Y,$$

correspondra aux valeurs

$$T^2 = \tau^2(m + \alpha n)^2, \qquad U = \upsilon^2(m + \beta n)(m + \gamma n).$$

Or il a été démontré plus haut que les formes de (f) et (F) correspondantes à des valeurs de t, u, T, U, liées de cette manière, étaient précisément les mêmes.

Cette proposition fait dépendre l'équivalence de deux formes, de l'égalité absolue entre les réduites, ou les groupes de réduites qui leur correspondent.

2° *Les formes à coefficients entiers, de même déterminant* θ, *se distribuent en un nombre fini de classes.*

Toutes ces formes ne donnent, en effet, qu'un nombre limité de réduites, car ces réduites étant représentées par

$$F = A_0 X^n + A_1 X^{n-1} Y + \ldots + A_{n-1} X Y^{n-1} + A_n Y^n,$$

on a, pour toutes les valeurs du nombre entier i, de zéro à n, la limitation

$$A_i A_{n-i} < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \frac{1}{n^n} \left(\frac{n.n-1\ldots n-i+1}{1.2\ldots i}\right)^2 \theta.$$

VII.

Pour première application des principes qui viennent d'être exposés, nous considérons les formes quadratiques à facteurs réels. Alors la fonction θ, comme on le voit immédiatement, est indépendante des variables t_1, t_2 et se réduit à l'expression connue du déterminant. On a alors l'exemple unique dans les formes à deux indéterminées, mais qui se reproduira dans la suite de ces recherches, et un peu plus étendu, d'un nombre infini de réduites pour une forme donnée. Effectivement, les variables t_1, t_2 restant arbitraires, les réduites d'une forme f donnent l'ensemble désigné par le symbole (f), et il s'agit maintenant de les obtenir par la réduction continuelle de la forme définie φ, lorsque les variables passent par tous les états de grandeur. Pour employer les notations habituelles, nous poserons

$$f = ax^2 + 2bxy + cy^2 = a(x+\alpha y)(x+\alpha' y);$$

on aura

$$\theta = a^2 \frac{t_1^2 t_2^2 (\alpha-\alpha')^2}{t_1^2 t_2^2} = a^2(\alpha-\alpha')^2 = 4(b^2-ac),$$

et, en introduisant dans φ le rapport $\left(\frac{t_2}{t_1}\right)^2$, qui y figure seul au fond,

$$\varphi = (x+\alpha y)^2 + \lambda(x+\alpha' y)^2;$$

de sorte que l'ensemble (f) des réduites s'obtiendra en faisant dans f toutes les substitutions propres à réduire φ, lorsque λ varie d'une manière continue de zéro à l'infini.

En restant dans le cas général, où les coefficients de f sont des quantités quelconques, nous nous fonderons d'abord sur l'observation suivante :

1° Concevons qu'on attribue aux indéterminées de φ tous les systèmes possibles de valeurs entières ; soient considérés toutefois comme distincts deux systèmes, tels que x, y et $-x$, $-y$, et qu'on range par ordre croissant de grandeur les valeurs obtenues.

On aura ainsi une suite qui dépendra de la valeur de λ, et que nous désignerons par le symbole (λ) ; en ayant soin, si plusieurs systèmes des indéterminées reproduisaient une même valeur de φ, de les réunir pour les comprendre dans un même groupe.

Cela étant, faisons croître λ d'une manière continue de zéro à l'infini positif, et cherchons comment s'introduisent des changements dans l'ordre des termes de l'ensemble (λ). J'observe à cet effet que tous ces termes sont des fonctions continues de λ, de telle sorte qu'en passant d'une valeur déterminée λ_0 à une autre infiniment voisine, $\lambda_0 + d\lambda$, on n'altérera jamais l'ordre de deux termes consécutifs, tant que leur différence sera une quantité finie. Mais supposons que les groupes formés de la réunion de deux ou plusieurs termes offrent, pour la valeur particulière λ_0, des valeurs numériques égales ; on voit clairement que deux termes réunis pour $\lambda = \lambda_0$ auront d'abord été séparés, puis auront interverti leurs rangs, en passant d'une valeur un peu inférieure à une valeur un peu supérieure à λ_0. Car, en représentant λ par une abscisse, ces deux termes seraient les ordonnées de deux droites qui, après leur intersection, changent de position relative par rapport à l'axe des x.

