貴重書

LETTRES DE M. HERMITE A M. JACOBI

SUR DIFFÉRENTS OBJETS

DE LA

THÉORIE DES NOMBRES.

Opuscula mathematica de Jacobi, tome II, et *Journal de Crelle,* tome 40.

Première Lettre.

Près de deux années se sont écoulées, sans que j'aie encore répondu à la lettre pleine de bonté que vous m'avez fait l'honneur de m'écrire [1]. Aujourd'hui je viens vous supplier de me pardonner ma longue négligence et vous exprimer toute la joie que j'ai ressentie en me voyant une place dans le recueil de vos Œuvres. Depuis longtemps éloigné du travail, j'ai été bien touché d'un tel témoignage de votre bienveillance; permettez-moi, Monsieur, de croire qu'elle ne m'abandonnera pas; elle me devient encore en quelque sorte d'un plus grand prix en me sentant, après un long intervalle, ramené de nouveau à l'étude, sur la voie de quelques-unes de vos pensées.

J'ai cru voir l'origine de belles et importantes questions d'Analyse dans cette partie de votre Mémoire : *De functionibus quadrupliciter periodicis,* etc., où vous établissez l'impossibilité d'une fonction à trois périodes imaginaires. L'algorithme si singu-

[1] Cette lettre, imprimée dans le *Journal de Liouville,* Vol. XI, p. 97, et dans le premier Volume des *Opuscula mathematica,* p. 357, porte la date du 6 août 1845. JACOBI.

lier, par lequel vous réduisez à un degré de petitesse arbitraire les deux expressions

$$ma + m'a' + m''a'', \qquad mb + m'b' + m''b'',$$

n'est-il pas le premier exemple d'un mode nouveau d'approximation, où les principales questions de la théorie des fractions continues viennent se représenter, sous un point de vue plus étendu ?

Par exemple, étant données deux irrationnelles A, B, on pourra déterminer, lorsqu'elle existe, toute relation linéaire telle que

$$\mathrm{A}a + \mathrm{B}b + c = 0,$$

où a, b, c sont entiers. Qu'on prenne, en effet,

$$m\mathrm{A} - m' = \alpha, \qquad m\mathrm{B} - m'' = \beta,$$

α et β pourront devenir aussi petits que l'on voudra; d'ailleurs on en conclura

$$a\alpha + b\beta = m(\mathrm{A}a + \mathrm{B}b) - am' - bm'' = -(am' + bm'' + cm).$$

Le second membre de cette égalité est un nombre entier, donc $a\alpha + b\beta$ ne pourra diminuer au delà de l'unité sans se réduire à zéro. Ainsi le calcul des nombres, m, m', m'', poussé à cette limite, il n'y aura plus qu'à convertir $\frac{\beta}{\alpha}$ en fraction continue pour obtenir la relation cherchée.

Cherchant à appliquer le nouvel algorithme aux irrationnelles définies par des équations du troisième degré à coefficients entiers, j'ai vu s'offrir quelques questions d'une grande étendue auxquelles je me suis principalement appliqué, et qui m'ont amené à considérer la méthode d'approximation que je me proposais d'étudier, sous un point de vue bien éloigné de son origine. C'est dans quelques propriétés très élémentaires des formes quadratiques, à un nombre quelconque de variables, que j'ai rencontré les principes d'Analyse dont je vous demande la permission de vous entretenir.

J'ai tiré de ces principes une démonstration de votre beau théorème sur la décomposition des nombres premiers $5m + 1$, en quatre facteurs complexes, formés des racines cinquièmes de l'unité. Je ne sais, Monsieur, s'il me sera donné de vous suivre dans les nouvelles régions de l'Arithmétique transcendante dont

貴重書

vous avez ainsi ouvert la voie. Jusqu'ici j'ai eu plutôt en vue, dans cette recherche, l'application qui s'offre d'elle-même à la théorie de la division des fonctions abéliennes dépendant de l'intégrale $\int \frac{dx}{\sqrt{1-x^5}}$. Peut-être, d'ailleurs, trouvera-t-on là des éléments nouveaux pour cette question si difficile des lois de réciprocité des résidus de cinquième puissance, sur laquelle vous avez le premier appelé l'attention des géomètres.

Tout polynome homogène du second degré à $n+1$ variables,

$$f(x_0, x_1, \ldots, x_n),$$

peut être mis sous la forme

$$f = \frac{1}{2}\frac{df}{dx_0}x_0 + \frac{1}{2}\frac{df}{dx_1}x_1 + \ldots + \frac{1}{2}\frac{df}{dx_n}x_n.$$

Si l'on pose

$$\frac{1}{2}\frac{df}{dx_0} = X_0, \qquad \frac{1}{2}\frac{df}{dx_1} = X_1, \qquad \ldots, \qquad \frac{1}{2}\frac{df}{dx_n} = X_n,$$

en nommant D le déterminant relatif à ce système d'équations linéaires, la substitution des variables $X_0, X_1, \ldots, X_n$ conduira à un nouveau polynome que je représenterai ainsi, savoir

$$\frac{F(X_0, X_1, \ldots, X_n)}{D}.$$

Cela étant, je nommerai D le déterminant de f, et F la forme adjointe à f; on trouve ensuite aisément *que la forme adjointe à* F, *sera* $D^{n-1}f$.

La notion des formes adjointes donne le théorème suivant :

Si la forme f, à $n+1$ variables $x_0, x_1, \ldots, x_n$, se change par la substitution

$$\begin{array}{l}
\alpha y_0 + \alpha' y_1 + \alpha'' y_2 + \ldots + \alpha^{(n-1)} y_{n-1} - x_0 = 0,\\
\beta y_0 + \beta' y_1 + \beta'' y_2 + \ldots + \beta^{(n-1)} y_{n-1} - x_1 = 0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\lambda y_0 + \lambda' y_1 + \lambda'' y_2 + \ldots + \lambda^{(n-1)} y_{n-1} - x_n = 0,
\end{array}$$

en la forme g, qui n'en renferme plus que n, le déterminant relatif à g s'obtiendra par la forme adjointe F, *en donnant aux variables* $X_0, X_1, \ldots, X_n$, *respectivement, les valeurs*

représentées par les coefficients des termes $x_0, x_1, \ldots, x_n$ dans le déterminant de la substitution, ces derniers termes étant regardés comme une $(n+1)^{ième}$ colonne de coefficients.

