10.

Extrait d'une lettre de M. *C. Hermite* à M. *Borchardt* sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés.

Permettez moi, en continuant en quelque sorte, ce que je Vous ai écrit au sujet de la détermination des racines imaginaires des équations algébriques, de Vous entretenir des questions arithmétiques aux quelles je songeais, lorsque chemin faisant, j'ai été ainsi amené aux théorèmes de M. *Cauchy* et de M. *Sturm*. Ces questions arithmétiques avaient pour objet la théorie des nombres complexes, et en particulier l'étude des formes décomposables en facteurs linéaires, lorsque les coefficients sont des entiers de l'espèce $a+b\sqrt{-1}$. Pour le cas des entiers réels, la réduction des formes quadratiques définies, avait été comme Vous savez l'instrument analytique que j'avais surtout mis en oeuvre, mais pour passer de là aux nombres complexes, il fallait à ma méthode une modification que j'ai été bien longtemps à découvrir. C'est le hazard en effet qui me l'a donnée, en traitant de la décomposition des nombres en quatre carrés, sous le point de vue que j'ai indiqué dans le tome 47 de ce journal. Je vais essayer de Vous en donner une idée précise, en démontrant ce théorême que j'ai eu déjà occasion d'énoncer dans une note de mon travail sur la théorie de la transformation des fonctions Abéliennes, savoir: *Les racines de toutes les équations à coefficients entiers complexes, d'un degré donné, et pour lesquelles le discriminant (déterminant de Gauss) a la même valeur, ne représentent qu'un nombre essentiellement limité d'irrationalités distinctes.* J'aurai pour cela, deux points principaux à établir. Le premier consiste dans la théorie arithmétique de la réduction de ces formes quadratiques à indéterminées imaginaires conjuguées que j'ai fait servir à la démonstrations du théorême de M. *Cauchy*. En désignant par $x, y, z, \dots v$, $n+1$ indéterminées imaginaires, et par $x_0, y_0, z_0, \dots v_0$ leurs conjuguées respectives, elles sont comme Vous savez définies de cette manière:

$$\begin{aligned} f = & \; x_0(a_{0,0}x + a_{0,1}y + a_{0,2}z + \cdots + a_{0,n}v) \\ & + y_0(a_{1,0}x + a_{1,1}y + a_{1,2}z + \cdots + a_{1,n}v) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + v_0(a_{n,0}x + a_{n,1}y + a_{n,2}z + \cdots + a_{n,n}v) \end{aligned}$$

avec la condition que $a_{\mu,\nu}$ et $a_{\nu,\mu}$ seront des quantités imaginaires conjuguées. En mettant en évidence tant dans les coefficients que dans les indéterminées, les parties réelles et les coefficients de $\sqrt{-1}$, la forme f, sera si l'on veut un cas particulier des formes réelles à $2n+2$ indéterminées, mais qu'on traite grace au jeu des quantités imaginaires, par les procédés essentiellement propres aux formes à $n+1$ indéterminées seulement. Sans insister d'avantage sur cette considération que j'ai développée ailleurs dans le cas de $n=1$, j'énoncerai les propositions algébriques suivantes, qui si simples qu'elles soient, doivent être au moins indiquées pour ne rien omettre dans l'enchainement des idées.

1°. En faisant dans f, la substitution:

$$S\begin{cases} x = \alpha X + \alpha' Y + \cdots + \alpha^{(n)} V \\ y = \beta X + \beta' Y + \cdots + \beta^{(n)} V \\ z = \gamma X + \gamma' Y + \cdots + \gamma^{(n)} V \\ \cdots\cdots\cdots\cdots\cdots \\ v = \lambda X + \lambda' Y + \cdots + \lambda^{(n)} V \end{cases} \qquad S_0\begin{cases} x_0 = \alpha_0 X_0 + \alpha'_0 Y_0 + \cdots + \alpha_0^{(n)} V_0 \\ y_0 = \beta_0 X_0 + \beta'_0 Y_0 + \cdots + \beta_0^{(n)} V_0 \\ z_0 = \gamma_0 X_0 + \gamma'_0 Y_0 + \cdots + \gamma_0^{(n)} V_0 \\ \cdots\cdots\cdots\cdots\cdots \\ v_0 = \lambda_0 X_0 + \lambda'_0 Y_0 + \cdots + \lambda_0^{(n)} V_0 \end{cases}$$

ou, α et α_0, β et β_0, etc. sont des quantités imaginaires conjuguées, on aura une transformée *de même nature:*

$$\begin{aligned} F = & \; X_0(A_{0,0}X + A_{0,1}Y + A_{0,2}Z + \cdots + A_{0,n}V) \\ & + Y_0(A_{1,0}X + A_{1,1}Y + A_{1,2}Z + \cdots + A_{1,n}V) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + V_0(A_{n,0}X + A_{n,1}Y + A_{n,2}Z + \cdots + A_{n,n}V) \end{aligned}$$

de sorte que, $A_{\mu,\nu}$ et $A_{\nu,\mu}$ seront comme $a_{\mu,\nu}$ et $a_{\nu,\mu}$ des quantités conjuguées.