C'est donc toujours en devenant égaux que deux termes consécutifs échangent leurs places pour entrer dans une suite nouvelle. Avec cette observation bien simple, l'opération arithmétique de la réduction continuelle de φ, pour toutes les valeurs positives de λ, de zéro à l'infini, devient facile à saisir, comme on va le voir.

2° Prenons pour point de départ une transformée déduite de φ, dont les coefficients extrêmes soient inégaux. Ces coefficients représenteront, comme on l'a établi, les deux premiers minima de φ; donc, lorsque λ, croissant d'une manière continue, atteint la limite au delà de laquelle une nouvelle réduite vient s'offrir, l'une ou l'autre de ces deux circonstances aura nécessairement lieu. Ou bien le troisième minimum deviendra égal au second, puis le remplacera, ou bien les deux premiers minima deviendront eux-mêmes égaux et intervertiront leur ordre. Le premier cas pourra d'abord se présenter plusieurs fois de suite, mais le second finira nécessairement par arriver; car, à moins d'être indépendant de λ, un même terme ne pourrait toujours être le premier minimum. Il est évident d'ailleurs qu'il n'aura lieu qu'une seule fois; ce qui conduit à le considérer d'une manière particulière. Nous nommerons donc *réduites principales* les formes de (f), auxquelles correspondent des réduites de φ dont les coefficients extrêmes sont égaux; toutes les autres recevront le nom d'*intermédiaires*. Cela posé, lorsque, λ croissant d'une manière continue, une transformée réduite de φ cesse de l'être, par suite de l'échange du troisième minimum avec le second, la substitution propre à obtenir la réduite suivante sera nécessairement

$$x = X + Y, \qquad y = Y,$$

ou son inverse

$$x = X - Y, \qquad y = Y.$$

En effet, le coefficient de X^2 reste égal au premier minimum, et celui de Y^2 est bien le troisième, en employant la première ou la seconde substitution, selon que le coefficient moyen sera négatif ou positif. De la même manière on obtiendra donc ainsi toute réduite intermédiaire de (f) au moyen de la réduite précédente. En second lieu, si une réduite de φ cesse de l'être, par suite de l'échange des deux premiers minima, on aura la substitution

$$x = Y, \qquad y = -X.$$

Mais alors on sera parvenu à l'une des réduites principales de (f), que cette substitution changera en son associée opposée. Et en continuant les opérations, on verra de nouveau s'offrir une suite de réduites intermédiaires, puis une réduite principale suivie de son associée opposée, et ainsi jusqu'à l'infini. Nommons, pour abréger, P et Q les substitutions

$$x = X + Y, \qquad y = Y \qquad \text{et} \qquad x = Y, \qquad y = -X;$$

en partant d'une réduite principale, de rang quelconque, la substitution pour obtenir la suivante sera Q, suivie de P ou son inverse P^{-1}, prise autant de fois de suite qu'il se présentera de formes intermédiaires, c'est-à-dire QP^i, le nombre entier i étant positif ou négatif. Et, en général, on peut résumer les opérations relatives à la réduction de la forme φ, pour toutes les valeurs de λ, croissant d'une manière continue de zéro à l'infini positif dans la formule

$$\ldots QP^i QP^j QP^k \ldots.$$

3° Les formes de (f), que nous avons nommées *principales*, ont des caractères distinctifs de toutes les autres, et qu'il importe d'établir.

A cet effet, soit

$$F = AX^2 + 2BXY + CY^2 = A(X + aY)(X + a'Y)$$

une transformée quelconque de f, obtenue par la substitution

$$x = mX + m_0 Y, \qquad y = nX + n_0 Y,$$

on prouvera d'abord immédiatement que F appartiendra à (f), si la forme définie

$$\Phi = (X + aY)^2 + \lambda(X + a'Y)^2$$

est réduite, en attribuant à λ une valeur positive convenable, et cette condition est à la fois nécessaire et suffisante. Mais, si l'on veut de plus que F soit une forme principale, il faut qu'on puisse faire

$$1 + \lambda = a^2 + \lambda a'^2;$$

ainsi, l'une des quantités a et a' doit être plus grande et l'autre plus petite que l'unité. D'ailleurs, d'après la valeur de λ, Φ devient

$$\Phi = \left(\frac{a^2 - a'^2}{1 - a'^2}\right)\left(X^2 + Y^2 + 2\,\frac{1 + aa'}{a + a'}\,XY\right);$$

donc, pour que ce soit une forme réduite, on doit poser

$$4\left(\frac{1 + aa'}{a + a'}\right)^2 < 1.$$

Réciproquement, cette condition nécessaire est à elle seule suffisante, car on peut l'écrire ainsi :

$$4(1 - a^2)(1 - a'^2) + 3(a + a')^2 < 0;$$

donc, $1 - a^2$ et $1 - a'^2$ sont de signes contraires, et il est possible de prendre pour Φ la valeur particulière

$$(1-a'^2)(X+aY)^2-(1-a^2)(X+a'Y)^2=(a^2-a'^2)\left(X^2+Y^2+2\,\frac{1+aa'}{a+a'}XY\right),$$

qui est bien une forme définie réduite, dont les coefficients extrêmes sont égaux.