Un autre théorème essentiel, dans mon analyse, se fonde sur la proposition, aisée à démontrer, qu'étant donnée une forme binaire (a, b, a') de déterminant négatif $-D$, et dont les coefficients ne sont plus entiers, mais des quantités quelconques, l'on peut toujours trouver deux nombres entiers premiers entre eux, α, β, tels qu'on ait

$$a\alpha^2 + 2b\alpha\beta + a'\beta^2 < \sqrt{\tfrac{4}{3}D}.$$

Quant aux formes de déterminant positif D, on obtient dans tous les cas la limite inférieure

$$a\alpha^2 + 2b\alpha\beta + a'\beta^2 < \sqrt{D}.$$

Soit actuellement $f(x_0, x_1, \ldots, x_n)$ une forme quelconque à $n+1$ variables, dont les coefficients soient entiers ou irrationnels, et dont le déterminant soit D en valeur absolue; *je dis qu'on pourra toujours trouver $n+1$ nombres entiers, $\alpha, \beta, \gamma, \ldots, \lambda$, tels qu'on ait*

$$f(\alpha, \beta, \gamma, \ldots, \lambda) < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \sqrt[n+1]{D}.$$

Supposons que ce théorème soit vrai pour les formes de n variables, on pourra démontrer qu'il est vrai aussi pour les formes de $n+1$ variables; il sera donc vrai, en général, puisqu'il a lieu pour les formes binaires. Cette démonstration se base sur le lemme :

Que l'on peut toujours déterminer n colonnes de $n+1$ nombres entiers telles qu'en ajoutant une $(n+1)^{ième}$ colonne et formant le déterminant, les coefficients multipliés dans ce déterminant par les différents termes de la $(n+1)^{ième}$ colonne soient des nombres entiers donnés.

En effet, étant proposés $n+1$ nombres entiers quelconques,

$$\alpha, \quad \beta, \quad \gamma, \quad \ldots, \quad \varkappa, \quad \lambda,$$

déterminons $a, b, c, \ldots, k$ d'une part, $c', d', \ldots, k'$ de l'autre, par les équations

$$a\beta - b\alpha = \alpha_1, \qquad c'\gamma - c\pi_1 = \pi_2, \qquad \ldots, \qquad k'\varkappa - k\pi_{n-2} = \pi_{n-1},$$

où π_1 désigne le plus grand commun diviseur de α et β, π_2 le plus grand commun diviseur de γ et $\pi_1, \ldots, \pi_{n-1}$ le plus grand commun diviseur de π_{n-2} et $\varkappa$, on saura prouver *que le déterminant du système*

$$\begin{array}{cccccccc}
(0) & \dfrac{\beta}{\pi_1} & \dfrac{b\gamma}{\pi_2} & \dfrac{bc\delta}{\pi_3} & \dfrac{bcd\varepsilon}{\pi_4} & \ldots & bcd\ldots k.\lambda, \\
(1) & -\dfrac{\alpha}{\pi_1} & -\dfrac{a\gamma}{\pi_2} & -\dfrac{ac\delta}{\pi_3} & -\dfrac{acd\varepsilon}{\pi_4} & \ldots & -acd\ldots k.\lambda, \\
(2) & 0 & \dfrac{\pi_1}{\pi_2} & \dfrac{c'\delta}{\pi_3} & \dfrac{c'd\varepsilon}{\pi_4} & \ldots & c'd\ldots k.\lambda, \\
(3) & 0 & 0 & -\dfrac{\pi_2}{\pi_3} & -\dfrac{d'\varepsilon}{\pi_4} & \ldots & -d'\ldots k.\lambda, \\
\ldots & . & . & .. & \ldots & \ldots & \ldots\ldots\ldots\ldots, \\
(n) & 0 & 0 & 0 & 0 & \ldots & (-1)^n \pi_{n-1},
\end{array}$$

est (¹)

$$\alpha(0) + \beta(1) + \gamma(2) + \ldots + \lambda(n).$$

Ce lemme, joint au théorème ci-dessus, fait voir que, *si l'on déduit d'une forme f, de $n+1$ variables, une autre f_0 de n variables, en substituant aux $n+1$ variables des fonctions linéaires de n variables affectées de coefficients entiers, on pourra choisir ces fonctions à substituer de manière que le déterminant de f_0 devienne*

$$F(\alpha, \beta, \ldots, \lambda),$$

F *étant la forme adjointe de f et $\alpha, \beta, \ldots, \lambda$ des entiers donnés à l'arbitraire.*

L'adjointe de F étant $D^{n-1}f$, on pourra donc aussi déduire de F une forme de n variables F_0 dont le déterminant sera

$$D^{n-1} f(\alpha, \beta, \ldots, \lambda),$$

$\alpha, \beta, \ldots, \lambda$ étant des entiers donnés quelconques. Donc, dans l'hypothèse admise pour des formes de n variables, la forme F_0 et,

(¹) Il faudrait mettre $(-1)^{\frac{n(n+1)}{2}}$ devant la somme ci-dessus, mais ce facteur est sans importance pour la suite. E. P.

par suite, la forme F elle-même pourront prendre une valeur moindre que

$$\left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{D^{n-1} f(\alpha, \beta, \ldots, \lambda)},$$

valeur que je désignerai par $F(\alpha_0, \beta_0, \ldots, \lambda_0)$. On prouve de la même manière que f pourra prendre une valeur moindre que

$$\left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{F(\alpha_0, \beta_0, \ldots, \lambda_0)},$$

valeur que je désignerai par $f(\alpha', \beta', \ldots, \lambda')$. On aura donc

$$f(\alpha', \beta', \ldots, \lambda') < \left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{F(\alpha_0, \beta_0, \ldots, \lambda_0)},$$

$$F(\alpha_0, \beta_0, \ldots, \lambda_0) < \left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{D^{n-1} f(\alpha, \beta, \ldots, \lambda)},$$

et, par suite,

$$f(\alpha', \beta', \ldots, \lambda') < \left(\frac{4}{3}\right)^{\frac{n^2-1}{2n}} \sqrt[n^2]{D^{n-1} f(\alpha, \beta, \ldots, \lambda)}.$$

En continuant de la même manière, et en posant

$$f(\alpha^{(i)}, \beta^{(i)}, \ldots, \lambda^{(i)}) = f^{(i)}, \qquad f(\alpha, \beta, \ldots, \lambda) = f^{(0)},$$

$$\left(\frac{4}{3}\right)^{\frac{n^2-1}{2n}} \sqrt[n^2]{D^{n-1}} = l,$$

on trouvera successivement

$$f' < l\sqrt[n^2]{f^{(0)}}, \quad f'' < l\sqrt[n^2]{f'}, \quad \ldots, \quad f^{(m)} < l\sqrt[n^2]{f^{(m-1)}},$$

d'où suit

$$f^{(m)} < l^{1 + \frac{1}{n^2} + \frac{1}{n^4} + \ldots + \frac{1}{n^{2(m-1)}}} \sqrt[n^{2m}]{f^{(0)}}.$$

On pourra donc, en prenant m assez grand, parvenir à une valeur de f,

$$f^{(m)} < l^{\frac{n^2}{n^2-1}} \quad \text{ou} \quad f^{(m)} < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \sqrt[n+1]{D},$$

ce qu'il fallait démontrer (¹).

