Werk

Titel: Sur l'introduction des variables continues dans la théorie des nombres.

Autor: Hermite, C.

Jahr: 1851

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0041|log16

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

13.
Sur l'introduction des variables continues dans la théorie des nombres.

(Par Mr. *C. Hermite*, examinateur d'admission à l'école polytechnique, à Paris.)

I.

Amené depuis long-temps par des recherches sur la théorie des fonctions elliptiques et Abeliennes, 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 arithm." (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 connait toute l'importance du probléme 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 tome 36 de ce journal. 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.

Soit

$$f(u) = u^n + Au^{n-1} + Bu^{n-2} + \cdots + Ku + L = 0$$

une équation irréductible à coefficients entiers, et

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

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

$$\textit{Norme}\ \{X\varphi_1(u) + Y\varphi_2(u) + \cdots + V\varphi_n(u)\}$$

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

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

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

$$\Phi = \frac{1}{\Delta}\ \textit{Norme}\ \{X\varphi_1(u) + Y\varphi_2(u) + \cdots + V\varphi_n(u)\}$$

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:

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

dont le déterminant a p' valeurs Δ, est remplacé par le suivant:

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

Les nombres entiers, désignés par les lettres, g, h, ... l, sont positifs et vérifient tous les conditions

$$g < \delta_1, \quad h < \delta_2, \quad \ldots\ldots \quad l < \delta_{n-1},$$

et on a toujours

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

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 concluerait

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

et la substitution

$$\begin{aligned} X &= -X' + Y' \\ Y &= \quad\;\; -Y' \end{aligned}$$

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

$$\begin{aligned} \pm 2B &< A \\ \pm 2B &< C \end{aligned}$$

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

$$\begin{aligned} F(x-1, y) &= F(x, y) - A(x-y) - y(A-2B) - A(x-1) \\ F(x, y-1) &= F(x, y) - C(y-x) - x(C-2B) - C(y-1) \end{aligned}$$

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:

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

dans laquelle a et $\varDelta$ sont des quantitées réelles quelconques; soit

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

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:

$$D = \frac{1}{\varDelta^2}, \quad A = (m - an)^2 + \frac{n^2}{\varDelta^2},$$

donc:

Pour une valeur donnée de $\varDelta$, on peut toujours déterminer deux entiers m et n, tels qu'on ait:

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

Or de là se tirent plusieurs conséquences:

1°. Le produit des deux facteurs $(m-an)^2$ et $\frac{n^2}{\varDelta^2}$ étant toujours inférieur à son minimum, savoir $\frac{1}{4}\left\{(m-an)^2 + \frac{n^2}{\varDelta^2}\right\}^2$, on aura a fortiori:

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

ou

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

On a d'ailleurs à la fois:

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

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 $n' < n$, entrainant $(m' - an')^2 > (m - an)^2$, 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 quelconques de x, et à des valeurs entières de y, inférieures à une limite donné, 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:

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

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

en mettant la seconde inégalité sous la forme

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

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

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

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

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

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:

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

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

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

lesquelles donnent $l = \frac{m''n' - n''m'}{m'n - mn'} = \pm 1$, 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 connue par la théorie des fractions continues; en faisant dépendre ces résultats de la seule notion de formes réduites de déterminant négatif; j'ai en 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 chaine 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 réproduire l'ouvrage même de Mr. *Gauss.* Laissant donc de côté les propositions importantes qui se rapportent à l'équivalence propre et impropre aux formes ambigues, j'arrive à la théorie des fonctions homogènes telles que

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

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:

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

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

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

la substitution qui change f en

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

posons

$$\mathrm{a} = \frac{m_0 + \alpha n_0}{m + \alpha n}, \quad \mathrm{b} = \frac{m_0 + \beta n_0}{m + \beta n}, \quad \mathrm{c} = \frac{m_0 + \gamma n_0}{m + \gamma n},$$

on aura

$$F = A_0(X + \mathrm{a}_1 Y)\ldots(X + \mathrm{a}_\mu Y).(X + \mathrm{b}_1 Y)(X + \mathrm{c}_1 Y)\ldots(X + \mathrm{b}_\nu Y)(X + \mathrm{c}_\nu Y),$$

