Deuxième Lettre.

Permettez-moi de venir encore vous soumettre ce qu'il m'est arrivé de rencontrer, sur la théorie des formes quadratiques, depuis que j'ai eu l'honneur de vous écrire. J'avais ébauché bien à la hâte, dans ma lettre, la démonstration de cette propriété générale des formes de même déterminant de se laisser distribuer en un nombre fini de classes; depuis, j'ai été amené à une méthode de réduction plus simple et surtout plus analogue à l'algorithme de Lagrange pour les formes binaires. Soyez assez bon, Monsieur, pour me pardonner s'il m'arrive ainsi de vous entretenir de choses que je n'ai pas encore suffisamment mûries; en présence d'une théorie d'une immense étendue, je cède au plaisir de vous communiquer quelques résultats placés à l'abord de questions difficiles et qui peut-être seront au-dessus de mes forces. Aussi me suis-je borné, comme application de ma nouvelle méthode de réduction, à calculer les formes définies réduites de déterminant 1, à 3, 4, 5, 6 et 7 variables, et j'ai trouvé, comme dans le cas des formes binaires, une seule classe, représentée par une somme de 3, 4, 5, 6 et 7 carrés. L'idée principale de cette méthode consiste dans l'introduction de certaines formes liées intimement, comme je suis parvenu à le reconnaître, aux formes adjointes de M. Gauss, mais qu'il me semble indispensable de considérer d'une manière explicite. En représentant par

$$f(x_0, x_1, x_2, \ldots, x_n) = \sum_0^n{}_j \sum_0^n{}_i a_{i,j} x_i x_j,$$

sous la condition

$$a_{i,j} = a_{j,i},$$

une forme quelconque d'ordre $n+1$ (c'est-à-dire à $n+1$ indéterminées), je les définis de la manière suivante :

$$g(y_1, y_2, y_3, \ldots, y_n) = \sum_1^n{}_j \sum_1^n{}_i b_{i,j} y_i y_j,$$

en prenant

$$b_{i,j} = a_{0,0} a_{i,j} - a_{0,i} a_{0,j},$$

et voici le théorème auquel elles donnent lieu :

Si la substitution

$$(1)\qquad \begin{cases} x_0 = X_0 + M_1 X_1 + M_2 X_2 + \ldots + M_n X_n, \\ x_1 = \quad m_1 X_1 + m_2 X_2 + \ldots + m_n X_n, \\ x_2 = \quad n_1 X_1 + n_2 X_2 + \ldots + n_n X_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n = \quad t_1 X_1 + t_2 X_2 + \ldots + t_n X_n \end{cases}$$

change $f(x_0, x_1, \ldots, x_n)$ *en* $F(X_0, X_1, \ldots, X_n)$, *en nommant* $G(Y_1, Y_2, \ldots, Y_n)$ *la forme d'ordre n déduite de* F, *comme g l'est de f, on aura*

$$g(y_1, y_2, \ldots, y_n) = G(Y_1, Y_2, \ldots, Y_n),$$

en posant

$$(2)\qquad \begin{cases} y_1 = m_1 Y_1 + m_2 Y_2 + \ldots + m_n Y_n, \\ y_2 = n_1 Y_1 + n_2 Y_2 + \ldots + n_n Y_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ y_n = t_1 Y_1 + t_2 Y_2 + \ldots + t_n Y_n. \end{cases}$$

Pour abréger, je nommerai g la *forme dérivée* de f, et (2) la substitution dérivée de (1). On trouve aisément que g est définie et positive, si f est elle-même définie et positive, que le déterminant de g est

$$D_0 = a_{0,0}^{n-1} D,$$

D étant le déterminant de f, et enfin que l'équivalence de f et F entraîne celle de g et G, la seule condition pour cela étant que le déterminant relatif aux équations (2) soit en valeur absolue l'unité.

De là se tire une conséquence importante; concevons que la substitution dérivée soit prise de telle sorte que G devienne une forme réduite de son ordre, les coefficients $M_1, M_2, \ldots, M_n$ resteront encore arbitraires; or, je dis qu'en posant

$$F(X_0, X_1, X_2, \ldots, X_n) = \sum_0^n{}_i \sum_0^n{}_j A_{i,j} X_i X_j,$$

on pourra les déterminer de manière à remplir la condition

$$A_{0,i} < \tfrac{1}{2} A_{0,0}$$

pour $i = 1, 2, \ldots, n$. Cela résulte, en effet, de la valeur suivante :

$$A_{0,i} = M_i a_{0,0} + m_i a_{0,1} + n_i a_{0,2} + \ldots + t_i a_{0,n},$$

qu'il est facile d'obtenir, et on a d'ailleurs $a_{0,0} = A_{0,0}$. Il est essentiel d'observer qu'au lieu de $a_{0,0}$, qui se conserve en passant de f à F, on aurait pu employer, dans ce qui précède, aussi bien l'un quelconque des coefficients $a_{\mu,\mu}$ des carrés des variables. Soit donc, pour plus de clarté, g_μ la forme dérivée composée avec ce coefficient; on pourra énoncer la proposition suivante :

Toute forme

$$f = \Sigma\Sigma a_{i,j} x_i x_j$$

peut être transformée en une autre équivalente

$$f' = \Sigma\Sigma a'_{i,j} x_i x_j,$$

telle qu'ayant, par exemple,

$$a'_{\mu,\mu} = a_{\mu,\mu},$$

la dérivée g'_μ soit une forme réduite de son ordre, et que la condition

$$a'_{\mu,i} < \tfrac{1}{2} a'_{\mu,\mu}$$

soit remplie pour toutes les valeurs de i autres que $i = \mu$.

C'est là-dessus que se fonde l'algorithme de réduction des formes définies, quelle que soit la nature de leurs coefficients, entiers ou irrationnels, mais voici d'abord le but des opérations. Supposons que, précédemment, on ait choisi pour $a_{\mu,\mu}$ le plus petit des coefficients $a_{i,i}$; deux cas peuvent se présenter : ou bien $a'_{\mu,\mu} = a_{\mu,\mu}$ restera encore la plus petite des quantités $a_{i,i}$ dans la transformée f', ou bien il s'offrira un autre coefficient $a'_{\mu',\mu'} < a'_{\mu,\mu}$. Or, dans le premier cas, toutes les autres conditions étant d'ailleurs remplies, f' sera ce que je nomme *une forme réduite*. Mais, si c'est le second qui se présente, on poursuivra les opérations en partant de f', comme tout à l'heure en partant de f, et, en général, on déduira successivement les unes des autres une suite de transformées

$$f,\ f',\ f'',\ \ldots,\ f^{(k)},$$

toutes équivalentes et telles que

$$a_{\mu,\mu},\ a'_{\mu',\mu'},\ a''_{\mu'',\mu''},\ \ldots,\ a^{(k)}_{\mu^{(k)},\mu^{(k)}},$$

désignant respectivement les plus petits des coefficients

$$a_{i,i},\ a'_{i,i},\ a''_{i,i},\ \ldots,\ a^{(k)}_{i,i},$$

on ait

$$a_{\mu,\mu} > a'_{\mu',\mu'} > a''_{\mu'',\mu''} \ldots > a^{(k)}_{\mu^{(k)},\mu^{(k)}},$$

$$a'_{\mu,i} < \tfrac{1}{2} a'_{\mu,\mu},\quad a''_{\mu',i} < \tfrac{1}{2} a''_{\mu',\mu'},\quad \ldots,\quad a^{(k)}_{\mu^{(k-1)},i} < a^{(k)}_{\mu^{(k-1)},\mu^{(k-1)}},$$

et que d'ailleurs les diverses dérivées

$$g_\mu,\ g'_\mu,\ g''_\mu,\ \ldots,\ g^{(k)}_{\mu^{(k)}}$$

soient des formes réduites de leur ordre.

Or je dis qu'un tel système d'opérations ne peut se prolonger à l'infini, et qu'on obtiendra nécessairement une transformée

$$\mathfrak{f} = \Sigma\Sigma \mathfrak{A}_{i,j} x_i x_j$$

devant être considérée comme une forme réduite. En effet, partant d'une forme *définie* f, les quantités $a_{\mu,\mu}$, $a'_{\mu',\mu'}$ seront des valeurs de f, en supposant aux indéterminées des valeurs entières, et l'on ne saurait former qu'un nombre limité de ces valeurs restant toujours inférieures à un certain maximum; donc on ne peut admettre l'hypothèse d'une infinité de quantités de cette sorte, continuellement décroissantes et, par conséquent, inégales.

Je vais maintenant faire voir que tous les coefficients $\mathfrak{A}_{i,j}$, d'une forme définie réduite $\mathfrak{f}$, ne peuvent excéder certaines limites, qui dépendent du déterminant et du nombre des indéterminées. Pour cela, il faut d'abord établir la condition suivante :

$$\mathfrak{A}_{0,0}\,\mathfrak{A}_{1,1}\,\mathfrak{A}_{2,2}\ldots\mathfrak{A}_{n,n} < \left(\frac{4}{3}\right)^{\frac{1}{2}n(n+1)} \mathrm{D},$$

qui est l'extension d'une relation obtenue dans la théorie des formes binaires.