(¹) M. Hermite fait dans le post-scriptum quelques observations complémen-

De nombreuses questions me semblent dépendre des résultats précédents. Voici, en premier lieu, comment j'ai essayé d'y ramener votre nouveau mode d'approximation :

A et B étant les quantités données, je considère la forme ternaire

$$f = (x' - \mathrm{A}x)^2 + (x'' - \mathrm{B}x)^2 + \frac{x^2}{\Delta},$$

dont le déterminant est une quantité positive quelconque $\frac{1}{\Delta}$. Pour toutes les valeurs de Δ, on saura déterminer trois nombres entiers, m, m', m'', tels qu'on ait

$$(m' - \mathrm{A}m)^2 + (m'' - \mathrm{B}m)^2 + \frac{m^2}{\Delta} < \frac{4}{3}\,\frac{1}{\sqrt[3]{\Delta}},$$

et, par suite,

$$m' - \mathrm{A}m < \frac{2}{\sqrt{3}}\,\frac{1}{\sqrt[6]{\Delta}}, \quad m'' - \mathrm{B}m < \frac{2}{\sqrt{3}}\,\frac{1}{\sqrt[6]{\Delta}}, \quad m < \frac{2}{\sqrt{3}}\,\sqrt[3]{\Delta}.$$

Les deux premières relations font voir qu'on peut rendre simultanément d'un degré de petitesse arbitraire, $m' - \mathrm{A}m$, $m'' - \mathrm{B}m$; la troisième donne la mesure précise de l'ordre d'approximation des fractions $\frac{m'}{m}$, $\frac{m''}{m}$, en montrant que l'erreur est proportionnelle à $\frac{1}{m\sqrt{m}}$. Enfin, la forme adjointe de f étant

$$(x + \mathrm{A}x' + \mathrm{B}x'')^2 + \frac{x'^2 + x''^2}{\Delta},$$

le calcul conduit encore à une suite de nombres entiers, tels que α, β, γ qui rendent la fonction linéaire $\mathrm{A}\alpha + \mathrm{B}\beta + \gamma$ de l'ordre $\frac{1}{\alpha^2}$ ou $\frac{1}{\beta^2}$, et l'on démontre que, s'il existe une relation telle que $\mathrm{A}a + \mathrm{B}b + c = 0$, a, b, c étant entiers, on verra la fonction $\mathrm{A}a + \mathrm{B}b + c$ s'offrir nécessairement à partir d'une certaine valeur de Δ, puis se reproduire indéfiniment, pour toutes les valeurs plus grandes.

---

taires sur cette démonstration. Remarquons que, s'il s'agit d'une forme indéfinie dont les coefficients ne sont pas entiers, la démonstration n'exclut pas que la forme puisse se rapprocher indéfiniment de la limite indiquée, en lui restant supérieure; mais on est certain que le minimum de la forme est aussi voisin de $\left(\frac{4}{3}\right)^{\frac{n}{2}} \sqrt[n+1]{\mathrm{D}}$ que l'on veut. E. P.

Voici d'autres conséquences :

Soit

$$\mathrm{F}(x) = x^n + \mathrm{A}x^{n-1} + \ldots + \mathrm{K}x + \mathrm{L} = 0$$

une équation quelconque irréductible à coefficients entiers et dont α, β, $\ldots$, λ soient les racines; si la congruence $\mathrm{F}(x) \equiv 0$ admet une solution $x \equiv a$ pour un certain module N, en posant

$$\varphi(\alpha) = \mathrm{N}x_0 + (\alpha - a)x_1 + (\alpha^2 - a^2)x_2 + \ldots + (\alpha^{n-1} - a^{n-1})x_{n-1},$$

x_0, x_1, $\ldots$ désignant des entiers, la forme

$$\mathfrak{f} = \varphi(\alpha)\varphi(\beta)\ldots\varphi(\lambda)$$

représentera toujours des nombres entiers multiples de N : or je dis qu'on pourra trouver une infinité de systèmes de valeurs de x_0, x_1, $\ldots$, x_{n-1} pour lesquelles on ait

$$\mathfrak{f} = \mathrm{MN},$$

l'entier M étant au-dessous de la limite,

$$\left(\frac{4}{3}\right)^{\frac{1}{4}n(n-1)} \left(\frac{\Delta}{n^n}\right)^{\frac{1}{2}},$$

dans laquelle Δ représente le produit des $n(n-1)$ différences des racines α, β, $\ldots$, λ prises deux à deux.

Supposons en premier lieu, les racines α, β, $\ldots$, λ réelles; je considère la forme quadratique à n variables

$$f = \mathrm{D}_0\varphi^2(\alpha) + \mathrm{D}_1\varphi^2(\beta) + \ldots + \mathrm{D}_{n-1}\varphi^2(\lambda),$$

où D_0, D_1, $\ldots$, D_{n-1} sont essentiellement positifs : soit D le déterminant de f, on saura trouver pour x_0, x_1, $\ldots$, x_{n-1}, un système de valeurs entières telles qu'on ait

$$f = \omega\left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{\mathrm{D}},$$

ω étant moindre que l'unité. Or le produit des quantités positives $\mathrm{D}_0\varphi^2\alpha$, $\mathrm{D}_1\varphi^2\beta$, $\ldots$ ne pourra jamais dépasser son maximum $\left(\frac{f}{n}\right)^n$, correspondant au cas où elles sont toutes égales; on aura donc

$$D_0 D_1 \ldots D_{n-1}\,\mathfrak{f}^2 < \left(\frac{4}{3}\right)^{\frac{1}{2}n(n-1)} \frac{D}{n^n}.$$

Il faut ici obtenir D, qui est le déterminant relatif au système des équations linéaires dont les premiers membres seraient

$$\frac{1}{2}\frac{df}{dx_0},\quad \frac{1}{2}\frac{df}{dx_1},\quad \ldots,\quad \frac{1}{2}\frac{df}{dx_{n-1}}.$$

Or on trouve sans difficulté

$$D = \Delta D_0 D_1 \ldots D_{n-1} N^2,$$

ce qui conduit à la limite annoncée.

Comme il ne reste dans le résultat aucune trace des quantités $D_0, D_1, \ldots, D_{n-1}$, il suit qu'en leur attribuant toutes les valeurs possibles, *les mêmes multiples de* N *se reproduiront nécessairement une infinité de fois, pour une infinité de systèmes de valeurs distinctes de* $x_0, x_1, \ldots, x_{n-1}$.

Si l'équation proposée, $F(x) = 0$, n'a plus toutes ses racines réelles, on fera correspondre dans la forme f, à chaque couple de racines conjuguées α, β, le produit $D_0\varphi(\alpha)\varphi(\beta)$, au lieu de $D_0\varphi^2(\alpha) + D_1\varphi^2(\beta)$. Dans le cas où toutes les racines seraient imaginaires, ce qui suppose le degré un nombre pair $n = 2\mu$, on sera conduit de la sorte à la forme

$$f = D_0\varphi(\alpha)\varphi(\beta) + D_1\varphi(\gamma)\varphi(\delta) + \ldots + D_{\mu-1}\varphi(\varkappa)\varphi(\lambda).$$

Le déterminant s'obtient aussi dans ce cas aisément, et l'on trouve

$$D = (D_0 D_1 \ldots D_{\mu-1})^2 \frac{\Delta}{2^n} N^2.$$

Comme on a, d'ailleurs,

$$D_0 D_1 \ldots D_{\mu-1}\,\mathfrak{f} < \left(\frac{f}{\mu}\right)^{\mu}$$

et

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

on en tire la limite

$$M < \left(\frac{4}{3}\right)^{\frac{1}{4}n(n-1)} \left(\frac{\Delta}{n^n}\right)^{\frac{1}{2}},$$

qui ne diffère pas de celle que nous venons d'obtenir dans le cas des racines réelles.