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

$$\Phi = T_1^2(X + \mathrm{a}_1 Y)^2 + \cdots + T_\mu^2(X + \mathrm{a}_\mu Y)^2 + 2U_1^2(X + \mathrm{b}_1 Y)(X + \mathrm{c}_1 Y) + \cdots$$
$$\cdots + 2U_\nu^2(X + \mathrm{b}_\nu Y)(X + \mathrm{c}_\nu Y).$$

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

$$t = \tau, \qquad u = v:$$

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

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

Soit 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,

$$\begin{aligned} x &= mX+m_0Y \\ y &= nX+n_0Y, \end{aligned}$$

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

$$\begin{aligned} \Phi = T_1^2(X+\mathrm{a}_1Y)^2+\cdots\cdots+T_\mu^2(X+\mathrm{a}_\mu Y)^2+2U_1^2(X+\mathrm{b}_1Y)(X+\mathrm{c}_1Y)+\cdots \\ \cdots+2U_\nu^2(X+\mathrm{b}_\nu Y)(X+\mathrm{c}_\nu Y) \end{aligned}$$

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

$$\begin{aligned} F &= A_0X^n+A_1X^{n-1}Y+\cdots\cdots+A_{n-1}XY^{n-1}+A_nY^n \\ &= A_0(X+\mathrm{a}_1Y)\ldots\ldots(X+\mathrm{a}_\mu Y)(X+\mathrm{b}_1Y)(X+\mathrm{c}_1Y)\ldots(X+\mathrm{b}_\nu Y)(X+\mathrm{c}_\nu Y). \end{aligned}$$

Soit encore, pour abréger,

$$\Phi = \mathrm{P}X^2+2\mathrm{Q}XY+\mathrm{R}Y^2,$$

de sorte que

$$\begin{aligned} T_1^2+\cdots\cdots+T_\mu^2+2U_1^2+\cdots\cdots+2U_\nu^2 &= \mathrm{P} \\ \mathrm{a}_1^2T_1^2+\cdots\cdots+\mathrm{a}_\mu T_\mu^2+2\mathrm{b}_1\mathrm{c}_1U_1^2+\cdots\cdots+2\mathrm{b}_\nu\mathrm{c}_\nu U_\nu^2 &= \mathrm{R}. \end{aligned}$$

On pourra faire en général:

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

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

$$\begin{aligned} \omega_1^2+\cdots\cdots+\omega_\mu^2+2\varpi_1^2+\cdots\cdots+2\varpi_\nu^2 &= 1 \\ \varphi_1^2+\cdots\cdots+\varphi_\mu^2+2\psi_1^2+\cdots\cdots+2\psi_\nu^2 &= 1. \end{aligned}$$

Enfin nous remplacerons l'équation unique

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

par les deux suivantes:

$$bU = \psi\sqrt{R}.e^{i\lambda}, \qquad cU = \psi\sqrt{R}.e^{-i\lambda};$$

λ étant l'argument de l'imaginaire b. Cela posé, nous transformerons comme il suit, l'expression en facteurs lineaires de F. Multiplions les facteurs réels $X+aY$ par T, et chacun des facteurs imaginaires conjugués, $X+bY$, $X+cY$, par U; on aura d'abord:

$$T_1T_2\ldots.T_\mu.U_1^2U_2^2\ldots.U_\nu^2F$$
$$= A_0\ldots.(TX+aTY)(UX+bUY)(UX+cUY)\ldots.;$$

puis en introduisant les quantités ω, ϖ, φ, ψ, et représentant, pour abréger, $T_1T_2\ldots.T_\mu.U_1^2U_2^2\ldots.U_\nu^2$ par (TU):

$$F = \frac{A_0}{(TU)}\ldots.(\omega\sqrt{P}.X+\varphi\sqrt{R}.Y)(\varpi\sqrt{P}.X+e^{i\lambda}\psi\sqrt{R}.Y)$$
$$(\varpi\sqrt{P}.X+e^{-i\lambda}\psi\sqrt{R}.Y)\ldots..$$