Supposons qu'elle soit admise pour les formes réduites d'ordre n, et désignons par exemple par $\mathfrak{A}_{0,0}$ le plus petit des coefficients $\mathfrak{A}_{i,i}$; la dérivée

$$\mathfrak{G} = \sum_1^n{}_j \sum_1^n{}_i \mathfrak{B}_{i,j} x_i x_j$$

étant une forme réduite de cet ordre, et son déterminant ayant pour valeur

$$\mathrm{D}_0 = \mathfrak{A}_{0,0}^{n-1} \mathrm{D},$$

on devra avoir

$$\mathfrak{B}_{1,1}\mathfrak{B}_{2,2}\mathfrak{B}_{3,3}\dots\mathfrak{B}_{n,n} < \left(\frac{4}{3}\right)^{\frac{1}{2}n(n-1)} \mathfrak{A}_{0,0}^{n-1} \mathrm{D}. \tag{3}$$

Or la valeur générale

$$\mathfrak{B}_{i,j} = \mathfrak{A}_{0,0}\mathfrak{A}_{i,j} - \mathfrak{A}_{0,i}\mathfrak{A}_{0,j} \tag{4}$$

donne, lorsque les deux indices sont égaux,

$$\mathfrak{B}_{i,i} = \mathfrak{A}_{0,0}\mathfrak{A}_{i,i} - \mathfrak{A}_{0,i}^2,$$

de sorte que les quantités positives $\mathfrak{B}_{i,i}$ peuvent être considérées comme les déterminants, changés de signes, d'autant de formes binaires $(\mathfrak{A}_{0,0}, \mathfrak{A}_{0,i}, \mathfrak{A}_{i,i})$ toutes réduites, car on a à la fois

$$\mathfrak{A}_{0,0} < \mathfrak{A}_{i,i} \quad \text{et} \quad \mathfrak{A}_{0,i} < \tfrac{1}{2}\mathfrak{A}_{0,0},$$

donc, on peut poser

$$\mathfrak{A}_{0,0}\mathfrak{A}_{i,i} < \tfrac{4}{3}\mathfrak{B}_{i,i};$$

de là on conclut, l'inégalité subsistant pour toutes les valeurs de i,

$$\mathfrak{A}_{0,0}^n\,\mathfrak{A}_{1,1}\mathfrak{A}_{2,2}\dots\mathfrak{A}_{n,n} < (\tfrac{4}{3})^n\,\mathfrak{B}_{1,1}\mathfrak{B}_{2,2}\dots\mathfrak{B}_{n,n},$$

et enfin d'après la relation (3)

$$\mathfrak{A}_{0,0}\mathfrak{A}_{1,1}\mathfrak{A}_{2,2}\dots\mathfrak{A}_{n,n} < \left(\frac{4}{3}\right)^{\frac{1}{2}n(n+1)} \mathrm{D}.$$

Cette condition est par là démontrée dans toute sa généralité puisqu'elle a lieu pour les formes binaires.

Comme conséquence immédiate, on voit que les quantités $\mathfrak{A}_{i,i}$, $\mathfrak{A}_{0,i}$ sont nécessairement limitées, et il en est de même encore du déterminant D_0 de la dérivée, qui a pour valeur $\mathfrak{A}_{0,0}^{n-1}\mathrm{D}$. Cela posé, admettons que les formes réduites d'ordre n aient tous leurs coefficients limités; je dis que la même chose aura lieu pour les formes d'ordre $n+1$. En effet, toutes les quantités $\mathfrak{B}_{i,j}$ devront se trouver finies; donc, d'après la relation (4), qui donne

$$\mathfrak{A}_{i,j} = \frac{\mathfrak{B}_{i,j} + \mathfrak{A}_{0,i}\mathfrak{A}_{0,j}}{\mathfrak{A}_{0,0}},$$

il en sera de même en général pour $\mathfrak{A}_{i,j}$. Or, la proposition à laquelle je voulais arriver résulte immédiatement de là, puisqu'elle

a lieu pour les formes binaires, et, dans le cas des coefficients *entiers,* elle donne ce théorème [1] :

Les formes définies ou indéfinies, réduites pour un déterminant donné, sont en nombre fini.

Maintenant, voici une remarque essentielle pour l'application des principes précédents au calcul de ces formes.

Soient toujours D le déterminant donné, et

$$\mathfrak{F} = \Sigma\Sigma\mathfrak{A}_{i,j}x_ix_j$$

l'une quelconque des formes définies réduites pour ce déterminant; la relation

$$\mathfrak{A}_{0,0}\mathfrak{A}_{1,1}\mathfrak{A}_{2,2}\dots\mathfrak{A}_{n,n} < \left(\frac{4}{3}\right)^{\frac{1}{2}n(n+1)} \mathrm{D}$$

donne d'abord la limite

$$\mathfrak{A}_{0,0} < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \sqrt[n+1]{\mathrm{D}}$$

pour le plus petit des coefficients $\mathfrak{A}_{i,i}$.

Soit encore

$$\mathfrak{G} = \Sigma\Sigma\mathfrak{B}_{i,j}x_ix_j$$

la dérivée réduite, composée avec $\mathfrak{A}_{0,0}$ et dont le déterminant est

$$\mathrm{D}_0 = \mathfrak{A}_{0,0}^{n-1}\mathrm{D}.$$

En désignant par $\mathfrak{B}_{\mu,\mu}$ le plus petit des coefficients $\mathfrak{B}_{i,i}$, on aura de même

$$\mathfrak{B}_{\mu,\mu} < \left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{\mathrm{D}_0}.$$

Mais, d'après ce que j'ai observé ci-dessus, $\mathfrak{B}_{\mu,\mu}$ peut être considéré comme le déterminant changé de signe de la forme binaire réduite $(\mathfrak{A}_{0,0}, \mathfrak{A}_{0,\mu}, \mathfrak{A}_{\mu,\mu})$, donc on aura :

---

[1] La démonstration suppose essentiellement que $\mathfrak{A}_{0,0}$ ne peut être nul, c'est-à-dire que la forme ne peut représenter zéro. Au reste, M. Hermite avait signalé ce cas d'exception dans une méthode de réduction analogue qui figure dans la Lettre précédente. E. P.

1° Si $\mathfrak{A}_{0,0}$ est pair,

$$\mathfrak{B}_{\mu,\mu} \geq \mathfrak{A}_{0,0}^2 - \left(\tfrac{1}{2}\mathfrak{A}_{0,0}\right)^2 \quad \text{ou} \quad \geq \tfrac{3}{4}\mathfrak{A}_{0,0}^2;$$

2° Si $\mathfrak{A}_{0,0}$ est impair,

$$\mathfrak{B}_{\mu,\mu} \geq \mathfrak{A}_{0,0}^2 - \left[\tfrac{1}{2}(\mathfrak{A}_{0,0}-1)\right]^2.$$

Or, en général, soient $\mathfrak{F}$, $\mathfrak{G}$, $\mathfrak{U}$, $\mathfrak{V}$, ... la suite des formes d'ordre $n+1$, n, $n-1$, $n-2$, ..., qu'on obtient en prenant, pour $\mathfrak{G}$, la dérivée réduite de $\mathfrak{F}$, pour $\mathfrak{U}$, la dérivée réduite de $\mathfrak{G}$, pour $\mathfrak{V}$, la dérivée réduite de $\mathfrak{U}$, ... Nommons respectivement $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, ... les plus petits coefficients des carrés des variables dans ces formes, et D, D_0, D_{01}, D_{02}, ... leurs divers déterminants. On aura d'abord

$$D_0 = \mathfrak{A}^{n-1}D, \qquad D_{01} = \mathfrak{B}^{n-2}D_0, \qquad D_{02} = \mathfrak{C}^{n-3}D_{01}, \qquad \ldots,$$

puis on obtiendra la série des limites supérieures

$$\mathfrak{A} < \left(\frac{4}{3}\right)^{\frac{1}{2}n} \sqrt[n+1]{D}, \qquad \mathfrak{B} < \left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)} \sqrt[n]{D_0}, \qquad \mathfrak{C} < \left(\frac{4}{3}\right)^{\frac{1}{2}(n-2)} \sqrt[n-1]{D_{01}}, \quad \ldots,$$

et, suivant les deux cas, l'une ou l'autre des limites inférieures suivantes :

$$\mathfrak{B} \geq \tfrac{3}{4}\mathfrak{A}^2, \qquad \mathfrak{C} \geq \tfrac{3}{4}\mathfrak{B}^2, \qquad \mathfrak{D} \geq \tfrac{3}{4}\mathfrak{C}^2, \quad \ldots,$$

ou

$$\mathfrak{B} \geq \mathfrak{A}^2 - \left[\tfrac{1}{2}(\mathfrak{A}-1)\right]^2, \qquad \mathfrak{C} \geq \mathfrak{B}^2 - \left[\tfrac{1}{2}(\mathfrak{B}-1)\right]^2, \qquad \mathfrak{D} \geq \mathfrak{C}^2 - \left[\tfrac{1}{2}(\mathfrak{C}-1)\right]^2, \quad \ldots.$$

L'exemple des formes de déterminant 1, que je vais traiter, montrera l'utilité de ces formules. Dans ce cas, on a en général

$$\mathfrak{A} < \left(\frac{4}{3}\right)^{\frac{1}{2}n},$$

ainsi depuis les formes binaires jusqu'aux formes quinaires inclusivement, $\mathfrak{A} < 2$, donc $\mathfrak{A} = 1$, et, depuis les formes à six indéterminées jusqu'à celles qui n'en comprennent pas plus de huit, $\mathfrak{A} < 3$, donc $\mathfrak{A} = 1$ ou $\mathfrak{A} = 2$. Or on va voir que cette seconde valeur doit être rejetée jusqu'à $n = 7$ inclusivement.

Considérons d'abord les formes à *six* indéterminées; on trouve :

1° Pour $\mathfrak{A}$ la limite supérieure

$$\left(\frac{4}{3}\right)^{\frac{5}{2}} = 2{,}05\ldots, \qquad \text{donc } \mathfrak{A} = 2;$$

2° Pour $\mathfrak{B}$ la limite supérieure

$$\left(\frac{4}{3}\right)^{2} \sqrt[5]{2^4} = 3{,}09\ldots, \qquad \text{donc } \mathfrak{B} = 3;$$

3° Pour $\mathfrak{C}$ la limite supérieure

$$\left(\frac{4}{3}\right)^{\frac{3}{2}} \sqrt[4]{2^4 3^3} = 7{,}01\ldots, \qquad \text{donc } \mathfrak{C} = 7.$$

Il est inutile d'aller plus loin, puisque la valeur de $\mathfrak{C}$ est en contradiction avec la limite

$$\mathfrak{C} \geq \mathfrak{B}^2 - \left[\tfrac{1}{2}(\mathfrak{B}-1)\right]^2;$$

il faut donc exclure déjà dans ce cas la valeur $\mathfrak{A} = 2$.

Passons aux formes à *sept* indéterminées; il viendra :

1° Pour $\mathfrak{A}$ la limite supérieure

$$\left(\frac{4}{3}\right)^{3} = 2{,}36\ldots, \qquad \text{donc } \mathfrak{A} = 2;$$

2° Pour $\mathfrak{B}$ la limite supérieure

$$\left(\frac{4}{3}\right)^{\frac{5}{2}} \sqrt[5]{2^5} = 3{,}65\ldots, \qquad \text{donc } \mathfrak{B} = 3;$$

3° Pour $\mathfrak{C}$ la limite supérieure

$$\left(\frac{4}{3}\right)^{2} \sqrt[5]{2^8 3^4} = 7{,}50\ldots, \qquad \text{donc } \mathfrak{C} = 7\,(1);$$

pour la même raison que précédemment, $\mathfrak{A} = 2$ doit encore être rejeté.