Supposons que l'équation proposée soit

$$\frac{x^p - 1}{x - 1} = 0,$$

qui donne lieu à une congruence soluble pour tout module premier $N = kp + 1$; Δ sera alors p^{p-2}. Ainsi dans le cas de $p = 5$, on aura la limite

$$\left(\frac{4}{3}\right)^3 \left(\frac{5^3}{4^4}\right)^{\frac{1}{2}}$$

laquelle est > 1 mais < 2, donc on aura précisément

$$\mathfrak{f} = N.$$

C'est, comme vous voyez, Monsieur, la démonstration de votre théorème.

Mais il y a plus. Prenant $p = 7$, on trouve l'expression

$$\left(\frac{4}{3}\right)^{\frac{15}{2}} \left(\frac{7^5}{6^6}\right)^{\frac{1}{2}},$$

qui est moindre que 6. Or, la forme $\mathfrak{f}$ étant toujours $\equiv 0$ ou 1 suivant le module 7, on ne pourra avoir encore dans ce cas que $\mathfrak{f} = N$.

Considérons, en second lieu, l'équation $F(z) = 0$, qui a pour racines les $\frac{1}{2}(p-1)$ périodes de deux racines de $\frac{x^p - 1}{x - 1} = 0$; on aura la proposition que la congruence $F(z) \equiv 0$ est résoluble pour tout module premier $N = kp - 1$. On trouvera alors

$$\Delta = p^{\frac{1}{2}(p-3)},$$

d'où l'on tirera comme ci-dessus la limite de M. Dans le cas de $p = 7$, $n = 3$, il vient

$$M < \left(\frac{4}{3}\right)^{\frac{3}{2}} \left(\frac{7^2}{3^3}\right)^{\frac{1}{2}}$$

et, par suite, $M < 3$. Or il est facile de voir que suivant le module 7 la forme $\mathfrak{f}$ est toujours $\equiv 0, 1$, ou -1. On ne peut donc admettre que $M = 1$.

貴重書

De là résulte ce théorème :

Que tout nombre premier $7m - 1$ est décomposable en trois facteurs complexes formés des racines de l'équation

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

En réfléchissant aux questions précédentes j'ai été conduit à m'occuper de la théorie de la *réduction* des formes quadratiques à un nombre quelconque de variables, qui m'a semblé devoir être introduite dans l'étude des expressions telles que f. De même que pour les formes binaires, on obtient ce résultat que, pour un déterminant donné, elles se laissent distribuer en un nombre toujours fini de classes. La méthode de réduction devra reposer encore sur l'emploi de substitutions linéaires à coefficients entiers, et au déterminant ± 1, par lesquelles une forme donnée est changée en une autre entièrement équivalente et de même déterminant. Voici quelques réflexions sur ce sujet.

Soient d'abord

$$\begin{aligned} x_0 &= \alpha X_0 + \alpha' X_1 + \alpha'' X_2 + \ldots + \alpha^{(n)} X_n, \\ x_1 &= \beta X_0 + \beta' X_1 + \beta'' X_2 + \ldots + \beta^{(n)} X_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n &= \lambda X_0 + \lambda' X_1 + \lambda'' X_2 + \ldots + \lambda^{(n)} X_n \end{aligned}$$

les substitutions qui changent $f(x_0, x_1, \ldots, x_n)$ en la forme équivalente et de même déterminant $F(X_0, X_1, \ldots, X_n)$. Nommons

$$g(y_0, y_1, \ldots, y_n), \qquad G(Y_0, Y_1, \ldots, Y_n),$$

les formes adjointes respectivement à f et F; par la définition même donnée ci-dessus des formes adjointes, on prouve très facilement que l'on aura

$$g(y_0, y_1, \ldots, y_n) = G(Y_0, Y_1, \ldots, Y_n),$$

en posant

$$\begin{aligned} Y_0 &= \alpha y_0 + \beta y_1 + \ldots + \lambda y_n, \\ Y_1 &= \alpha' y_0 + \beta' y_1 + \ldots + \lambda' y_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ Y_n &= \alpha^{(n)} y_0 + \beta^{(n)} y_1 + \ldots + \lambda^{(n)} y_n. \end{aligned}$$

Il suit de cette proposition que, si dans la forme f on change seulement les n variables $x_1, x_2, \ldots, x_n$ en d'autres $X_1, X_2, \ldots, X_n$,

pour obtenir la transformation correspondante de la forme adjointe, on aura à changer seulement les n variables $y_1, y_2, \ldots, y_n$ en d'autres $Y_1, Y_2, \ldots, Y_n$, et réciproquement. D'où l'on voit *qu'en changeant dans la forme adjointe les n variables $y_1, y_2, \ldots, y_n$ en d'autres $Y_1, Y_2, \ldots, Y_n$ par la transformation correspondante de la forme proposée, le coefficient de x_0^2 ne sera pas altéré.*

Changeant au contraire, dans la forme proposée, la seule variable x_0 en X par la substitution

$$x_0 = X + \alpha' x_1 + \alpha'' x_2 + \ldots + \alpha^{(n)} x_n,$$

les substitutions correspondantes à faire dans la forme adjointe seront

$$y_1 = Y_1 - \alpha' y_0, \qquad y_2 = Y_2 - \alpha'' y_0, \qquad \ldots, \qquad y_n = Y_n - \alpha^{(n)} y_0.$$

D'où l'on voit *qu'en changeant, dans la forme proposée, la seule variable x_0 par la transformation correspondante de la forme adjointe ne seront altérés que les termes multipliés par y_0 et y_0^2.*

Voici le résultat que j'ai obtenu au moyen de ces lemmes :

Nommons réduite *une forme*

$$F(X_0, X_1, \ldots, X_n)$$

du déterminant D, *telle, en premier lieu, qu'en faisant*

$$\frac{1}{2}\frac{dF}{dX_0} = AX_0 + BX_1 + CX_2 + \ldots + LX_n$$

on ait (1)

$$A < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \sqrt[n+1]{D}, \quad B < \frac{1}{2}A, \quad C < \frac{1}{2}A, \quad \ldots, \quad L < \frac{1}{2}A,$$

telle encore que la forme adjointe à F, $G(Y_0, Y_1, \ldots, Y_n)$, *représente pour* $Y_0 = 0$, *elle aussi, une forme réduite : si l'on sait ramener les formes d'ordre n à des formes équivalentes*

(1) Ces inégalités et, en général, celles que l'on rencontrera dans les questions de réduction sont relatives aux valeurs absolues, et D représente la valeur absolue du discriminant de la forme. E. P.

貴重書

réduites, on saura aussi ramener à des formes équivalentes réduites les formes d'ordre $n+1$.