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

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

$$A_iA_{n-i} = \frac{A_0^2(PR)^{\frac{1}{2}n}}{(TU)^2}.(i),$$

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

$$A_0A_n = \frac{A_0^2(PR)^{\frac{1}{2}n}}{(TU)^2}.\omega_1\ldots.\omega_\mu.\varphi_1\ldots.\varphi_\mu.\varpi_1^2\ldots.\varpi_\nu^2.\psi_1^2\ldots.\psi_\nu^2.$$

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 fut réduite. Or cette condition donne, en représentant par D le déterminant $PR - Q^2$,

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

d'où l'on déduit la limitation:

$$A_i A_{n-i} < (\tfrac{4}{3})^{\frac{1}{2}n}(i) \cdot \frac{A_0^2 D^{\frac{1}{2}n}}{(TU)^2}.$$

On est ainsi conduit à étudier avec attention l'expression

$$\theta = \frac{A_0^2 D^{\frac{1}{2}n}}{(TU)^2},$$

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

$$A_0 = f(m,n)$$
$$= a_0(m+\alpha_1 n)\dots(m+\alpha_\mu n)(m+\beta_1 n)(m+\gamma_1 n)\dots\dots(m+\beta_\nu n)(m+\gamma_\nu n).$$

On a posé d'ailleurs

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

et on en déduit immédiatement que

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

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 quantités 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

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

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

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

respectivement par

$$A_0, \quad \mathrm{a}, \quad \mathrm{b}, \quad \mathrm{c}.$$

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

$$\Phi = T_1^2(X+\mathrm{a}_1 Y)^2 + \cdots + T_\mu^2(X+\mathrm{a}_\mu Y)^2 + U_1^2(X+\mathrm{b}_1 Y)(X+\mathrm{c}_1 Y) + \cdots,$$

ou bien dans l'hypothèse admise:

$$\Phi = t_1^2(m+\alpha_1 n)^2(X+\mathrm{a}_1 Y)^2 + \cdots + t_\mu^2(m+\alpha_\mu n)^2(X+\mathrm{a}_\mu Y)^2 + \text{etc.},$$

se déduira de φ, par la substitution

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

donc les déterminants de ces deux formes seront les mêmes; donc le rapport établi entre les variables de Θ, et celle de θ, rend ces deux fonctions identiques.

Delà 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 de 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 désignerons 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:

$$t = \tau, \qquad u = v,$$

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

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

correspondra aux valeurs:

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

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

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

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

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

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 réproduira 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 systêmes possibles de valeurs entières; soient considérés toutefois comme distincts, deux systêmes 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'altèrera jamais l'ordre de deux termes consécutifs, tant que leur différence sera une quantité finie. Mais considérons 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 intervertis 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'arc 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 voir.

2°. Prenons pour point de départ, une transformée réduite 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 même 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

$$\begin{aligned} x &= X + Y, \\ y &= \quad\;\; Y, \end{aligned}$$

ou son inverse:

$$\begin{aligned} x &= X - Y, \\ y &= \quad\;\; Y. \end{aligned}$$

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

$$\begin{aligned} x &= \;\;\; Y, \\ y &= -X. \end{aligned}$$

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 opposée, et ainsi jusqu'à l'infini. Nommons, pour abréger, P et Q, les substitutions:

$$\begin{aligned} x &= X + Y \\ y &= \phantom{X+{}} Y \end{aligned} \quad \text{et} \quad \begin{aligned} x &= Y, \\ y &= -X; \end{aligned}$$

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. à d. 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

$$F = AX^2 + 2BXY + CY^2 = A(X + \mathrm{a}Y)(X + \mathrm{a}'Y)$$

une transformée quelconque de f, obtenue par la substitution

$$\begin{aligned} x &= mX + m_0 Y, \\ y &= nX + n_0 Y, \end{aligned}$$

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

$$\Phi = (X + \mathrm{a}Y)^2 + \lambda(X + \mathrm{a}'Y)^2,$$

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:

$$1 + \lambda = \mathrm{a}^2 + \lambda \mathrm{a}'^2;$$

ainsi l'une des deux 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

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

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

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

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

$$4(1-\mathrm{a}^2)(1-\mathrm{a}'^2)+2(\mathrm{a}^2+\mathrm{a}'^2)+(\mathrm{a}-\mathrm{a}')^2<0;$$