Donc, comme dans les cas précédents, il n'existe que la seule valeur $\mathfrak{A} = 1$ (2), et voici maintenant les conséquences qui s'en déduisent :

En premier lieu, pour toutes les formes définies de détermi-

(1) M. Stouff, en reprenant le calcul indiqué, trouve 8,56 au lieu de 7,50 et, par suite, $\mathfrak{C} = 8$, et il n'y a pas de contradiction avec la limite inférieure, qui est aussi égale à 8. Le théorème énoncé par M. Hermite resterait donc douteux pour les formes à *sept* indéterminées; il est cependant exact, comme l'a vérifié M. Stouff en utilisant un résultat de MM. Korkine et Zolotareff. E. P.

(2) M. Hermite arrivait encore au même résultat pour les formes à *huit* in-

nant 1, dont le nombre des indéterminées ne surpasse pas 7, la dérivée réduite a encore l'unité pour déterminant. Soit donc

$$f = \Sigma\Sigma A_{i,j} x_i x_j \quad \text{et} \quad \mathfrak{G} = \Sigma\Sigma B_{i,j} x_i x_j$$

une forme et sa dérivée réduites, toutes deux ayant l'unité pour déterminant. Admettons que, pour les formes $\mathfrak{G}$, dont l'ordre est inférieur d'une unité, on ait

$$B_{i,i} = 1 \quad \text{et} \quad B_{i,j} = 0$$

lorsque i est différent de j; les deux conditions

$$A_{0,0} = 1, \qquad A_{0,i} < \tfrac{1}{2} A_{0,0}$$

donneront d'abord

$$A_{0,i} = 0,$$

et l'équation

$$B_{i,j} = A_{0,0} A_{i,j} - A_{0,i} A_{0,j}$$

conduira successivement, pour $i = j$ et i différent de j, aux deux valeurs

$$A_{i,i} = 1, \qquad A_{i,j} = 0.$$

Or les formes définies binaires réduites offrant la seule classe $x^2 + y^2$ de déterminant 1, on en conclut que, pour les formes ternaires, quaternaires, etc., jusqu'à celle de sept indéterminées, il n'existera pareillement qu'une seule classe représentée successivement par une somme de 3, 4, ..., 7 carrés.

Je n'essayerai pas, Monsieur, de vous développer encore d'autres applications particulières de ma méthode de réduction. Au reste, les formes réduites auxquelles on est ainsi conduit, pour un déterminant donné, n'offrent plus ce caractère, propre aux formes binaires, de ne pouvoir être équivalentes entre elles, à moins d'être identiques, aux signes près de certains coefficients; seulement, on peut démontrer que la limite du nombre des formes réduites équivalentes ne dépend que du nombre des indéterminées, et nullement de la valeur particulière du déterminant. Mais permettez-moi, Monsieur, de revenir un instant sur les circonstances remarquables

déterminées, mais il y avait une lacune dans sa discussion, et le résultat n'est pas exact. Aussi avons-nous supprimé cette partie du texte et, dans les lignes qui suivent, remplacé 8 par 7. E. P.

auxquelles donne lieu la réduction des formes dont les coefficients dépendent de racines d'équations algébriques à coefficients entiers. Peut-être parviendra-t-on à déduire de là un système complet de caractères pour chaque espèce de ce genre de quantités, analogue par exemple à ceux que donne la théorie des fractions continues pour les racines des équations du second degré. On ne peut du moins faire concourir trop d'éléments pour jeter quelque lumière sur cette variété infinie des irrationnelles algébriques, dont les symboles d'extraction de racines ne nous représentent que la plus faible partie. Ici, comme dans la théorie des transcendantes, il a été facile de trouver à une longue suite de notions analytiques de plus en plus complexes une origine commune, une définition unique et complète où n'entrent que les premiers éléments du calcul; mais quelle tâche immense, pour la théorie des nombres et le calcul intégral, de pénétrer dans la nature d'une telle multiplicité d'êtres de raison, en les classant en groupes irréductibles entre eux, de les constituer tous individuellement par des définitions caractéristiques et élémentaires!

L'exemple le plus simple auquel puisse s'appliquer ma méthode de réduction est celui des racines cubiques des nombres entiers. En désignant donc par α la valeur réelle, et par β et γ les deux valeurs imaginaires de $\sqrt[3]{\mathrm{A}}$, on sera conduit, d'après le point de vue auquel je me suis placé, à réduire pour toutes les valeurs de la quantité Δ, croissantes depuis zéro jusqu'à l'infini, la forme ternaire

$$f = (x + \alpha y + \alpha^2 z)^2 + \Delta(x + \beta y + \beta^2 z)(x + \gamma y + \gamma^2 z),$$

dont le déterminant $\mathrm{D} = \frac{27}{4} \Delta^2 \mathrm{A}^2$. Soit, dans l'hypothèse d'une valeur donnée quelconque de Δ, que je représenterai par Δ_0, la substitution correspondante

$$x = m\,\mathrm{X} + n\,\mathrm{Y} + p\,\mathrm{Z},$$
$$y = m'\mathrm{X} + n'\mathrm{Y} + p'\mathrm{Z},$$
$$z = m''\mathrm{X} + n''\mathrm{Y} + p''\mathrm{Z},$$

en posant, pour abréger,

$$\mathrm{M}(\alpha) = m + \alpha m' + \alpha^2 m'', \quad \mathrm{N}(\alpha) = n + \alpha n' + \alpha^2 n'', \quad \mathrm{P}(\alpha) = p + \alpha p' + \alpha^2 p'',$$
$$\mathrm{M}(\beta) = m + \beta m' + \beta^2 m'', \quad \mathrm{N}(\beta) = n + \beta n' + \beta^2 n'', \quad \mathrm{P}(\beta) = p + \beta p' + \beta^2 p'',$$
$$\mathrm{M}(\gamma) = m + \gamma m' + \gamma^2 m'', \quad \mathrm{N}(\gamma) = n + \gamma n' + \gamma^2 n'' \quad \mathrm{P}(\gamma) = p + \gamma p' + \gamma^2 p'',$$

f deviendra

$$F = [XM(\alpha) + YN(\alpha) + ZP(\alpha)]^2 + \Delta[XM(\beta) + YN(\beta) + ZP(\beta)][XM(\gamma) + YN(\gamma) + ZP(\gamma)].$$

Soit encore

$$(1)\qquad \begin{cases} \mathfrak{M} = M^2(\alpha) + \Delta M(\beta) M(\gamma), \\ \mathfrak{N} = N^2(\alpha) + \Delta N(\beta) N(\gamma), \\ \mathfrak{P} = P^2(\alpha) + \Delta P(\beta) P(\gamma); \end{cases}$$

on aura, d'après le caractère principal des formes définies réduites,

$$\mathfrak{M}\mathfrak{N}\mathfrak{P} < (\tfrac{4}{3})^3 D \quad \text{ou} \quad < (\tfrac{4}{3}A\Delta)^2,$$

d'où, en supposant $\mathfrak{M} < \mathfrak{N} < \mathfrak{P}$,

$$(2)\qquad \mathfrak{M} < (\tfrac{4}{3}A\Delta)^{\frac{2}{3}}, \qquad \mathfrak{M}^2\mathfrak{N} < (\tfrac{4}{3}A\Delta)^2, \qquad \mathfrak{M}^2\mathfrak{P} < (\tfrac{4}{3}A\Delta)^2.$$

Or de là résultent plusieurs propriétés essentielles que je vais d'abord établir.

En premier lieu, le nombre entier

$$\Omega = M(\alpha) M(\beta) M(\gamma)$$

vérifie la condition

$$\Omega < \left(\frac{4}{3}\right)^{\frac{3}{2}} A;$$

car, d'après la première des équations (1), le produit des deux facteurs $M(\alpha)$, $\Delta M(\beta) M(\gamma)$ ne peut dépasser son maximum

$$\tfrac{2}{3}\mathfrak{M}\sqrt{(\tfrac{1}{3}\mathfrak{M})},$$

d'où se tire la limite indiquée.

Secondement, les deux polynomes à coefficients entiers, savoir:

$$\Phi(\alpha) = N(\alpha) M(\beta) M(\gamma), \qquad \Psi(\alpha) = P(\alpha) M(\beta) M(\gamma),$$

qui sont respectivement de la forme

$$\Phi(\alpha) = \varphi + \alpha\varphi' + \alpha^2\varphi'', \qquad \Psi(\alpha) = \psi + \alpha\psi' + \alpha^2\psi'',$$

ont de même leurs coefficients limités. En effet, on a, d'après les relations (1),

$$N(\alpha) < \sqrt{\mathfrak{N}}, \qquad \Delta M(\beta) M(\gamma) < \mathfrak{M},$$

donc

$$\Delta\Phi(\alpha) < \mathfrak{M}\sqrt{\mathfrak{N}},$$

et, par la seconde des équations (2),

$$\Phi(\alpha) < \tfrac{4}{3}A,$$

et l'on aura de même

$$\Psi(\alpha) < \tfrac{4}{3}A.$$

Soit ensuite, puisque β et γ sont deux imaginaires conjuguées,

$$\Phi(\beta) = \rho e^{\theta\sqrt{-1}}, \qquad \Phi(\gamma) = \rho e^{-\theta\sqrt{-1}},$$

d'où

$$\rho^2 = \Phi(\beta)\Phi(\gamma) = N(\beta) N(\gamma) M^2(\alpha) M(\beta) M(\gamma).$$