En effet, lorsqu'on se propose de changer la forme donnée f dans une autre équivalente $f_1(x'_0, x'_1, \ldots, x'_n)$, au moyen de la substitution,

$$\begin{aligned} x_0 &= \alpha x'_0 + \alpha' x'_1 + \ldots + \alpha^{(n)} x'_n, \\ x_1 &= \beta x'_0 + \beta' x'_1 + \ldots + \beta^{(n)} x'_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n &= \lambda x'_0 + \lambda' x'_1 + \ldots + \lambda^{(n)} x'_n, \end{aligned}$$

on peut prendre pour $\alpha, \beta, \ldots, \lambda$ des entiers quelconques sans commun diviseur, puisqu'on sera toujours maître de déterminer les autres nombres $\alpha', \beta', \ldots, \lambda', \alpha'', \beta'', \ldots$, de manière que le déterminant des $(n+1)^2$ coefficients soit égal à ± 1 [1]. Prenons donc pour $\alpha, \beta, \ldots, \lambda$ les entiers sans commun diviseur par lesquels on peut satisfaire à l'inégalité

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

en nommant A le coefficient de x'^2_0 dans la transformée f_1, on aura

$$A = f(\alpha, \beta, \ldots, \lambda)$$

et, par suite,

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

La forme $f(x_0, x_1, \ldots, x_n)$ étant transformée dans la forme équivalente $f_1(x'_0, x'_1, \ldots, x'_n)$, supposons en même temps la forme adjointe à f,

$$g(y_0, y_1, \ldots, y_n)$$

transformée dans l'adjointe à f_1,

$$g_1(Y_0, y'_1, y'_2, \ldots, y'_n).$$

Faisons ensuite dans cette dernière $Y_0 = 0$, et ramenons la forme d'ordre n,

$$g_1(0, y'_1, y'_2, \ldots, y'_n),$$

[1] M. Hermite avait ajouté à sa Lettre la résolution la plus générale de ce problème, publiée depuis dans le *Journal de Liouville*, vol. XIV, p. 21.

à une forme équivalente réduite aux variables $y''_1, y''_2, \ldots, y''_n$. Supposons que par la même substitution la forme $g_1(Y_0, y'_1, y'_2, \ldots, y'_n)$ soit changée en $g_2(Y_0, y''_1, y''_2, \ldots, y''_n)$; cette forme représentera, pour $Y_0 = 0$, la forme réduite d'ordre n. Transformons en même temps la forme $f_1(x'_0, x'_1, \ldots, x'_n)$, dont g_1 est l'adjointe, dans la forme $f_2(x'_0, X_1, X_2, \ldots, X_n)$, dont l'adjointe est g_2. De ce qu'on a remarqué ci-dessus il suit que, par cette dernière transformation, le coefficient de x'^2_0, A, ne sera pas altéré. Enfin, faisons

$$x'_0 = X_0 + m_1 X_1 + m_2 X_2 + \ldots + m_n X_n,$$
$$y''_1 = Y_1 - m_1 Y_0, \qquad y''_2 = Y_2 - m_2 Y_0, \qquad \ldots, \qquad y''_n = Y_n - m_n Y_0,$$

et supposons que par ces substitutions f_2 et g_2 soient changées respectivement en

$$F(X_0, X_1, X_2, \ldots, X_n) \quad \text{et} \quad G(Y_0, Y_1, Y_2, \ldots, Y_n);$$

le coefficient de X_0^2 dans F sera encore A et la forme G représentera encore pour $Y_0 = 0$ la réduite d'ordre n. Or, posant

$$\frac{1}{2}\frac{\partial f_2}{\partial x'_0} = A x'_0 + b X_1 + c X_2 + \ldots + l X_n,$$
$$\frac{1}{2}\frac{\partial F}{\partial X_0} = A X_0 + B X_1 + C X_2 + \ldots + L X_n,$$

on aura

$$\frac{\partial f_2}{\partial x'_0} = \frac{\partial F}{\partial X_0}$$

et, par suite,

$$B = b + m_1 A, \qquad C = c + m_2 A, \qquad \ldots, \qquad L = l + m_n A.$$

Donc, $m_1, m_2, \ldots, m_n$ pouvant être des entiers quelconques, on saura les déterminer de manière qu'on ait

$$B < \tfrac{1}{2}A, \quad C < \tfrac{1}{2}A, \quad \ldots, \quad L < \tfrac{1}{2}A,$$

et l'on aura satisfait à toutes les conditions.

Je remarquerai à présent *qu'étant donnés*

$$\frac{\partial F}{\partial X_0} \quad \text{et} \quad G(0, Y_1, Y_2, \ldots, Y_n),$$

en même temps que le déterminant D *de* F, *on connaîtra la forme* $G(Y_0, Y_1, \ldots, Y_n)$ *et, par suite,* $F(X_0, X_1, \ldots, X_n)$.

En effet, soit

$$\begin{aligned}
\mathrm{F} = {} & \mathrm{X}_0(\mathrm{A}\mathrm{X}_0 + \mathrm{B}\mathrm{X}_1 + \mathrm{C}\mathrm{X}_2 + \ldots + \mathrm{L}\mathrm{X}_n)\\
& + \mathrm{X}_1(\mathrm{B}\mathrm{X}_0 + \mathrm{B}'\mathrm{X}_1 + \mathrm{C}'\mathrm{X}_2 + \ldots + \mathrm{L}'\mathrm{X}_n)\\
& + \mathrm{X}_2(\mathrm{C}\mathrm{X}_0 + \mathrm{C}'\mathrm{X}_1 + \mathrm{C}''\mathrm{X}_2 + \ldots + \mathrm{L}''\mathrm{X}_n)\\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
& + \mathrm{X}_n(\mathrm{L}\mathrm{X}_0 + \mathrm{L}'\mathrm{X}_1 + \mathrm{L}''\mathrm{X}_2 + \ldots + \mathrm{L}^{(n)}\mathrm{X}_n),\\
\mathrm{G} = {} & \mathrm{Y}_0[(\mathrm{A})\mathrm{Y}_0 + (\mathrm{B})\mathrm{Y}_1 + \ldots + (\mathrm{L})\mathrm{Y}_n]\\
& + \mathrm{Y}_1[(\mathrm{B})\mathrm{Y}_0 + (\mathrm{B}')\mathrm{Y}_1 + \ldots + (\mathrm{L}')\mathrm{Y}_n]\\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
& + \mathrm{Y}_n[(\mathrm{L})\mathrm{Y}_0 + (\mathrm{L}')\mathrm{Y}_1 + \ldots + (\mathrm{L}^{(n)})\mathrm{Y}_n];
\end{aligned}$$

on aura

$$\begin{aligned}
&\mathrm{A}(\mathrm{A}) + \mathrm{B}(\mathrm{B}) + \mathrm{C}(\mathrm{C}) + \ldots + \mathrm{L}(\mathrm{L}) = \mathrm{D},\\
&\mathrm{A}(\mathrm{B}) + \mathrm{B}(\mathrm{B}') + \mathrm{C}(\mathrm{C}') + \ldots + \mathrm{L}(\mathrm{L}') = 0,\\
&\mathrm{A}(\mathrm{C}) + \mathrm{B}(\mathrm{C}') + \mathrm{C}(\mathrm{C}'') + \ldots + \mathrm{L}(\mathrm{L}'') = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\mathrm{A}(\mathrm{L}) + \mathrm{B}(\mathrm{L}') + \mathrm{C}(\mathrm{L}'') + \ldots + \mathrm{L}(\mathrm{L}^{(n)}) = 0.
\end{aligned}$$