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

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

qui est bien une forme définie réduite, dont les coëfficients 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 surpasse pas 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 précisement dans les considérations 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'elle 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 proportionelle à $x^2\pm xy+y^2$, et susceptible de se transformer elle même par une substitution de la forme $P^{\mp1}Q$. 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 Mr. *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:

$$B^2 - AC = D,$$
$$B^2 > (A+C)^2,$$

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 on calculera de même la période des réduites principales de (G). Delà on déduira une nouvelle classe distincte de la précédente, et 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 chacunes, 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 Mr. *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. La belle solution donnée par Mr. *Gauss* §. 162, dépend d'une méthode profonde et cachée, qui, si je ne me trompe, reparaît encore dans d'autres circonstances, p. ex. dans les recherches relatives à la multiplication des classes. J'aurais plutôt, à essayer d'en pénétrer les principes, qu'à y ajouter quelque chose; aussi je me bornerai à déduire des considérations précédentes, ce cas particulier:

Le calcul de l'ensemble désigné par (f), donne toutes les transformations possibles des réduites principales et intermédiaires en elles mêmes.

Soit $F = A(x + \mathfrak{a}y)(x + \mathfrak{a}'y)$ l'une d'elles: nous savons que toutes les autres réduites s'obtiendront par la réduction continuelle de la forme définie

$$\Phi = (x + \mathfrak{a}y)^2 + \lambda(x + \mathfrak{a}'y)^2,$$

et cette forme définie, comme correspondante à F, est elle même réduite, p. ex. pour $\lambda = \lambda_0$. Soit donc:

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

la substitution qui change F, en elle même; par cette substitution la forme

$$\frac{1}{(m + \mathfrak{a}n)^2}(x + \mathfrak{a}y)^2 + \frac{\lambda_0}{(m + \mathfrak{a}'n)^2}(x + \mathfrak{a}'y)^2$$

deviendra précisément Φ, quand on y fait $\lambda = \lambda_0$; ainsi donc en réduisant la forme définie dans l'hypothèse $\lambda = \lambda_0 . \left(\frac{m + \mathfrak{a}n}{m + \mathfrak{a}'n}\right)^2$, on obtiendra bien une transformée semblable quelconque de F.

Maintenant nommons P, la substitution qui reproduit F, pour la première fois lorsque λ croît depuis la valeur λ_0, d'une manière continue, jusqu'à une certaine limite λ_1; à partir de cette limite, les opérations se reproduiront périodiquement jusqu'à l'infini; c'est donc la substitution P, prise un nombre quelconque de fois qui donnera toutes les transformations semblables. Et si l'on considère les valeurs décroissantes de λ, de λ_1 à λ_0, on aura dans un ordre inverse la même série d'opérations, qu'on pourra prolonger à l'infini, dans l'autre sens, et qui donnera pour transformations semblables la substitution inverse P^{-1}, prise de même un nombre quelconque de fois. Les mêmes choses auraient lieu relativement à la transformation de toute réduite F en $-F$, lorsque cette transformation est possible.

X.

L'équation $x^2 - Dy^2 = 1$, a une infinité de solutions.

En prenant en effet $f = x^2 - Dy^2$, on a l'une des réduites intermédiaires comprises dans (f), car la forme définie correspondante

$$(x + y\sqrt{D})^2 + \lambda(x - y\sqrt{D})^2$$

est réduite pour $\lambda = 1$. Delà résulte l'existence d'une infinité de transformations semblables, telles que

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

et toutes donnent nécessairement

$$m^2 - Dn^2 = 1.$$

Pour obtenir la loi de toutes ces solutions, nous employerons la méthode suivante. Soit $\Pi(z)$ une fonction discontinue, égale pour toutes les valeurs réelles de z, au minimum de la forme

$$e^{2z}(x + y\sqrt{D})^2 + e^{-2z}(x - y\sqrt{D})^2,$$

lorsqu'on y suppose x et y entiers. Je dis que toute solution $x = a$, $y = b$, de l'équation proposée, donnera un indice de périodicité de la fonction Π. On pourra déterminer en effet une quantité réelle ω, telle que

$$e^{\omega} = a + b\sqrt{D}, \qquad e^{-\omega} = a - b\sqrt{D},$$

et on trouvera

$$\Pi(z + \omega) = e^{2z}\left(\frac{x + y\sqrt{D}}{a - b\sqrt{D}}\right)^2 + e^{-2z}\left(\frac{x - y\sqrt{D}}{a + b\sqrt{D}}\right)^2.$$