La seconde des équations (1) donne d'abord

$$\Delta N(\beta) N(\gamma) < \mathfrak{N};$$

on tire ensuite de la première

$$M^2(\alpha)\Delta M(\beta) M(\gamma) < \tfrac{1}{4}\mathfrak{M}^2,$$

et l'on en conclut la limite

$$\rho < 2A.$$

Ainsi on peut poser, en désignant par ε et η_i des quantités comprises entre $+1$ et -1,

$$\begin{aligned} \Phi(\alpha) &= \varphi + \alpha\varphi' + \alpha^2\varphi'' = \tfrac{4}{3}A\varepsilon, \\ \Phi(\beta) &= \varphi + \beta\varphi' + \beta^2\varphi'' = 2A\eta_i e^{\theta\sqrt{-1}}, \\ \Phi(\gamma) &= \varphi + \gamma\varphi' + \gamma^2\varphi'' = 2A\eta_i e^{-\theta\sqrt{-1}}, \end{aligned}$$

d'où

$$\begin{aligned} 3\varphi &= 4A(\varepsilon + \eta_i\cos\theta), \\ 3\varphi' &= 4\sqrt[3]{A^2}[\varepsilon + \eta_i\cos(\theta + \tfrac{2}{3}\pi)], \\ 3\varphi'' &= 4\sqrt[3]{A}[\varepsilon + \eta_i\cos(\theta - \tfrac{2}{3}\pi)]; \end{aligned}$$

donc

$$\varphi < \tfrac{8}{3}A, \qquad \varphi' < \tfrac{8}{3}\sqrt[3]{A^2}, \qquad \varphi'' < \tfrac{8}{3}\sqrt[3]{A},$$

et l'on obtiendrait des limites semblables pour les coefficients du polynome Ψ, lesquels donnent lieu d'ailleurs à la condition remarquable

$$\varphi'\psi'' - \varphi''\psi' = \pm\Omega.$$

Cela posé, d'apèrs tout ce qui vient d'être établi, nous représenterons la transformée déduite de la substitution effectuée dans f,

non plus par F, mais par $\frac{F}{M^2(\alpha)} = \mathcal{F}$, forme évidemment réduite en même temps que F et que j'écrirai ainsi

$$\mathcal{F} = \left[X + \frac{N(\alpha)}{M(\alpha)}Y + \frac{P(\alpha)}{M(\alpha)}Z\right]^2 + \Delta\frac{M(\beta)M(\gamma)}{M^2(\alpha)}\left[X + \frac{N(\beta)}{M(\beta)}Y + \frac{P(\beta)}{M(\beta)}Z\right]\left[X + \frac{N(\gamma)}{M(\gamma)}Y + \frac{P(\gamma)}{M(\gamma)}Z\right],$$

ou bien

$$\mathcal{F} = \left[X + \frac{\Phi(\alpha)}{\Omega}Y + \frac{\Psi(\alpha)}{\Omega}Z\right]^2 + \frac{\Delta\Omega}{M^3(\alpha)}\left[X + \frac{\Phi(\beta)}{\Omega}Y + \frac{\Psi(\beta)}{\Omega}Z\right]\left[X + \frac{\Phi(\gamma)}{\Omega}Y + \frac{\Psi(\gamma)}{\Omega}Z\right].$$

Or, Δ croissant d'une manière continue à partir de Δ_0, nommons $\Delta_1, \Delta_2, \Delta_3, \ldots$ la série des valeurs auxquelles viennent successivement correspondre des formes réduites distinctes $\mathcal{F}, \mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \ldots$. Toutes ces formes seront comprises dans le même type que $\mathcal{F}$, mais on peut concevoir que l'une quelconque d'entre elles soit obtenue au moyen de la précédente, en y introduisant la valeur de Δ, à partir de laquelle elle cesse d'être une forme réduite, puis lui appliquant la méthode générale de réduction. En procédant ainsi, le calcul relatif à la série entière des valeurs de Δ, est ramené à un nombre limité d'opérations. En effet, le nombre entier désigné d'une manière générale par Ω, et les coefficients entiers des polynomes Φ et Ψ ayant des limites finies, on arrivera nécessairement à deux valeurs de Δ, Δ_i et $\Delta_{i'}$, auxquelles correspondront deux formes, $\mathcal{F}_i$, $\mathcal{F}_{i'}$, qui représenteront absolument la même combinaison de ces quantités. Faisant donc croître Δ, dans $\mathcal{F}_{i'}$, à partir de la limite $\Delta_{i'}$, on verra se reproduire, dans le même ordre, les divers termes $\mathcal{F}_{i+1}, \mathcal{F}_{i+2}, \ldots$ de la suite obtenue pour le premier intervalle de Δ_i à $\Delta_{i'}$, et, jusqu'à la limite extrême des valeurs de Δ, l'ensemble des formes réduites sera cette série d'un nombre fini de formes, reproduite une infinité de fois.

En la considérant d'ailleurs dans l'ordre inverse, elle offrirait le résultat d'un système d'opérations où l'on aurait fait décroître la quantité Δ d'une manière continue depuis $\Delta_{i'}$ jusqu'à Δ_i; l'ensemble des formes correspondantes aux valeurs indéfiniment décroissantes de Δ sera donc encore la même suite prolongée à l'infini dans un sens opposé.

Si ce n'est pas trop présumer de votre indulgence et si j'avais réussi à vous intéresser un peu à ces recherches, je m'estimerais bien heureux de vous adresser encore ce qu'il pourra m'arriver de rencontrer dans la même voie. Après avoir prouvé que les propriétés précédentes sont caractéristiques pour les racines de toutes les équations du troisième degré à coefficients entiers, je me suis arrêté à quelques recherches sur l'équation $M(\alpha)M(\beta)M(\gamma) = 1$ dont je pense obtenir la solution complète. Mais je désirerais surtout pouvoir vous soumettre un Travail sur les équations modulaires, dans lequel j'ai établi une proposition énoncée dans les *Œuvres posthumes de Galois,* imprimées dans le *Journal de Mathématiques,* et qui consiste en ce que les équations modulaires du sixième, huitième et douzième degré peuvent être abaissées respectivement au cinquième, septième et onzième degré. Je me suis proposé en même temps de retrouver ces relations si singulières que vous avez le premier découvertes entre les racines M, M′, M″, ... de l'équation $F(k, M) = 0$, mais je n'ai pu y réussir malgré tous mes efforts. Ces premières propriétés d'irrationnelles algébriques, non exprimables par radicaux, me paraissent du plus grand intérêt; comme les propriétés des racines des équations relatives à la division du cercle, elles serviront de point de départ pour pénétrer plus avant dans la théorie générale des équations. Ne publierez-vous donc pas un jour, Monsieur, les principes si cachés qui vous ont conduit à ces beaux théorèmes? Il me semble que ce serait encore une voie nouvelle que vous ouvririez aux recherches des géomètres, dans une des théories les plus vastes et les plus difficiles.

Troisième Lettre.

Je dois à l'obligeance de M. Borchardt d'avoir reçu votre dernière Lettre qui m'a été bien précieuse, en portant à ma connaissance l'écrit de M. Gauss sur les formes quadratiques ternaires. Permettez-moi de vous remercier aussi de toutes les autres indications que vous avez eu la bonté de me donner, mais dont mon ignorance de la langue allemande m'empêche malheureusement de profiter comme je le souhaiterais. C'est M. Borchardt lui-même qui a bien voulu me traduire l'article de M. Gauss, mais jusqu'ici je n'ai pu trouver personne pour me continuer le même service, et, à mon grand regret, je reste complètement étranger aux travaux de M. Kummer sur les nombres complexes, qui m'intéresseraient vivement.

Comme vous le savez, Monsieur, le but de mes premières recherches avait été d'examiner le nouveau mode d'approximation que vous avez donné en établissant l'impossibilité d'une fonction à trois périodes imaginaires. Ce n'est que longtemps après que j'ai vu comment cette question, et une infinité d'autres du même genre, dépendaient de la réduction des formes quadratiques. Mais, une fois arrivé à ce point de vue, les problèmes si vastes que j'avais cru me proposer m'ont semblé peu de chose à côté des grandes questions de la théorie des formes, considérée d'une manière générale. Dans cette immense étendue de recherches qui nous a été ouverte par M. Gauss, l'Algèbre et la Théorie des nombres me paraissent devoir se confondre dans un même ordre de notions analytiques, dont nos connaissances actuelles ne nous permettent pas encore de nous faire une juste idée. Peut-être, cependant, doit-on entrevoir qu'il appartiendra à cette partie de la science, constituée ainsi sur ses véritables bases, d'offrir le tableau de tous les éléments, en nombre fini ou illimité, dont dépendent les racines des équations algébriques, séparées en types irréductibles et classés suivant leurs rapports naturels.

Je ne sais si j'aurai réussi à faire un premier pas vers un but si éloigné, en donnant une méthode pour la réduction des formes bi-

naires de degré quelconque (1). J'essayerai plus tard de poursuivre, sous ce point de vue, les conséquences des résultats que j'ai obtenus, mais, jusqu'à présent, j'ai été plutôt préoccupé de la recherche des principes propres à la réduction des formes les plus générales composées d'un nombre quelconque de variables, question capitale et qui peut-être sera bien au-dessus de mes forces. Voici néanmoins sur ce sujet un premier théorème destiné à présenter, dans le sens le plus étendu, la notion des formes adjointes de M. Gauss.

Soit

$$\text{(1)} \qquad X = f(x_1, x_2, \ldots, x_n)$$

l'expression générale d'une fonction homogène du $m^{ième}$ degré à n variables. Faisons

$$\text{(2)} \qquad \frac{dX}{dx_1} = y_1, \qquad \frac{dX}{dx_2} = y_2, \qquad \ldots, \qquad \frac{dX}{dx_n} = y_n;$$

par l'élimination de $x_1, x_2, \ldots, x_n$ on arrivera à une équation

$$\text{(3)} \qquad \pi(X, y_1, y_2, \ldots, y_n) = 0.$$

Cela étant, les coefficients des diverses puissances de X seront ce que j'appellerai les *formes des divers degrés adjointes à $f(x_1, x_2, \ldots, x_n)$*, et je les désignerai généralement, en supposant égal à l'unité le coefficient de la puissance la plus élevée de X, par

$$g(y_1, y_2, \ldots, y_n).$$

Or on aura le théorème suivant, comme conséquence immédiate de la définition qu'on vient de proposer :

La fonction homogène

$$f(x_1, x_2, \ldots, x_n)$$

devenant

$$F(X_1, X_2, \ldots, X_n),$$

par la substitution

$$\begin{aligned} x_1 &= a_1 X_1 + a_2 X_2 + \ldots + a_n X_n, \\ x_2 &= b_1 X_1 + b_2 X_2 + \ldots + b_n X_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n &= l_1 X_1 + l_2 X_2 + \ldots + l_n X_n, \end{aligned}$$

(1) *Journal de Crelle*, t. 36, p. 357, et p. 84 de ce Volume.