Or, étant donnés $\frac{\partial \mathrm{F}}{\partial \mathrm{X}_0}$ et $\mathrm{G}(0, \mathrm{Y}_1, \ldots, \mathrm{Y}_n)$, on connaîtra

$$\mathrm{A},\quad \mathrm{B},\quad \mathrm{C},\quad \ldots,\quad \mathrm{L}$$

et tous les n^2 coefficients (B'), (C'), ..., d'où l'on déduira, par les n dernières équations, les valeurs des coefficients

$$(\mathrm{B}),\quad (\mathrm{C}),\quad \ldots,\quad (\mathrm{L}),$$

et par la première, D étant aussi donné, celle du coefficient (A). On connaîtra donc tous les coefficients de $\mathrm{G}(\mathrm{Y}_0, \mathrm{Y}_1, \ldots, \mathrm{Y}_n)$ et, par suite, ceux de $\mathrm{F}(\mathrm{X}_0, \mathrm{X}_1, \ldots, \mathrm{X}_n)$.

Par ce qui précède on prouve aisément que *les formes d'un ordre quelconque, attachées à un même déterminant, peuvent être ramenées à un nombre fini d'entre elles* [1]. Et d'abord il suit des conditions ci-dessus que les coefficients A, B, ..., L ne pourront prendre qu'un nombre fini de valeurs, ensuite le déterminant de la forme $\mathrm{G}(0, \mathrm{Y}_1, \mathrm{Y}_2, \ldots, \mathrm{Y}_n)$ étant $\mathrm{D}^{n-1}\mathrm{A}$, s'il est démontré que les formes d'ordre n d'un même déterminant peuvent être ramenées à un nombre fini d'entre elles, on n'aura pour chaque valeur de A qu'un nombre limité de formes $\mathrm{G}(0, \mathrm{Y}_1, \mathrm{Y}_2, \ldots, \mathrm{Y}_n)$.

[1] M. Hermite suppose ici implicitement qu'il s'agit de formes à coefficients entiers. E. P.

Or, par les nombres A, B, ..., L et la forme $\mathrm{G}(0, \mathrm{Y}_1, \mathrm{Y}_2, \ldots, \mathrm{Y}_n)$, étant déterminée la forme d'ordre $n+1$, $\mathrm{F}(\mathrm{X}_0, \mathrm{X}_1, \ldots, \mathrm{X}_n)$, ces formes aussi seront en nombre fini. Ainsi, la proposition étant admise pour les formes d'ordre n, elle sera démontrée pour les formes d'ordre $n+1$. Elle est donc vraie en général, puisqu'elle a lieu pour les formes binaires.

Vous voyez, Monsieur, que j'omets tout à fait le cas important où l'on a $\mathrm{A} = 0$; mais cette circonstance n'est point à considérer, lorsqu'on se propose seulement de poursuivre les rapports que j'ai essayé d'établir entre les formes quadratiques définies et les expressions désignées ci-dessus par $\mathfrak{f}$. Les résultats précédents me semblent alors ouvrir un vaste champ de recherches, mais dans lequel je n'ai presque fait jusqu'ici qu'entrevoir une longue série de questions et de problèmes difficiles à résoudre.

Convenons d'abord des notations suivantes, savoir :

$$\mathfrak{f} = f(\omega_0)\,f(\omega_1)\ldots f(\omega_n),$$

en prenant

$$f(\omega) = x_0\varphi_0(\omega) + x_1\varphi_1(\omega) + \ldots + x_n\varphi_n(\omega),$$

$\varphi_i(\omega)$ désignant la fonction à coefficients entiers

$$a_i + b_i\omega + c_i\omega^2 + \ldots + l_i\omega^n,$$

et les quantités $\omega_0, \omega_1, \ldots, \omega_n$ étant toujours les racines d'une même équation irréductible à coefficients entiers et dont celui de la plus haute puissance est l'unité. Je considère ensuite (dans le cas où toutes les racines sont réelles) la forme quadratique définie, d'ordre $n+1$,

$$\mathrm{f} = \mathrm{D}_0 f^2(\omega_0) + \mathrm{D}_1 f^2(\omega_1) + \ldots + \mathrm{D}_n f^2(\omega_n),$$

où $\mathrm{D}_0, \mathrm{D}_1, \ldots, \mathrm{D}_n$ sont supposés essentiellement positifs. En nommant Ω le produit des $n(n+1)$ différences des racines ω prises deux à deux, et Δ le déterminant du système

$$\begin{matrix}
a_0, & a_1, & \ldots, & a_n,\\
b_0, & b_1, & \ldots, & b_n,\\
\ldots & \ldots & \ldots & \ldots,\\
l_0, & l_1, & \ldots, & l_n,
\end{matrix}$$

on trouvera, pour le déterminant de f, l'expression

$$\mathrm{D} = \mathrm{D}_0\mathrm{D}_1\ldots\mathrm{D}_n\Delta^2\Omega.$$

貴重書

Cela posé, faisons la substitution

$$\begin{aligned} x_0 &= \alpha X_0 + \alpha' X_1 + \ldots + \alpha^{(n)} X_n, \\ x_1 &= \beta X_0 + \beta' X_1 + \ldots + \beta^{(n)} X_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n &= \lambda X_0 + \lambda' X_1 + \ldots + \lambda^{(n)} X_n, \end{aligned}$$

les coefficients étant déterminés par la méthode exposée tout à l'heure, de manière à réduire la forme adjointe à f. En posant, pour abréger,

$$\begin{aligned} \Phi_i(\omega) &= \alpha^{(i)}\varphi_0(\omega) + \beta^{(i)}\varphi_1(\omega) + \ldots + \lambda^{(i)}\varphi_n(\omega), \\ \mathfrak{F}(\omega) &= X_0\Phi_0(\omega) + X_1\Phi_1(\omega) + \ldots + X_n\Phi_n(\omega), \end{aligned}$$

la forme quadratique f deviendra, d'une part,

$$F = D_0\mathfrak{F}^2(\omega_0) + D_1\mathfrak{F}^2(\omega_1) + \ldots + D_n\mathfrak{F}^2(\omega_n),$$

et la forme $\mathfrak{f}$, de l'autre,

$$\mathfrak{f} = \mathfrak{F}(\omega_0)\,\mathfrak{F}(\omega_1)\ldots\mathfrak{F}(\omega_n).$$

Or voici le dernier résultat auquel je suis arrivé, et qui me paraît appeler bien des recherches après lui :

Les substitutions en nombre infini, correspondantes à tous les systèmes possibles de valeurs des quantités $D_0, D_1, \ldots, D_n$, *ne conduiront jamais qu'à un nombre essentiellement limité de formes* $\mathfrak{f}$.