Or on peut faire:

$$x + y\sqrt{D} = (a - b\sqrt{D})(X + Y\sqrt{D})$$
$$x - y\sqrt{D} = (a + b\sqrt{D})(X - Y\sqrt{D}),$$

car cela revient à la substitution au déterminant 1:

$$x = +aX - bDY$$
$$y = -bX + aY;$$

donc $\Pi(z + \omega)$ ne diffère pas de $\Pi(z)$.

Or la fonction discontinue $\Pi(z)$, est néanmoins par sa définition, du genre des fonctions parfaitement déterminées dans toute l'étendue des valeurs réelles de la variable: donc, d'après l'observation bien connue de Mr. *Jacobi*, tous les indices de périodicité, tels que ω, sont des multiples entiers du plus petit d'entre eux. Autrement dit: toutes les solutions $x = A$, $y = B$ de l'équation proposée, se tirent de la solution unique $x = a$, $y = b$ (pour laquelle $a + b\sqrt{D}$ est le plus petit possible) par la formule

$$A + B\sqrt{D} = (a + b\sqrt{D})^i,$$

i étant un nombre entier positif ou négatif.

Toutes ces solutions d'ailleurs s'obtiendront en cherchant effectivement les minima successifs de $\Pi(z)$, ou bien, ce qui est au fond la même chose, en formant la période de $x^2 - Dy^2$. On a en effet cette proposition plus générale:

Toute représentation de minimum absolu d'une forme à facteurs réels $f = a(x+\alpha y)(x+\alpha' y)$, sera donnée en cherchant pour des valeurs convenables de t et t', le minimum de la forme définie

$$\varphi = t^2(x+\alpha y)^2 + t'^2(x+\alpha' y)^2.$$

Supposons que f soit le plus petit possible pour

$$x = a, \qquad y = b.$$

Si le minimum de φ dans l'hypothèse suivante:

$$t = \frac{1}{a+\alpha b}, \qquad t' = \frac{1}{a+\alpha' b}$$

n'était pas donné par le même système de valeurs, c'est qu'il en existerait un autre:

$$x = A, \qquad y = B,$$

tel qu'on ait

$$\left(\frac{A+\alpha B}{a+\alpha b}\right)^2 + \left(\frac{A+\alpha' B}{a+\alpha' b}\right)^2 < 2;$$

or on en conclurait

$$\left(\frac{A+\alpha B}{a+\alpha b}\right)^2 \left(\frac{A+\alpha' B}{a+\alpha' b}\right)^2 < 1,$$

donc f ne serait pas, contre l'hypothèse, un minimum absolu pour $x = a$, $y = b$.

XI.

Mr. *Gauss* a encore déduit du développement de la période de la forme $(1, 0, -D)$, la décomposition en deux carrés du déterminant, lorsqu'il est un nombre premier $4n+1$. Ce beau résultat dépend des spéculations les plus élévées de l'Arithmétique transcendante, car il repose en entier sur cette proposition, que les formes proprement primitives de déterminant premier $4n+1$, n'ont jamais qu'une classe ambiguë. Je vais essayer cependant, sans sortir des considérations élémentaires, de donner la raison de ces rapports singuliers, entre deux points bien différents de la théorie des formes quadratiques.