si l'on désigne par G *la forme adjointe, composée avec les coefficients de* F, *comme g est composée avec les coefficients de f, on aura*

$$g(y_1, y_2, \ldots, y_n) = \mathrm{G}(\mathrm{Y}_1, \mathrm{Y}_2, \ldots, \mathrm{Y}_n),$$

en prenant

$$\begin{aligned}
\mathrm{Y}_1 &= a_1 y_1 + b_1 y_2 + \ldots + l_1 y_n,\\
\mathrm{Y}_2 &= a_2 y_1 + b_2 y_2 + \ldots + l_2 y_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\mathrm{Y}_n &= a_n y_1 + b_n y_2 + \ldots + l_n y_n.
\end{aligned}$$

Mais il importait surtout d'obtenir le résultat général de l'élimination des variables $x_1, x_2, \ldots, x_n$, entre les équations (1) et (2). Voici comment on peut y parvenir :

Soit

$$\varphi = \mathrm{X}^{m-1} f(x_1, x_2, \ldots, x_n) - \frac{(x_1 y_1 + x_2 y_2 + \ldots + x_n y_n)^m}{m^m}$$

une nouvelle fonction homogène du $m^{\text{ième}}$ degré de $x_1, x_2, \ldots, x_n$; j'observe que, au moyen des équations proposées, les suivantes ont lieu, savoir :

$$\varphi = 0$$

et

$$\frac{d\varphi}{dx_1} = 0, \qquad \frac{d\varphi}{dx_2} = 0, \qquad \ldots, \qquad \frac{d\varphi}{dx_n} = 0.$$

Elles se réduisent en effet à des identités, en mettant à la place de X, d'une part, et de $y_1, y_2, \ldots, y_n$, de l'autre, leurs valeurs en $x_1, x_2, \ldots, x_n$, telles que les donnent les équations (1) et (2). Donc la question est ramenée à l'élimination de $x_1, x_2, \ldots, x_n$ entre les équations homogènes

$$\frac{d\varphi}{dx_1} = 0, \qquad \frac{d\varphi}{dx_2} = 0, \qquad \ldots, \qquad \frac{d\varphi}{dx_n} = 0,$$

car l'équation $\varphi = 0$ rentre dans celles-là, et on peut l'omettre.

Ainsi, représentant la forme f par la somme des valeurs du produit

$$x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \mathrm{A}_{i_1, i_2, \ldots, i_n},$$

lorsqu'on attribue aux quantités i tous les systèmes de valeurs entières et positives qui vérifient la condition

$$i_1 + i_2 + \ldots + i_n = m,$$

et désignant par

$$\mathfrak{f} = 0$$

la relation entre les coefficients A qui résulte de l'élimination de $x_1, x_2, \ldots, x_n$ entre les équations

$$\frac{df}{dx_1} = 0, \qquad \frac{df}{dx_2} = 0, \qquad \ldots, \qquad \frac{df}{dx_n} = 0,$$

on aura le théorème suivant :

L'équation

$$\Pi(\mathrm{X}, y_1, y_2, \ldots, y_n) = 0$$

s'obtiendra en remplaçant $\mathrm{A}_{i_1, i_2, \ldots, i_n}$, *dans*

$$\mathfrak{f} = 0,$$

par

$$\mathrm{X}^{m-1} \mathrm{A}_{i_1, i_2, \ldots, i_n} - (i_1, i_2, \ldots, i_n) \frac{y_1^{i_1} y_2^{i_2} \ldots y_n^{i_n}}{m^m},$$

$(i_1, i_2, \ldots, i_n)$ *étant le coefficient numérique de* $y_1^{i_1} y_2^{i_2} \ldots y_n^{i_n}$ *dans le développement de la puissance polynomiale*

$$(y_1 + y_2 + \ldots + y_n)^m.$$

On observera seulement qu'il y aura lieu de supprimer comme facteur étranger une certaine puissance de X, ce qui n'altère en rien la forme analytique du résultat que je viens d'obtenir.

L'application aux formes quadratiques est bien simple. La forme proposée étant

$$f = \sum_1^n{}_i \sum_1^n{}_j a_{i,j} x_i x_j,$$

sous la condition ordinaire

$$a_{i,j} = a_{j,i},$$

la forme adjointe g sera

$$g = \sum_1^n{}_i \sum_1^n{}_j \frac{d\mathrm{D}}{da_{i,j}} y_i y_j,$$

D étant le déterminant de la forme f.

Je prendrai encore comme exemple les formes cubiques binaires

$$f = ax^3 + 3bx^2 y + 3cxy^2 + ey^3.$$

Dans ce cas, l'expression désignée par $\mathfrak{F}$ coïncide avec le déterminant unique de la forme, tel que je l'ai obtenu dans la théorie de la réduction, et le coefficient du second terme de l'équation en X donne la forme adjointe

$$\frac{1}{\mathfrak{F}}\left(\frac{d\mathfrak{F}}{da}x^3+\frac{d\mathfrak{F}}{db}x^2y+\frac{d\mathfrak{F}}{dc}xy^2+\frac{d\mathfrak{F}}{de}y^3\right)$$
$$=\frac{1}{\mathfrak{F}}[(ae^2-3bce+2c^3)x^3-3(ace-2b^2e+bc^2)x^2y$$
$$+3(2ac^2-abe-b^2c)xy^2-(3abc-a^2e-2b^3)y^3].$$

En étudiant cette forme que je trouve dans un des Mémoires de M. Eisenstein, j'ai reconnu qu'elle se déduisait de f, en y remplaçant les variables par les deux expressions linéaires

$$\frac{d\Phi}{dx},\qquad \frac{d\Phi}{dy},$$

Φ étant l'expression quadratique

$$(ac-b^2)y^2-(ae-bc)xy+(be-c^2)x^2,$$

considérée encore par M. Eisenstein, et par moi-même dans la Note du *Journal de Crelle*, sous la forme

$$(\alpha-\beta)^2(y-\gamma x)^2+(\beta-\gamma)^2(y-\alpha x)^2+(\gamma-\alpha)^2(y-\beta x)^2,$$

α, β, γ étant les racines de l'équation

$$ax^3+3bx^2+3cx+e=0.$$

Maintenant, Monsieur, je reviens à la théorie des formes quadratiques, pour essayer de vous compléter quelques points de la dernière Lettre que j'ai eu l'honneur de vous écrire. Et d'abord, j'ai dû reconnaître que ce qu'on devait se proposer avant tout, dans la théorie de la réduction, était de découvrir les valeurs entières des indéterminées pour lesquelles une forme définie donnée était *la plus petite possible*. De là, en effet, se tireraient les conséquences suivantes :

1° En cherchant la série des *minima* de la forme binaire

$$(y-ax)^2+\frac{x^2}{\Delta},$$

pour toutes les valeurs positives de la quantité Δ croissant d'une manière continue de zéro à l'infini, *les diverses fractions* $\frac{y}{x}$ *représenteraient l'ensemble des réduites de la fraction continue équivalente à a.*

2° En cherchant de même la série des *minima* de la forme ternaire

$$A(z-ax)^2+B(y-bx)^2+\frac{x^2}{\Delta},$$

où A et B sont deux quantités positives quelconques, a et b deux quantités réelles, *toutes les fractions* $\frac{z}{x}$, $\frac{y}{x}$ *auraient ce caractère essentiel qu'en choisissant un dénominateur* x_0 *moindre que* x; *deux autres fractions,* $\frac{z_0}{x_0}$, $\frac{y_0}{x_0}$, *donneraient nécessairement*

$$A(z_0-ax_0)^2+B(y_0-bx_0)^2>A(z-ax)^2+B(y-bx)^2.$$

Car, si cette inégalité n'avait pas lieu, l'expression

$$A(z_0-ax_0)^2+B(y_0-bx_0)^2+\frac{x_0^2}{\Delta}$$

serait moindre que

$$A(z-ax)^2+B(y-bx)^2+\frac{x^2}{\Delta};$$

donc cette dernière ne serait pas, comme on l'a supposé, un *minimum*.

Cela étant, si l'on observe qu'on peut toujours faire

$$A(z-ax)^2+B(y-bx)^2+\frac{x^2}{\Delta}<\sqrt[3]{\frac{2AB}{\Delta}},$$

et *a fortiori*

$$A(z-ax)^2+B(y-bx)^2<\sqrt[3]{\frac{2AB}{\Delta}},$$

on voit que, en faisant croître continuellement Δ, la série des fractions $\frac{z}{x}$, $\frac{y}{x}$ converge indéfiniment vers les limites a et b, et que, pour chaque approximation, la somme des carrés des erreurs $z-ax$, $y-bx$, multipliés par les constantes A et B, est un *minimum*, c'est-à-dire que cette somme augmente, si le dénominateur commun x diminue.

Ce qui précède indique suffisamment une infinité d'autres conséquences analogues, qui toutes viennent dépendre de la recherche difficile d'une limite précise du *minimum* d'une forme définie quelconque. Là-dessus je ne puis former qu'une conjecture. Mes premières recherches, dans le cas d'une forme à n variables de déterminant D, m'avaient donné la limite

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

je suis porté à présumer, mais sans pouvoir le démontrer, que le coefficient numérique $\left(\frac{4}{3}\right)^{\frac{1}{2}(n-1)}$ doit être remplacé par $\frac{2}{\sqrt[n]{(n+1)}}$.

Comme application des mêmes principes, je considérerai encore la question suivante :

Étant donnée une expression imaginaire $a+b\sqrt{-1}$: *déterminer les entiers complexes*

$$x+y\sqrt{-1}, \qquad t+u\sqrt{-1},$$

pour lesquels la norme de

$$(x+y\sqrt{-1})(a+b\sqrt{-1})-(t+u\sqrt{-1})$$

soit la plus petite possible, sous la condition que x^2+y^2 *soit au-dessous d'une certaine limite.*

On cherchera les minima successifs de la forme à *quatre* variables

$$f=(ax-by-t)^2+(ay+bx-u)^2+\frac{x^2+y^2}{\Delta},$$

pour toutes les valeurs de Δ; les diverses fractions complexes

$$\frac{t+u\sqrt{-1}}{x+y\sqrt{-1}},$$

auxquelles on parviendra ainsi, jouiront de cette propriété caractéristique *que le module de la différence*

$$a+b\sqrt{-1}-\frac{t+u\sqrt{-1}}{x+y\sqrt{-1}}$$

croîtra nécessairement en prenant toute autre fraction dont le dénominateur aurait un module moindre.