De là se tire aussi toute la théorie de la réduction des formes $\mathfrak{f}$. Je me suis principalement fondé sur la proposition suivante :

Étant donnée une forme quadratique f d'ordre $n+1$, *de déterminant* D, *réduite d'après la méthode ci-dessus, soient*

$$(a),\quad (a'),\quad (a''),\quad \ldots,\quad (a^{(n)})$$

les coefficients des carrés dans la forme adjointe g; on aura d'abord

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

puis, pour toutes les valeurs $i = 1, 2, \ldots, n$,

$$(a^{(n)})^i\,(a^{(n-i)}) < \mu \sqrt[n+1]{D^{n(i+1)}},$$

μ étant un facteur numérique dépendant uniquement de n et i.

Je vais prendre les formes *ternaires* pour exemple de la méthode qui donne ce résultat.

Soit

$$ax_0^2 + 2bx_0x_1 + 2cx_0x_2 + \ldots$$

la forme réduite donnée, et

$$(a)y_0^2 + (a')y_1^2 + (a'')y_2^2 + 2(b)y_0y_1 + 2(c)y_0y_2 + 2(c')y_1y_2$$

son adjointe g; la théorie générale donne, en premier lieu, les relations

$$a < \tfrac{4}{3}\sqrt[3]{D}, \qquad b < \tfrac{1}{2}a, \qquad c < \tfrac{1}{2}a;$$

ensuite, pour $y_0 = 0$, g doit devenir une forme binaire réduite. Cette dernière étant représentée par

$$(a')y_1^2 + 2(c')y_1y_2 + (a'')y_2^2,$$

son déterminant, comme on le sait, est aD; on a donc encore

$$(a'') < \sqrt{\tfrac{4}{3}aD}, \qquad (a')(a'') < \tfrac{4}{3}aD, \qquad (c') < \tfrac{1}{2}(a'').$$

Or, des relations

$$\begin{aligned} a(a) + b(b) + c(c) &= D, \\ a(b) + b(a') + c(c') &= 0, \\ a(c) + b(c') + c(a'') &= 0, \end{aligned}$$

on déduit sans difficulté

$$(c) < \tfrac{3}{4}(a''), \qquad (b)(a'') < aD, \qquad (c)(a'') < aD.$$

Donc, après avoir multiplié les deux membres de la première équation par $(a'')^2$ et divisé par a, on obtient

$$(a)(a'')^2 < \tfrac{4}{3}D^2 + aD\sqrt{\tfrac{4}{3}aD},$$

et enfin, en remplaçant a par sa limite supérieure,

$$(a)(a'')^2 < \tfrac{28}{9}D^2.$$

La propriété énoncée ci-dessus des formes réduites, qui m'a longtemps échappé, donne lieu à beaucoup d'autres conséquences que je suis forcé d'omettre. Seulement, j'observerai encore qu'en prenant pour point de départ g au lieu de f, et nommant $a^{(i)}$ les coefficients des carrés dans cette dernière forme, on serait arrivé pour les formes ternaires aux relations

$$a'' < \tfrac{4}{3}\sqrt[3]{\mathrm{D}}, \qquad a'a'' < \left(\tfrac{4}{3}\right)^2 \sqrt[3]{\mathrm{D}^2}, \qquad a a''^2 < \tfrac{28}{9}\,\mathrm{D},$$

et l'on trouverait dans le cas général

$$a^{(n)} < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \sqrt[n+1]{\mathrm{D}}, \qquad a^{(n)i} a^{(n-i)} < \mu \sqrt[n+1]{\mathrm{D}^{i+1}},$$

d'où l'on tire encore

$$a^{(n)n} a^{(n-i)} < \nu\,\mathrm{D}.$$

Appliquons maintenant ces résultats à la forme quadratique

$$\mathrm{F} = \mathrm{D}_0 \mathfrak{F}^2(\omega_0) + \mathrm{D}_1 \mathfrak{F}^2(\omega_1) + \ldots + \mathrm{D}_n \mathfrak{F}^2(\omega_n),$$

dont le déterminant a pour valeur

$$\mathrm{D} = \mathrm{D}_0 \mathrm{D}_1 \ldots \mathrm{D}_n \Delta^2 \Omega.$$

Il est aisé de voir qu'on aura

$$a^{(i)} = \mathrm{D}_0 \Phi_i^2(\omega_0) + \mathrm{D}_1 \Phi_i^2(\omega_1) + \ldots + \mathrm{D}_n \Phi_i^2(\omega_n),$$

donc, en premier lieu,

$$\mathrm{D}_0 \mathrm{D}_1 \ldots \mathrm{D}_n \Phi_n^2(\omega_0) \Phi_n^2(\omega_1) \ldots \Phi_n^2(\omega_n) < a^{(n)n+1},$$

d'où

$$\Phi_n(\omega_0) \Phi_n(\omega_1) \ldots \Phi_n(\omega_n) < \mu \Delta \Omega^{\frac{1}{2}},$$

ce qui reproduit une conséquence obtenue précédemment. Secondement, faisons abstraction, dans $a^{(n)}$, du terme $\mathrm{D}_k \Phi_n^2(\omega_k)$; il est clair qu'on aura

$$\mathrm{D}_0 \mathrm{D}_1 \ldots \mathrm{D}_{k-1} \mathrm{D}_{k+1} \ldots \mathrm{D}_n,$$

$$\Phi_n^2(\omega_0) \Phi_n^2(\omega_1) \ldots \Phi_n^2(\omega_{k-1}) \Phi_n^2(\omega_{k+1}) \ldots \Phi_n(\omega_n) < (a^{(n)})^n;$$

donc combinant cette inégalité avec la suivante

$$\mathrm{D}_k \Phi_i(\omega_k) < a^{(i)},$$

et posant, pour abréger,

$$\Psi_i(\omega_k) = \Phi_i(\omega_k) \Phi_n(\omega_0) \Phi_n(\omega_1) \ldots \Phi_n(\omega_{k-1}) \Phi_n(\omega_{k+1}) \ldots \Phi_n(\omega_n),$$

il viendra

$$\mathrm{D}_0 \mathrm{D}_1 \ldots \mathrm{D}_n \Psi_i^2(\omega_k) < (a^{(n)})^n (a^{(i)}) < \nu\,\mathrm{D},$$

d'où

$$\Psi_i(\omega_k) < \nu \Delta \Omega^{\frac{1}{2}}.$$

Or $\Psi_i(\omega)$ est, comme on le voit aisément, un polynome entier en ω. Les diverses valeurs de ce polynome correspondantes aux diverses racines $\omega_0, \omega_1, \ldots, \omega_n$ étant toutes finies et même proportionnelles à $\Delta\Omega^{\frac{1}{2}}$, il en sera de même de tous ses coefficients qui sont des nombres entiers; de là suit immédiatement le résultat que je voulais obtenir.