Soient a et b deux nombres entiers, tels qu'on ait

$$a^2 - Db^2 = -\Delta,$$

Δ étant essentiellement positif. La période de $(1, 0, -D)$ contiendra une transformée obtenue par la réduction de la forme que nous avons nommée φ, dans l'hypothère suivante:

$$\begin{aligned}\varphi &= (x+y\sqrt{D})^2(a+b\sqrt{D})-(x-y\sqrt{D})^2(a-b\sqrt{D})\\ &= 2\sqrt{D}(b,\ a,\ bD).\end{aligned}$$

Or on obtient ainsi une forme à coefficients entiers de déterminant $-\Delta$. Soit donc

$$(\mathrm{A},\ \mathrm{B},\ \mathrm{C})$$

l'une quelconque des réduites pour ce déterminant, et

$$\begin{aligned}x &= mX+m_0Y,\\ y &= nX+n_0Y\end{aligned}$$

la substitution propre à passer de $(b,\ a,\ bD)$ à (A, B, C). Cette substitution se présentera nécessairement, pour déduire de $(1,\ 0,\ -D)$ l'une des réduites principales ou intermédiaires de sa période; soit $(A,\ B,\ C)$ cette réduite, on aura d'une part

$$AX^2+2BXY+CY^2 = (mX+m_0Y)^2-D(nX+n_0Y)^2,$$

et de l'autre

$$\begin{aligned}&\mathrm{A}X^2+2\mathrm{B}XY+\mathrm{C}Y^2\\ &= b(mX+m_0Y)^2+2a(mX+m_0Y)(nX+n_0Y)+bD(nX+n_0Y)^2;\end{aligned}$$

or on tire aisément delà l'équation suivante:

$$A\mathrm{C}+2B\mathrm{B}+C\mathrm{A} = 0,$$

dont nous allons montrer les conséquences.

Soit en effet $\Delta = 1,\ 2,\ 3,\ 4,\ 5$ etc. Au moyen des réduites connues pour ces déterminants, on trouvera successivement

$$\begin{array}{rcl} A+C=0, & & \\ 2A+C=0, & & \\ 3A+C=0 & \text{ou} & A-B+C=0,\\ 4A+C=0 & & A+C=0,\\ 5A+C=0 & & 3A-2B+2C=0,\\ \text{etc.} & & \end{array}$$

et ces relations donneront les représentations suivantes du déterminant D:

$$\begin{array}{lcl} A^2+B^2 & & \\ 2A^2+B^2 & & \\ 3A^2+B^2 & \text{ou} & B^2-AB+A^2\\ 4A^2+B^2 & & A^2+B^2\\ 5A^2+B^2 & & B^2-AB+\tfrac{3}{2}A^2. \end{array}$$

Dans la dernière A est nécessairement un nombre pair, et en écrivant $2A$ à la place de A, elle devient $B^2 - 2AB + CA^2$ ou $(B - A)^2 + 5A^2$; ainsi la représentation de D, par la forme $(1, 0, -5)$, s'obtiendra par le développement de la période de $(1, 0, D)$, toutes les fois que l'équation

$$a^2 - Db^2 = -5$$

sera possible. Mais de tous ces cas, le premier est le seul où nous puissions affirmer que la forme (A, B, C) est une réduite principale; alors en effet la relation $B^2 > (A + C)^2$ se réduit à $B^2 > 0$, qui est satisfaite d'elle-même. Le second a été l'objet de recherches de Mr. *Göpel,* auteur à jamais illustre du mémoire „Adumbratio levis theoriae functionum Abelianarum", comme on le voit dans la notice où Mr. *Jacobi* a rendu un digne hommage à sa mémoire.

Dans ce champ de recherches sur les fonctions Abeliennes, ouverte en même temps par un autre géomêtre dont il eut été l'émule, tous ceux qui suivront ses traces, trouveront à côté de leurs méditations le regret d'une destinée cruelle. Qu'il me soit permis, pour avoir eu quelques pensées en partage avec Mr. *Göpel,* de joindre l'expression sincère de ce regret, à celle de mon admiration pour son génie.

XII.

En passant des formes quadratiques à facteurs réels, aux formes de degré plus élevé, la recherche des classes distinctes pour un déterminant donné, dépend en premier lieu de la détermination du minimum de la fonction que nous avons désignée par θ. On n'a plus alors cet ensemble de circonstances analytiques remarquables que nous venons de parcourir, mais que nous retrouverons dans la théorie des formes à facteurs linéaires que nous avons définies §. II. Le fait le plus important à observer, en abordant la théorie des formes cubiques, biquadratiques etc., consiste peut-être dans l'existence pour chaque degré d'un certain nombre de formes comme celles que nous avons nommées précédemment correspondantes. Mr. *Eisenstein* a découvert le premier une correspondante du second degré pour les formes cubiques, et on peut voir le rôle qu'elle joue dans les savantes recherches sur le nombre des classes distinctes pour un déterminant donné. Nos principes, comme on va voir, conduisent directement à cette même forme.