Mais une autre propriété de ces fractions les rapprochera encore davantage des réduites de la théorie des fractions continues. Soient

$$\frac{t+u\sqrt{-1}}{x+y\sqrt{-1}}, \qquad \frac{t_0+u_0\sqrt{-1}}{x_0+y_0\sqrt{-1}},$$

deux fractions différentes qui correspondent à deux *minima* consécutifs de la forme f, de sorte que les deux valeurs de Δ qui ont donné lieu à ces deux fractions soient *infiniment peu* différentes l'une de l'autre. Alors, en observant que le déterminant de f est en général $\frac{1}{\Delta^2}$, le premier minimum donnera, en admettant la conjecture ci-dessus,

$$(ax-by-t)^2+(ay+bx-u)^2+\frac{x^2+y^2}{\Delta}<\frac{2}{\sqrt[4]{5}}\frac{1}{\sqrt{\Delta}},$$

et le second

$$(ax_0-by_0-t_0)^2+(ay_0+bx_0-u_0)^2+\frac{x_0^2+y_0^2}{\Delta+\omega}<\frac{2}{\sqrt[4]{5}}\frac{1}{\sqrt{\Delta+\omega}},$$

ω désignant une quantité aussi petite qu'on voudra. Cela posé, multiplions ces deux inégalités, membre à membre; on trouvera, en employant une formule bien connue (1),

$$\begin{aligned}
&\left\{(ax-by-t)(ax_0-by_0-t_0)+(ay+bx-u)(ay_0+bx_0-u_0)+\frac{xx_0+yy_0}{\sqrt{\Delta(\Delta+\omega)}}\right\}^2\\
&+\left\{-(ax-by-t)(ay_0+bx_0-u_0)+(ax_0-by_0-t_0)(ay+bx-u)+\frac{yx_0-y_0x}{\sqrt{\Delta(\Delta+\omega)}}\right\}^2\\
&+\left\{\frac{(\sqrt{\Delta+\omega}-\sqrt{\Delta})[a(yy_0-xx_0)+b(x_0y+xy_0)+t_0x-u_0y]+\sqrt{\Delta}(uy_0-u_0y+t_0x-x_0t)}{\sqrt{\Delta(\Delta+\omega)}}\right\}^2\\
&+\left\{\frac{(\sqrt{\Delta+\omega}-\sqrt{\Delta})[a(yx_0+xy_0)+b(xx_0-yy_0)-t_0y-u_0x]+\sqrt{\Delta}(ty_0-t_0y+ux_0-u_0x)}{\sqrt{\Delta(\Delta+\omega)}}\right\}^2\\
&<\frac{4}{\sqrt{5}}\frac{1}{\sqrt{\Delta(\Delta+\omega)}};
\end{aligned}$$

d'où, en négligeant les deux premiers carrés et introduisant la

(1) La formule d'Euler, qui donne sous la forme d'une somme de quatre carrés le produit de deux sommes de quatre carrés, suit immédiatement de ce que le

condition que ω est infiniment petit,

$$(uy_0 - u_0y + t_0x - x_0t)^2 + (ty_0 - t_0y + ux_0 - u_0x)^2 < \frac{4}{\sqrt{5}},$$

et, par conséquent,

$$(uy_0 - u_0y + t_0x - x_0t)^2 + (ty_0 - t_0y + ux_0 - u_0x)^2 = 1.$$

Ainsi, la norme du numérateur de la différence de deux fractions complexes consécutives est l'*unité;* on eût obtenu l'*unité* ou le nombre *deux*, en employant dans l'expression du minimum de f le facteur $\left(\frac{4}{3}\right)^{\frac{3}{2}}$ au lieu du coefficient hypothétique $\frac{2}{\sqrt[4]{5}}$ (1).

La méthode précédente s'applique encore aux nombres complexes $x + y\sqrt{-n}$, dont la théorie est plus difficile et sur laquelle

---

produit des deux déterminants $(ad - bc)$, $(a'd' - b'c')$ est le déterminant du système

$$\begin{bmatrix} aa' + bc', & ab' + bd' \\ ca' + dc', & cb' + dd' \end{bmatrix}.$$

En effet, il suffit de supposer

$$a = p + q\sqrt{-1}, \quad b = r + s\sqrt{-1}, \quad c = -r + s\sqrt{-1}, \quad d = p - q\sqrt{-1},$$
$$a' = p' + q'\sqrt{-1}, \quad b' = r' + s'\sqrt{-1}, \quad c' = -r' + s'\sqrt{-1}, \quad d' = p' - q'\sqrt{-1}$$

pour obtenir

$$(p^2 + q^2 + r^2 + s^2)(p'^2 + q'^2 + r'^2 + s'^2)$$
$$= (pp' - qq' - rr' - ss')^2 + (pq' + qp' + rs' - sr')^2$$
$$+ (pr' - qs' + rp' + sq')^2 + (ps' + qr' + p's - q'r)^2.$$

Celle de Lagrange vient en mettant $q\sqrt{\mathrm{A}}$, $r\sqrt{\mathrm{B}}$, $s\sqrt{\mathrm{AB}}$, ... au lieu de $q, r, s, \ldots$.

(1) M. Hermite a repris cette question dans un Mémoire ultérieur en se servant des formes quadratiques binaires à indéterminées conjuguées, et démontré rigoureusement que la norme est bien égale à *un*.

On doit remarquer que la limite hypothétique $\frac{2}{\sqrt[n]{n+1}}\sqrt[n]{\mathrm{D}}$ admise par M. Hermite est trop faible. Pour $n = 4$, elle ne donne déjà plus la limite supérieure du minimum. En effet, cette limite est alors, d'après MM. Korkine et Zolotareff, $\sqrt{2}\sqrt[4]{\mathrm{D}}$, et c'est là une limite précise que l'on ne peut abaisser. Comme $\sqrt{2}$ surpasse $\frac{2}{\sqrt[4]{5}}$, la limite hypothétique est trop faible. Si l'on reprend le calcul ci-dessus, en remplaçant $\frac{2}{\sqrt[4]{5}}$ par $\sqrt{2}$, on retrouve d'ailleurs le résultat de M. Hermite, qui se trouve alors aussi complètement établi par cette voie. E. P.

je me propose de revenir. Mais ce n'est qu'au moyen de la réduction de formes de degrés plus élevés qu'on pourra résoudre les questions analogues à la précédente, dans lesquelles entreraient les nombres complexes *réels* $x + y\sqrt{n}$ et ceux qui dépendent d'irrationnelles numériques plus compliquées que les radicaux carrés.

Voici maintenant une autre série de questions importantes dont la solution dépend encore de la recherche du minimum d'une forme quadratique et qu'on peut comprendre dans cet énoncé général :

Trouver, en nombres entiers, le minimum du produit d'un certain nombre de fonctions linéaires et homogènes, à coefficients réels ou imaginaires.

Nommons

$$f_1, \quad f_2, \quad \ldots, \quad f_n$$

les fonctions linéaires à coefficients réels,

$$g_1, \quad g_2, \quad \ldots, \quad g_{n'}; \qquad h_1, \quad h_2, \quad \ldots, \quad h_{n'}$$

les fonctions à coefficients imaginaires, g_i et h_i étant des fonctions conjuguées. Si l'on suppose que leur produit prenne la plus petite valeur possible en attribuant aux indéterminées les valeurs entières $x = x_0$, $y = y_0$, ..., et qu'on désigne alors par

$$f_1^0, \quad f_2^0, \quad \ldots, \quad f_n^0$$

ce que deviennent les facteurs linéaires réels, et de même par

$$g_1^0, \quad h_1^0; \quad g_2^0, \quad h_2^0; \quad \ldots, \quad g_{n'}^0, \quad h_{n'}^0,$$

les diverses couples de facteurs conjugués, *je dis que la forme quadratique*

$$\left(\frac{f_1}{f_1^0}\right)^2 + \left(\frac{f_2}{f_2^0}\right)^2 + \ldots + \left(\frac{f_n}{f_n^0}\right)^2 + 2\frac{g_1h_1}{g_1^0h_1^0} + 2\frac{g_2h_2}{g_2^0h_2^0} + \ldots + 2\frac{g_{n'}h_{n'}}{g_{n'}^0h_{n'}^0}$$

sera elle-même la plus petite possible pour $x = x_0, y = y_0, \ldots$.

Supposons, en effet, qu'on puisse avoir

$$\left(\frac{f_1}{f_1^0}\right)^2 + \left(\frac{f_2}{f_2^0}\right)^2 + \ldots + \left(\frac{f_n}{f_n^0}\right)^2 + 2\frac{g_1h_1}{g_1^0h_1^0} + 2\frac{g_2h_2}{g_2^0h_2^0} + \ldots + 2\frac{g_{n'}h_{n'}}{g_{n'}^0h_{n'}^0} = \mathrm{M},$$

M étant moindre que $n+2n'$; comme le produit des facteurs

$$(a)\qquad \left(\frac{f_1}{f_1^0}\right)^2\left(\frac{f_2}{f_2^0}\right)^2\cdots\left(\frac{f_n}{f_n^0}\right)^2\left(\frac{g_1h_1}{g_1^0h_1^0}\right)^2\left(\frac{g_2h_2}{g_2^0h_2^0}\right)^2\cdots\left(\frac{g_{n'}h_{n'}}{g_{n'}^0h_{n'}^0}\right)^2$$

sera toujours inférieur à son *maximum*

$$\left(\frac{\mathrm{M}}{n+2n'}\right)^{n+2n'},$$

la supposition de $\mathrm{M}<n+2n'$ conduirait à

$$f_1f_2\ldots f_n.g_1h_1.g_2h_2\ldots g_{n'}h_{n'}<f_1^0f_2^0\ldots f_n^0.g_1^0h_1^0.g_2^0h_2^0\ldots g_{n'}^0h_{n'}^0,$$

et, par suite, le produit des facteurs linéaires ne serait pas, contre l'hypothèse, le plus petit possible pour $x=x_0$, $y=y_0$, ... J'ajoute qu'en faisant $\mathrm{M}=n+2n'$ le produit (a) ne pourra atteindre son maximum ou l'unité qu'autant qu'on aura

$$\left(\frac{f_1}{f_1^0}\right)^2=1,\qquad \left(\frac{f_2}{f_2^0}\right)^2=1,\qquad \ldots,\qquad \left(\frac{f_n}{f_n^0}\right)^2=1,$$
$$\frac{g_1h_1}{g_1^0h_1^0}=1,\qquad \frac{g_2h_2}{g_2^0h_2^0}=1,\qquad \ldots,\qquad \frac{g_{n'}h_{n'}}{g_{n'}^0h_{n'}^0}=1.$$