Ainsi, pour qu'une transformée $F=(A, B, C)$ soit une réduite principale, il faut et il suffit que la valeur absolue du coefficient moyen ne soit pas inférieure à la valeur absolue de la somme des coefficients extrêmes.

4° On a supposé implicitement, dans tout ce qui précède, qu'à une forme définie donnée corresponde toujours une réduite unique. Il en est effectivement ainsi en général; cependant nous devons tenir compte des cas d'exception, qui se présentent précisément dans les conditions précédentes, savoir, lorsque le second et le troisième, ou bien les deux premiers minima, sont égaux entre eux. On a alors deux réduites qui diffèrent seulement par le signe du coefficient moyen et, dans (f), deux formes différentes qui leur correspondent. Mais, de ces deux formes, l'une d'elles répond à la réduite unique pour une valeur de λ un peu inférieure, l'autre à la réduite unique pour une valeur de λ un peu supérieure à celle qui rend égaux les deux minima. Enfin, dans le cas plus particulier où les trois premiers minima seraient tous égaux, on aurait une forme définie proportionnelle à $x^2 \pm xy + y^2$, et susceptible de se transformer elle-même par une substitution de la forme $P^{\mp 1}Q$. Quatre formes de (f), correspondantes à cette réduite, seront alors deux principales et leurs opposées.

VIII.

Nous avons toujours supposé jusqu'ici que les coefficients de la forme quadratique f étaient des quantités quelconques. Voyons maintenant les circonstances remarquables qui se présentent lorsqu'on les suppose entiers. Alors l'ensemble (f) des réduites ne comprend plus qu'un nombre fini de formes distinctes, puisque leurs coefficients sont limités. Donc, lorsque la réduction continuelle de φ, pour des valeurs croissantes de λ, aura conduit à une

forme déjà obtenue, la nature même des opérations montre clairement qu'elles se reproduiront dès lors périodiquement en faisant croître λ jusqu'à l'infini, ou en le faisant décroître jusqu'à zéro. Ainsi (f) sera composé d'un groupe de formes en nombre fini se reproduisant une infinité de fois. Nous pouvons donc raisonner comme le fait M. Gauss, § 187, pour obtenir toutes les classes distinctes de formes de déterminant D. Calculons pour cela l'ensemble Ω des réduites principales, en employant tous les nombres A, B, C satisfaisant aux conditions

$$B^2 - AC = D, \qquad B^2 \geqq (A+C)^2,$$

et prenons l'une d'elles, F. Il résulte immédiatement de nos principes qu'à la période des réduites principales de (F) appartiendront toutes les formes équivalentes de Ω. Cette période obtenue, on prendra une autre forme G de Ω qui n'y soit pas comprise, et l'on calculera de même la période des réduites principales de (G). De là on déduira une nouvelle classe distincte de la précédente, et l'on poursuivra les mêmes opérations jusqu'à ce qu'on ait épuisé toutes les formes de Ω. Alors on aura obtenu toutes les classes différentes de déterminant D, représentées chacune, non par une forme unique, mais par une période répétée indéfiniment d'un petit nombre de réduites principales. Ces périodes ne coïncident pas absolument avec celles de M. Gauss, comme on le voit par la définition des réduites données § 183. Remarquons néanmoins qu'elles présentent, comme celles de l'illustre analyste, une série de formes dont chacune est contiguë à la précédente par la première partie. En effet, la substitution QP^i, par laquelle on passe de l'une à l'autre, est précisément le type des substitutions qui donnent une transformée contiguë. On pourrait même sans doute calculer le nombre i, par la condition que la forme contiguë soit une réduite principale; mais je laisserai cette recherche au lecteur.

IX.

Nous avons encore à présenter quelques considérations sur le problème important dont l'objet est de trouver toutes les transformations possibles de deux formes équivalentes l'une dans l'autre.