Posons, pour employer les notations suivies:

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

on aura pour la fonction θ, deux expressions bien distinctes, l'une pour le cas où les facteurs linéaires $x+\alpha y$, $x+\alpha' y$, $x+\alpha'' y$ sont réels, savoir:

$$\theta = a^2 \cdot \frac{\{t^2 t'^2(\alpha-\alpha')^2 + t^2 t''^2(\alpha-\alpha'')^2 + t' t'^2(\alpha'-\alpha'')^2\}^{\frac{3}{2}}}{t^2 t'^2 t''^2},$$

l'autre pour le cas où $x+\alpha y$ étant réel, $x+\alpha' y$ et $x+\alpha'' y$, sont imaginaires conjugués:

$$\theta = a^2 \cdot \frac{\{2t^2 t'^2(\alpha-\alpha')(\alpha-\alpha'') - t'^4(\alpha'-\alpha'')^2\}^{\frac{3}{2}}}{t^2 t'^4}.$$

Ces deux expressions différentes peuvent néanmoins être rapprochées l'une de l'autre de la manière suivante. Faisons dans la première:

$$t^2 = \tau^2(\alpha'-\alpha'')^2, \qquad t'^2 = \tau'^2(\alpha-\alpha'')^2, \qquad t'^2 = \tau''^2(\alpha-\alpha')^2,$$

et dans la seconde:

$$t^2 = -\tau^2(\alpha'-\alpha'')^2, \qquad t'^2 = \tau'^2(\alpha-\alpha')(\alpha-\alpha''),$$

elles deviendront respectivement:

$$\theta = a^2(\alpha-\alpha')(\alpha-\alpha'')(\alpha'-\alpha'')\left\{\left(\frac{\tau\tau'}{\tau''^2}\right)^{\frac{2}{3}} + \left(\frac{\tau\tau''}{\tau'^2}\right)^{\frac{2}{3}} + \left(\frac{\tau'\tau''}{\tau^2}\right)^{\frac{2}{3}}\right\}^{\frac{3}{2}},$$

$$\theta = a^2(\alpha-\alpha')(\alpha-\alpha'')(\alpha'-\alpha'')\left\{-2\left(\frac{\tau}{\tau'}\right)^{\frac{2}{3}} - \left(\frac{\tau'^2}{\tau^2}\right)^{\frac{2}{3}}\right\}^{\frac{3}{2}}.$$

Or il est visible qu'au facteur $\sqrt{-1}$ près, la seconde valeur se déduit de la première en y supposant $\tau'' = \tau'$. D'un autre côté le minimum de l'expression

$$\left(\frac{\tau\tau'}{\tau''^2}\right)^{\frac{2}{3}} + \left(\frac{\tau\tau''}{\tau'^2}\right)^{\frac{2}{3}} + \left(\frac{\tau'\tau''}{\tau^2}\right)^{\frac{2}{3}},$$

composée de trois parties dont le produit est l'unité, s'obtiendra en rendant les variables égales, et la même hypothèse donnera la même valeur pour le minimum de la seconde fonction. Posant

$$a^4(\alpha-\alpha')^2(\alpha-\alpha'')^2(\alpha'-\alpha'')^2$$
$$= 27(-a^2d^2 + 3b^2c^2 - 4ac^3 - 4db^3 + 6abcd) = 27D,$$

on trouvera respectivement pour les minima des deux expressions, les valeurs

$$\sqrt{(3^6.D)} \quad \text{et} \quad \sqrt{(-3^6.D)},$$

et pour les formes définies auxquelles nous avons donné le nom général de correspondantes:

$$\varphi = +(\alpha'-\alpha'')^2(x+\alpha y)^2 + (\alpha-\alpha'')^2)(x+\alpha' y)^2 + (\alpha-\alpha')^2(x+\alpha'' y)^2,$$
$$\varphi = -(\alpha'-\alpha'')^2(x+\alpha y)^2 + 2(\alpha-\alpha')(\alpha-\alpha'')(x+\alpha' y)(x+\alpha'' y).$$