Nous voici donc encore conduit, comme vous le voyez, Monsieur, à cette recherche singulière *de tous les minima, d'une forme quadratique, correspondant aux divers systèmes de valeurs de plusieurs paramètres qu'il faudra supposer passer par tous les états possibles de grandeur*. Telle est du moins la voie qui nous est ouverte, par l'analyse précédente, pour la solution de nombreuses questions, parmi lesquelles je choisirai celle-ci:

$\varphi(\alpha)$ désignant un nombre entier complexe, composé avec une racine α de l'équation $\mathrm{F}(x)=0$ à coefficients entiers, celui du premier terme étant l'unité, trouver toutes les solutions de l'équation

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

Soit M un *minimum* d'une quelconque des formes définies

$$\Phi=\left[\frac{\varphi(\alpha_1)}{\mathrm{A}_1}\right]^2+\left[\frac{\varphi(\alpha_2)}{\mathrm{A}_2}\right]^2+\ldots+\left[\frac{\varphi(\alpha_n)}{\mathrm{A}_n}\right]^2$$
$$+2\,\frac{\varphi(\beta_1)\varphi(\gamma_1)}{\mathrm{K}_1^2}+2\,\frac{\varphi(\beta_2)\varphi(\gamma_2)}{\mathrm{K}_2^2}+\ldots+2\,\frac{\varphi(\beta_{n'})\varphi(\gamma_{n'})}{\mathrm{K}_{n'}^2},$$

dans lesquelles $\alpha_1, \alpha_2, \ldots, \alpha_n$ désignent les racines réelles, et β_1, γ_1; β_2, γ_2; $\ldots$; $\beta_{n'}, \gamma_{n'}$ les couples des racines imaginaires de l'équation $\mathrm{F}(x)=0$. En faisant, pour abréger, $n+2n'=m$, on déduira de la limite

$$\mathrm{M}<\left(\frac{4}{3}\right)^{\frac{1}{2}m(m-1)}\sqrt[m]{\mathrm{D}},$$

où D est le déterminant de Φ, la relation suivante :

$$\text{Norme } \varphi^2(\alpha)<\left(\frac{4}{3}\right)^{\frac{1}{2}m(m-1)}\frac{\Delta}{m^m},$$

dans laquelle Δ représente la valeur absolue de l'expression

$$\mathrm{F}'(\alpha_1)\,\mathrm{F}'(\alpha_2)\ldots\mathrm{F}'(\beta_{n'})\,\mathrm{F}'(\gamma_{n'}),$$

et où n'entrent plus les valeurs de $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{K}_1, \mathrm{K}_2, \ldots$.

Donc, quelles que soient les quantités $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{K}_{n'}$, le minimum de Φ conduit à une valeur toujours limitée pour la norme de $\varphi(\alpha)$; mais ce qui a été établi précédemment fait voir, de plus, qu'en faisant passer $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{K}_1, \mathrm{K}_2, \ldots$ par tous les états possibles de grandeur, on obtiendra nécessairement toutes les *unités complexes*, toutes les solutions de l'équation

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

Considérons une solution particulière telle que $\mathrm{N}\varphi_0(\alpha)=1$, elle sera donnée, par le minimum de φ, dans l'hypothèse suivante :

$$\Phi=\left[\frac{\varphi(\alpha_1)}{\varphi_0(\alpha_1)}\right]^2+\left[\frac{\varphi(\alpha_2)}{\varphi_0(\alpha_2)}\right]^2+\ldots+\left[\frac{\varphi(\alpha_n)}{\varphi_0(\alpha_n)}\right]^2$$
$$+2\,\frac{\varphi(\beta_1)\varphi(\gamma_1)}{\varphi_0(\beta_1)\varphi_0(\gamma_1)}+\ldots+2\,\frac{\varphi(\beta_{n'})\varphi(\gamma_{n'})}{\varphi_0(\beta_{n'})\varphi_0(\gamma_{n'})}$$

Mais ne pourrait-il pas exister deux ou plusieurs autres représentations distinctes du même *minimum* et conduisant, par suite, à de nouvelles solutions?

Observons, à cet effet, qu'on a les conditions

$$\left[\frac{\varphi(\alpha_1)}{\varphi_0(\alpha_1)}\right]^2=1,\qquad \left[\frac{\varphi(\alpha_2)}{\varphi_0(\alpha_2)}\right]^2=1,\qquad \ldots,\qquad \left[\frac{\varphi(\alpha_n)}{\varphi_0(\alpha_n)}\right]^2=1,$$
$$\frac{\varphi(\beta_1)\varphi(\gamma_1)}{\varphi_0(\beta_1)\varphi_0(\gamma_1)}=1,\qquad \ldots,\qquad \frac{\varphi(\beta_{n'})\varphi(\gamma_{n'})}{\varphi_0(\beta_{n'})\varphi_0(\gamma_{n'})}=1,$$

déjà établies précédemment, de sorte qu'en supposant l'équation

$F(x)=0$ irréductible, si l'on prend $\varphi(\alpha_1)=\varphi_0(\alpha_1)$, la même équation aura lieu pour toute autre racine réelle ou imaginaire, et il en serait de même en partant de la condition $\varphi(\alpha_1)=-\varphi_0(\alpha_1)$. Or, le premier cas conduit nécessairement à $x=x_0, y=y_0, \ldots$, et le second à $x=-x_0, y=-y_0, \ldots$.

Mais, si toutes les racines étaient imaginaires, la démonstration serait en défaut; dans ce cas, on est conduit à détacher de l'ensemble général des solutions un certain nombre d'entre elles qui offrent ce caractère singulier de donner lieu *à des entiers complexes dont le module analytique est l'unité*. Ainsi du minimum de la forme

$$\Phi=\frac{\varphi(\beta_1)\,\varphi(\gamma_1)}{\varphi_0(\beta_1)\,\varphi_0(\gamma_1)}+\frac{\varphi(\beta_2)\,\varphi(\gamma_2)}{\varphi_0(\beta_2)\,\varphi_0(\gamma_2)}+\ldots+\frac{\varphi(\beta_{n'})\,\varphi(\gamma_{n'})}{\varphi_0(\beta_{n'})\,\varphi_0(\gamma_{n'})}$$

on déduira non seulement

$$\varphi(\beta_1)=\varphi_0(\beta_1),\quad \varphi(\gamma_1)=\varphi_0(\gamma_1),\quad \ldots,\quad \varphi(\beta_{n'})=\varphi_0(\beta_{n'}),\quad \varphi(\gamma_{n'})=\varphi_0(\gamma_{n'}),$$

mais encore

$$\varphi(\beta_1)=\varphi_0(\beta_1)\,\psi(\beta_1),\qquad \varphi(\gamma_1)=\varphi_0(\gamma_1)\,\psi(\gamma_1),\qquad \ldots,$$
$$\varphi(\beta_{n'})=\varphi_0(\beta_{n'})\,\psi(\beta_{n'}),\qquad \varphi(\gamma_{n'})=\varphi_0(\gamma_{n'})\,\psi(\gamma_{n'}),$$

les nombres entiers complexes ψ satisfaisant aux conditions suivantes :

$$\psi(\beta_1)\,\psi(\gamma_1)=1,\qquad \psi(\beta_2)\,\psi(\gamma_2)=1,\qquad \ldots,\qquad \psi(\beta_{n'})\,\psi(\gamma_{n'})=1,$$

et l'on pourra en faire abstraction puisqu'ils peuvent être déterminés d'avance. J'ai trouvé, du moins, *qu'ils ne pouvaient être que de cette forme, savoir :*

$$\psi=e^{\frac{2k\pi}{l}\sqrt{-1}},$$

k et l étant entiers. Le dénominateur l est sans doute égal au nombre $2n'+1$, mais je n'ai pu encore suffisamment approfondir toutes ces circonstances qui me paraissent bien singulières.

Quoi qu'il en soit, les considérations qui précèdent établissent qu'on n'aura jamais à rechercher qu'une seule représentation, en nombres entiers, de chacun des minima distincts, donnant lieu à une unité complexe, qu'offrira la forme Φ, lorsque les quantités

$$A_1,\quad A_2,\quad \ldots,\quad A_n,\qquad K_1,\quad K_2,\quad \ldots,\quad K_{n'}$$

passeront par tous les états possibles de grandeur. Mais, une fois amenés à cette nouvelle recherche, il faut recourir à la théorie de la *réduction* des formes quadratiques quelconques. Je vais, avant tout, définir *ce que j'appelle réduire une forme donnée* (1).

Soient f cette forme, et f', f'', ... la série entière de toutes celles qui lui sont équivalentes, et que je représenterai, d'une manière générale, par

$$f=\sum_1^n{}_j\sum_1^n{}_i a_{j,i}x_ix_j,$$

en supposant que les coefficients des carrés, rangés par ordre croissant de grandeur, soient

$$a_{1,1},\quad a_{2,2},\quad \ldots,\quad a_{n,n}.$$

Cela étant, nous subdiviserons, progressivement, l'ensemble de toutes les formes équivalentes, en réunissant dans un même groupe :

1° Toutes les formes où $a_{1,1}$ a la plus petite valeur possible;

2° Parmi celles-ci, toutes celles où $a_{2,2}$ est également un minimum;

3° Parmi les précédentes, celles où $a_{3,3}$ est encore un minimum; et ainsi de suite, de telle sorte qu'après avoir épuisé la série $a_{1,1}$, $a_{2,2}$, ..., $a_{n,n}$ on arrive à *une* ou *plusieurs* formes dont les coefficients des carrés sont nécessairement les mêmes.

Ces formes offrent un caractère essentiel qui consiste en ce que toutes les expressions quadratiques

$$(a_{i,i},\ a_{i,j},\ a_{j,j})$$

sont réduites. On peut établir qu'on a la limite

$$a_{1,1}a_{2,2}\ldots a_{n,n}<\mu D,$$

μ étant un coefficient numérique ne dépendant que du nombre n des variables; mais je ne m'arrêterai pas à la démonstration.