On peut mettre en effet $\mathfrak{F}(\omega_k)$ sous la forme

$$\mathfrak{F}(\omega_k) = \Phi_n(\omega_k) \left[\mathrm{X}_n + \mathrm{X}_{n-1} \frac{\Phi_{n-1}(\omega_k)}{\Phi_n(\omega_k)} + \ldots + \mathrm{X}_i \frac{\Phi_i(\omega_k)}{\Phi_n(\omega_k)} + \ldots \right],$$

ou bien

$$\mathfrak{F}(\omega_k) = \Phi_n(\omega_k) \left[\mathrm{X}_n + \mathrm{X}_{n-1} \frac{\Psi_{n-1}(\omega_k)}{\Psi_n(\omega_k)} + \ldots + \mathrm{X}_i \frac{\Psi_i(\omega_k)}{\Psi_n(\omega_k)} + \ldots \right].$$

Donc, toutes les formes $\mathfrak{f}$ en nombre infini, qui correspondent à une même valeur du déterminant Δ, peuvent être ramenées par les substitutions précédentes à un nombre d'entre elles essentiellement limité, car les combinaisons de toutes les valeurs entières possibles pour les coefficients des polynomes $\Psi_i(\omega)$ sont en nombre fini. Enfin, ces dernières formes, qu'on peut nommer *réduites*, se représenteront elles-mêmes une infinité de fois en employant successivement les diverses substitutions qui correspondent à tous les systèmes de valeurs imaginables des quantités positives $\mathrm{D}_0, \mathrm{D}_1, \ldots, \mathrm{D}_n$.

Dans le cas spécial des formes $\mathfrak{f}$ que j'ai d'abord considéré pour démontrer votre théorème sur les nombres premiers $5m+1$, on démontre facilement que les polynomes $\Psi_i(\omega)$ contiennent tous en facteur le nombre N; c'est donc uniquement de Ω que dépendront les limites des coefficients dans les formes réduites. On entrevoit ainsi la possibilité d'obtenir, par exemple, tout ce qui se rattache à la représentation des nombres premiers $11m+1$, par des facteurs complexes formés des racines onzièmes de l'unité, en opérant non plus sur chaque nombre donné, mais en général sur les racines de l'équation $x^{11} = 1$.

Mais j'ai hâte, Monsieur, de finir cette longue lettre, où il n'y a plus place pour la théorie des fonctions elliptiques. Je n'ai pu jusqu'ici faire à mon gré cette recherche de l'ensemble des transformations de la fonction Θ, ni retrouver ce résultat si remarquable de la réduction du module q à la limite $e^{-\pi\sqrt{\frac{3}{4}}}$, dont vous m'avez parlé dans votre lettre. Oserais-je vous demander quelques éclaircissements sur ce point? M. Borchardt a eu la bonté de me mettre un peu sur la voie pour déduire les propriétés des fonctions Θ de la multiplication des quatre séries $\Sigma e^{-(ax+ib)^2}$, mais je ne sais si je pourrai marcher bien loin. Permettez-moi, Monsieur, de vous prier de me rappeler à son souvenir; j'ai entendu M. Sturm parler avec de grands éloges de son Mémoire publié par M. Liouville.

Ayez la bonté, si vous le jugez convenable, de faire paraître dans le *Journal de M. Crelle* quelques-uns des résultats précédents; j'essayerai ensuite de les développer plus complètement.

P.-S. J'aperçois à l'instant que l'algorithme indiqué pour déterminer les nombres entiers α, β, ..., λ, tels qu'on ait

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

peut être présenté d'une manière bien plus précise.

En premier lieu, pour les formes *binaires* de déterminant $-\mathrm{D}$, « on ne peut objecter que les opérations continuent à l'infini, car on verrait s'offrir une infinité de quantités a, a', a'', ... liées par les relations $a > a' > a''$, ... et, par conséquent, différentes. Mais à chacune d'elles correspondent deux nombres entiers $\alpha^{(m)}$, $\beta^{(m)}$ qui donnent, par exemple,

$$a^{(m)} = a\alpha^{(m)2} + 2b\alpha^{(m)}\beta^{(m)} + a'\beta^{(m)2}.$$

Ces nombres sont essentiellement limités, donc il faudrait qu'une même combinaison α, β se produisît dans le cours du calcul une infinité de fois, ce qui conduirait à supposer égaux, contre l'hypothèse, une infinité de termes de la suite a, a', a'', ... »

Pour les formes *ternaires :* « désignant, pour abréger,

$$f[\alpha^{(m)}, \beta^{(m)}, \gamma^{(m)}] \quad \text{par} \quad f^{(m)},$$

on voit naître de la continuation du calcul précédemment proposé une suite de quantités, f, f', f'', ... liées par les relations

$$f' < \sqrt[4]{\left(\tfrac{4}{3}\right)^3 \mathrm{D}f}, \qquad f'' < \sqrt[4]{\left(\tfrac{4}{3}\right)^3 \mathrm{D}f'}, \qquad \ldots.$$

Or, on obtiendra la limite annoncée dès qu'il se présentera une valeur $f^{(m+1)}$ égale ou supérieure à la précédente $f^{(m)}$. En effet, de

$$f^{(m+1)} > f^{(m)} \quad \text{et} \quad f^{(m+1)} < \sqrt[4]{\left(\tfrac{4}{3}\right)^3 \mathrm{D} f^{(m)}}$$

on déduit aisément

$$f^{(m)} < \tfrac{4}{3}\sqrt[3]{\mathrm{D}}.$$

D'ailleurs, on ne peut admettre, dans le cas d'une forme définie, que les opérations se prolongent indéfiniment, car, les nombres $\alpha^{(m)}$, $\beta^{(m)}$, $\gamma^{(m)}$ étant essentiellement limités, on verrait se reproduire une infinité de fois une même combinaison de ces nombres entiers, ce qui ramènerait les mêmes termes dans la suite f, f', f'', contrairement à l'hypothèse. Si la forme f est indéfinie, mais à coefficients entiers (seul cas dont j'aurai besoin plus tard), la même conclusion subsiste, puisqu'une suite de nombres entiers décroissants ne peut aller à l'infini. »

Pour les formes *quaternaires :* « Or ici se représentent les mêmes considérations que dans le cas des formes ternaires; dès que le calcul conduira à un terme $f^{(m+1)}$ égal ou supérieur au précédent, on obtiendra la limite annoncée, car de

$$f^{(m+1)} \geqq f^{(m)} \quad \text{et} \quad f^{(m+1)} < \sqrt[9]{\left(\tfrac{4}{3}\right)^{12} \mathrm{D}^2 f^{(m)}}$$

on déduit

$$f^{(m)} < \left(\frac{4}{3}\right)^{\frac{3}{2}} \sqrt[4]{\mathrm{D}}.$$

D'ailleurs les opérations s'arrêteront toujours, quels que soient les coefficients, si l'on opère sur une forme définie, et la même chose aura lieu pour une forme, même indéfinie, mais à coefficients entiers. »