La différence analytique de ces deux formes, manifeste la différence de nature entre les formes cubiques à facteurs réels et à facteurs imaginaires; dans le premiers cas φ, s'exprime rationnellement par les coefficients de f, et on arrive à la forme de Mr. ***Eisenstein***, en multipliant par le facteur a^2, savoir:

$$\varphi = (ac - b^2)x^2 + (ad - bc)xy + (bd - c^2)y^2.$$

Dans le second il n'en est plus de même, et l'opération de la réduction exigera le calcul numérique de la racine réelle α. Mais les limitations des coefficients pour les transformées réduites $\mathrm{A}X^3 + 3\mathrm{B}X^2Y + 3\mathrm{C}XY^2 + \mathrm{D}Y^3$, dépendent toujours de ces formules:

$$\mathrm{AD} < (\tfrac{4}{3})^{\frac{3}{2}}\sqrt{D},$$
$$\mathrm{BC} < (\tfrac{4}{3})^{\frac{3}{2}}\sqrt{D},$$

en ayant soin de prendre la valeur absolue de D.

La correspondante à coefficients rationnels peut être aussi rattachée à une origine différente de celle que nous venons de lui donner, en la considérant comme le déterminant du système:

$$\begin{matrix} \dfrac{d^2f}{dx^2} & \dfrac{d^2f}{dx\,dy} \\[2ex] \dfrac{d^2f}{dx\,dy} & \dfrac{d^2f}{dy^2} \end{matrix},$$

et de là se déduirait une démonstration facile de sa propriété caractéristique. Mais je veux surtout faire remarquer, comment cette seconde expression conduit au théorême suivant, qu'en multipliant φ par elle-même, le produit est toujours transformable en son opposée.

Partons à cet effet des substitutions:

$$X = (ax + by)x' + (bx + cy)y',$$
$$Y = (bx + cy)x' + (cx + dy)y',$$

et représentons par φ, φ', Φ les déterminants des systèmes

$$\left\{\begin{matrix} ax + by, & bx + cy \\ bx + cy, & cx + dy \end{matrix}\right\}, \quad \left\{\begin{matrix} ax' + by', & bx' + cy' \\ bx' + cy', & cx' + dy' \end{matrix}\right\}, \quad \left\{\begin{matrix} cX - bY, & dX - cY \\ bX - aY, & cX - bY \end{matrix}\right\}.$$

On trouvera d'abord, en résolvant successivement par rapport à x', y', et x, y,

$$x' = \frac{X(cx + dy) - Y(bx + cy)}{\varphi}, \qquad y' = \frac{-(bx + cy)X + (ax + by)Y}{\varphi},$$
$$x = \frac{X(cx' + dy') - Y(bx' + cy')}{\varphi'}, \qquad y = \frac{-(bx' + cy')X + (ax' + by')Y}{\varphi'}.$$

Les deux premières formules donneront ensuite:

$$x = f\frac{y'(cX - bY) + y'(dX - cY)}{\Phi}, \qquad y = f\frac{-y'(cX - bY) + x'(-bX + aY)}{\Phi},$$

et en égalant entre elles les deux valeurs obtenues, par exemple pour x, on trouvera

$$\varphi\varphi' = \Phi.$$

Or on vérifie de suite que Φ est précisement l'opposée des deux correspondantes semblables φ et φ'; ce qui démontre la proposition énoncée.

Si de plus, le coefficient moyen étant pair, ces formes sont proprement primitives, Φ, composée de nouveau avec φ, donnera la forme principale de même déterminant; toutes les classes de formes cubiques auront une correspondante quadratique, dont la triplication donnera cette forme principale. Mais il a été établi en outre par Mr. ***Eisenstein*** qu'à toute classe quadratique $\sqrt[3]{k}$ répondait effectivement une seule et unique classe cubique, lorsque le déterminant n'avait pas de diviseur carré. Ce beau théorème montre, comme on voit, un rapport digne de remarque entre deux théories qui n'offrent au premier abord aucun point de contact.

Paris, Juillet 1850.

(La continuation prochainement.)