Revenons au dernier groupe de formes équivalentes auquel nous venons de parvenir, il pourra être subdivisé de nouveau, d'après la

(1) Il est clair, d'après les opérations indiquées, qu'il s'agit seulement ici de formes définies. E. P.

grandeur des déterminants

$$A_{i,j} = a_{i,i}a_{j,j} - a_{i,j}^2,$$

en réunissant ensemble :

1° Toutes les formes où $A_{1,2}$ sera le plus petit possible;

2° Parmi ces dernières, toutes celles où $A_{1,3}$ est également un minimum;

3° Parmi les précédentes, celles où $A_{1,4}$ est encore un minimum; et ainsi de suite, de telle sorte qu'après avoir épuisé la série

$$A_{1,2},\quad A_{1,3},\quad \ldots,\quad A_{1,n},$$

on passe à la suivante

$$A_{2,3},\quad A_{2,4},\quad \ldots,\quad A_{2,n},$$

puis à celle-ci

$$A_{3,4},\quad A_{3,5},\quad \ldots,\quad A_{3,n},$$

et l'on continuera jusqu'à ce qu'on soit arrivé, en dernière analyse, à une ou à plusieurs formes offrant des valeurs numériques égales, pour toutes les quantités $A_{i,j}$.

Mais il est évident qu'alors les valeurs *absolues* des coefficients $a_{i,j}$ sont pareillement les mêmes. Or la forme unique qu'il faudra définitivement choisir pour réduire s'obtiendra par la considération des déterminants ternaires

$$A_{i,j,k} = a_{i,i}a_{j,j}a_{k,k} + 2a_{i,j}a_{i,k}a_{j,k} - a_{i,i}a_{j,k}^2 - a_{j,j}a_{i,k}^2 - a_{k,k}a_{i,j}^2,$$

en opérant comme on a fait précédemment avec les fonctions $A_{i,j}$. Les formes réunies en dernier lieu, offrant les mêmes valeurs des diverses expressions $A_{i,j,k}$, deviendront *identiques* (1), en rendant positifs par exemple, comme cela est toujours possible, tous les coefficients $a_{1,i}$.

Réduire une forme donnée f, ce sera donc chercher la transformation de cette forme en la réduite équivalente telle qu'elle vient d'être définie. Cette réduite, comme vous le voyez, Monsieur, n'est pas celle à laquelle conduit la méthode que j'ai eu l'honneur de vous soumettre dans ma dernière Lettre. Il y aura donc lieu d'es-

(1) Si certains des coefficients $a_{1i}(i = 2, 3, \ldots, n)$ étaient nuls, on n'obtiendrait pas nécessairement ainsi l'identité des deux formes, mais il est facile de combler cette lacune de manière à avoir toujours une réduite unique. E. P.

pérer une nouvelle substitution, mais jusqu'ici je n'ai vu d'autre moyen à employer que celui qui est indiqué par l'analyse précédente et qui consiste à former la série entière des formes aux plus petits coefficients des carrés. Seulement, il est facile de démontrer *que leur nombre a une limite indépendante du déterminant et qui est fonction uniquement du nombre des indéterminées.*

Dans le cas des formes ternaires, les réduites jouissent d'une propriété qui mérite peut-être d'être remarquée, *car elle ne me paraît pas s'étendre aux formes contenant un plus grand nombre de variables.* Elle consiste en ce que *toute forme ternaire réduite* $\varphi(x, y, z)$ *prend une valeur moindre, en diminuant celle des variables dont la valeur absolue est plus grande.*

Soit

$$\varphi = ax^2 + a'y^2 + a''z^2 + 2byz + 2b'xz + 2b''xy.$$

En supposant quelconques les signes des coefficients b, b', b'', on peut admettre que les indéterminées sont positives. Or, en supposant $x \geq y$, $x > z$, on prouve aisément la proposition énoncée (1), dans chacun des quatre cas qu'offrent les signes de b' et b'', au moyen des équations identiques

$$\begin{aligned}
&\varphi(x-1, y, z) - \varphi(x, y, z)\\
&= -2(x-1)(a + b'' + b') + 2b''(x - y - 1) + 2b'(x - z - 1) - a\\
&= -2(x-1)(a + b') - 2b''y + 2b'(x - z - 1) - a\\
&= -2(x-1)(a + b'') + 2b''(x - y - 1) - 2b'z - a\\
&= -2(x-1)a - 2b''y - 2b'z - a,
\end{aligned}$$

les quatre expressions précédentes correspondant aux quatre cas

$$b' : - - + +,$$
$$b'' : - + - +.$$

Je reviens maintenant à la recherche de toutes les représentations distinctes des divers *minima* de la forme quadratique

$$\Phi = \left[\frac{\varphi(x_1)}{A_1}\right]^2 + \left[\frac{\varphi(x_2)}{A_2}\right]^2 + \ldots + \left[\frac{\varphi(x_n)}{A_n}\right]^2 + 2\frac{\varphi(\beta_1)\varphi(\gamma_1)}{K_1^2} + 2\frac{\varphi(\beta_2)\varphi(\gamma_2)}{K_2^2} + \ldots + 2\frac{\varphi(\beta_{n'})\varphi(\gamma_{n'})}{K_{n'}^2},$$

(1) Il peut y avoir un cas d'exception, auquel ne s'applique pas d'ailleurs la démonstration de M. Hermite; c'est celui dans lequel les trois variables ont leurs valeurs absolues égales à l'unité. E. P.

correspondant à tous les systèmes possibles de valeurs de A_1, $A_2, \ldots, K_1, K_2, \ldots$.

Dans cette forme, les quantités $\varphi(\alpha)$ sont les valeurs d'une expression telle que

$$x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{m-1} x_{m-1},$$

en supposant α, l'une quelconque des racines de l'équation,

$$F(x) = 0,$$

dont le degré $n + 2n'$ est toujours désigné par m. Cela posé, soit pour un système déterminé de valeurs des quantités A et K,

$$\begin{aligned} x_0 &= a_0 y_0 + a_1 y_1 + \ldots + a_{m-1} y_{m-1}, \\ x_1 &= b_0 y_0 + b_1 y_1 + \ldots + b_{m-1} y_{m-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_{m-1} &= l_0 y_0 + l_1 y_1 + \ldots + l_{m-1} y_{m-1}, \end{aligned}$$

la substitution propre à réduire Φ. En posant, pour abréger,

$$\begin{aligned} (\alpha)_i &= a_i + \alpha b_i + \alpha^2 c_i + \ldots + \alpha^{m-1} l_i, \\ \psi(\alpha) &= y_0 (\alpha)_0 + y_1 (\alpha)_1 + \ldots\ldots\ldots + y_{m-1} (\alpha)_{m-1}, \end{aligned}$$

la transformée réduite sera

$$\Psi = \left[\frac{\psi(\alpha_1)}{A_1}\right]^2 + \left[\frac{\psi(\alpha_2)}{A_2}\right]^2 + \ldots + \left[\frac{\psi(\alpha_n)}{A_n}\right]^2 + 2\frac{\psi(\beta_1)\psi(\gamma_1)}{K_1^2} + 2\frac{\psi(\beta_2)\psi(\gamma_2)}{K_2^2} + \ldots + 2\frac{\psi(\beta_{n'})\psi(\gamma_{n'})}{K_{n'}^2}.$$

Mais on peut l'écrire d'une autre manière.

Soit y_0 celle des indéterminées dont le carré a le plus petit coefficient, et posons

$$N = (\alpha_1)_0 (\alpha_2)_0 \ldots (\alpha_n)_0 (\beta_1)_0 (\gamma_1)_0 \ldots (\beta_{n'})_0 (\gamma_{n'})_0,$$

il est clair que, α désignant l'une quelconque des racines, $\frac{N}{(\alpha)_0}$ sera un polynome à coefficients entiers en α, et qu'il en sera de même de

$$\frac{N}{(\alpha)_0}(\alpha)_i,$$

que je désignerai par $\psi_i(\alpha)$. Or, de la valeur-limite du produit des coefficients des carrés des indéterminées dans toute forme réduite, telle qu'elle a été indiquée plus haut, on déduit facilement, *que*

tous ces polynomes $\psi_i(\alpha)$ ont pour coefficients des nombres entiers ayant aussi des limites finies. Il en est de même d'ailleurs de N, comme on l'a vu précédemment d'une manière spéciale. Donc, transformant ainsi les fonctions $\psi(\alpha)$, savoir :

$$\psi(\alpha) = \frac{(\alpha)_0}{N}[y_0 N + y_1 \psi_1(\alpha) + y_2 \psi_2(\alpha) + \ldots + y_{m-1}\psi_{m-1}(\alpha)],$$

et posant

$$\chi(\alpha) = y_0 N + y_1 \psi_1(\alpha) + y_2 \psi_2(\alpha) + \ldots + y_{m-1}\psi_{m-1}(\alpha),$$

$$\frac{(\alpha_i)_0}{N A_i} = \frac{1}{A_i'}, \qquad \frac{(\beta_i)_0 (\gamma_i)_0}{N^2 K_i^2} = \frac{1}{K_i'^2},$$

l'expression de ψ devient

$$\Psi = \left[\frac{\chi(\alpha_1)}{A_1'}\right]^2 + \left[\frac{\chi(\alpha_2)}{A_2'}\right]^2 + \ldots + \left[\frac{\chi(\alpha_n)}{A_n'}\right]^2 + 2\frac{\chi(\beta_1)\chi(\gamma_1)}{K_1'^2} + \ldots,$$

et c'est là *le type analytique* (1) auquel je voulais arriver pour y rapporter toute forme réduite. Le nombre de ces types, comme on le voit d'après le caractère des fonctions $\chi(\alpha)$, est essentiellement *fini,* et c'est là un résultat qui ouvre la voie à un nouvel ordre de recherches destinées, si je ne m'abuse étrangement, à jeter un grand jour sur la nature si inconnue des irrationnelles algébriques.

Et d'abord, *on en déduit immédiatement une démonstration directe de la possibilité de l'équation que je me suis proposé de résoudre, savoir*

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

En effet, on a pour cela le théorème : *Que lorsqu'une substitution*

$$\begin{aligned} x_0 &= p_0 y_0 + p_1 y_1 + \ldots + p_{m-1} y_{m-1}, \\ x_1 &= q_0 y_0 + q_1 y_1 + \ldots + q_{m-1} y_{m-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_{m-1} &= s_0 y_0 + s_1 y_1 + \ldots + s_{m-1} y_{m-1}, \end{aligned}$$

correspondant à un système différent de valeurs de $A_1, A_2, \ldots, K_1, K_2, \ldots$, *conduit au même type réduit* Ψ, *le nombre entier*

(1) D'après M. Hermite deux de ces types sont les mêmes lorsqu'ils ne diffèrent entre eux que par rapport aux quantités A' et K'. JACOBI.