2°. Soient D, d, ω, ω_0 les déterminants des systèmes suivants:

$$D = \begin{Bmatrix} A_{0,0} & A_{0,1} & \ldots & A_{0,n} \\ A_{1,0} & A_{1,1} & \ldots & A_{1,n} \\ \cdot & \cdot & \cdot & \cdot \\ A_{n,0} & A_{n,1} & \ldots & A_{n,n} \end{Bmatrix} \qquad d = \begin{Bmatrix} a_{0,0} & a_{0,1} & \ldots & a_{0,n} \\ a_{1,0} & a_{1,1} & \ldots & a_{1,n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n,0} & a_{n,1} & \ldots & a_{n,n} \end{Bmatrix}$$

$$\omega = \begin{Bmatrix} \alpha & \alpha' & \ldots & \alpha^{(n)} \\ \beta & \beta' & \ldots & \beta^{(n)} \\ \cdot & \cdot & \cdot & \cdot \\ \lambda & \lambda' & \ldots & \lambda^{(n)} \end{Bmatrix} \qquad \omega_0 = \begin{Bmatrix} \alpha_0 & \alpha'_0 & \ldots & \alpha_0^{(n)} \\ \beta_0 & \beta'_0 & \ldots & \beta_0^{(n)} \\ \cdot & \cdot & \cdot & \cdot \\ \lambda_0 & \lambda'_0 & \ldots & \lambda_0^{(n)} \end{Bmatrix}$$

on aura l'équation $D = d\omega\omega_0$, d'où résulte que d peut être regardé comme l'invariant de la forme f.

En vue de la théorie de la réduction, j'ajouterai cette remarque, qu'en posant:

$$\begin{aligned} g = a_{0,0}f - \frac{df}{dx}\cdot\frac{df}{dx_0} = & \; y_0(b_{1,1}y + b_{1,2}z + \cdots + b_{1,n}v) \\ & + z_0(b_{2,1}y + b_{2,2}z + \cdots + b_{2,n}v) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + v_0(b_{n,1}y + b_{n,2}z + \cdots + b_{n,n}v) \end{aligned}$$

ou $b_{\mu,\nu} = a_{0,0}a_{\mu,\nu} - a_{\mu,0}a_{0,\nu}$ on obtient une forme aux indéterminées y et y_0, z et z_0 ... v et v_0 qui est un *covariant* de f, relativement à la substitution (S, S_0) quand on y suppose $\alpha = 1$, $\beta = 0$, $\gamma = 0$, ... $\lambda = 0$. Et si l'on appelle D' l'invariant de g, on aura $D' = a_{0,0}^{n-1}D$. Cela posé, je vais établir qu'étant donnée une forme f *définie,* on peut trouver pour les coefficients de la substitution S, des nombres entiers complexes, dont le déterminant ω soit un, et tels que dans la transformée F, on ait:

$$(a.) \qquad A_{0,0}A_{1,1}\ldots A_{n,n} < 2^{\frac{n(n+1)}{2}} D$$

Ce sera cette transformée que j'appellerai réduite. A cet effet, je considère l'ensemble des formes déduites de f, par toutes les substitutions (S, S_0) à coefficients entiers complexes et au déterminant 1. Je distingue ensuite dans ces transformées, celles ou le coefficient de XX_0 est le plus petit possible. Parmis ces dernières, je dis qu'il en existe une que je représenterai ainsi:

$$\begin{aligned} F = & \; X_0(A_{0,0}X + A_{0,1}Y + \cdots + A_{0,n}V) \\ & + Y_0(A_{1,0}X + A_{1,1}Y + \cdots + A_{1,n}V) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + V_0(A_{n,0}X + A_{n,1}Y + \cdots + A_{n,n}V) \end{aligned}$$

et remplissant ces deux conditions, premièrement que la forme:

$$\begin{aligned} G = A_{0,0}F - \frac{dF}{dX}\cdot\frac{dF}{dX_0} = & \; Y_0(B_{1,1}Y + B_{1,2}Z + \cdots + B_{1,n}V) \\ & + Z_0(B_{2,1}Y + B_{2,2}Z + \cdots + B_{2,n}V) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + V_0(B_{n,1}Y + B_{n,2}Z + \cdots + B_{n,n}V) \end{aligned}$$

soit réduite dans le sens propre aux formes à n paires d'indéterminées, secondement, que les parties réelles et les coefficients de $\sqrt{-1}$ dans les diverses quantités $A_{0,\mu}$ soient moindres que la moitié du coefficient minimum $A_{0,0}$.

En effet, en faisant dans F, la substitution:

$$\begin{array}{ll}
X = \mathfrak{x} + \mathfrak{m}\mathfrak{y} + \mathfrak{n}\mathfrak{z} + \cdots + \mathfrak{r}\mathfrak{v} & X_0 = \mathfrak{x}_0 + \mathfrak{m}_0\mathfrak{y}_0 + \mathfrak{n}_0\mathfrak{z}_0 + \cdots + \mathfrak{r}_0\mathfrak{v}_0 \\
Y = \mathfrak{m}'\mathfrak{y} + \mathfrak{n}'\mathfrak{z} + \cdots + \mathfrak{r}'\mathfrak{v} & Y_0 = \mathfrak{m}'_0\mathfrak{y}_0 + \mathfrak{n}'_0\mathfrak{z}_0 + \cdots + \mathfrak{r}'_0\mathfrak{v}_0 \\
Z = \mathfrak{m}''\mathfrak{y} + \mathfrak{n}''\mathfrak{z} + \cdots + \mathfrak{r}''\mathfrak{v} & Z_0 = \mathfrak{m}''_0\mathfrak{y}_0 + \mathfrak{n}''_0\mathfrak{z}_0 + \cdots + \mathfrak{r}''_0\mathfrak{v}_0 \\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\
V = \mathfrak{m}^{(n)}\mathfrak{y} + \mathfrak{n}^{(n)}\mathfrak{z} + \cdots + \mathfrak{r}^{(n)}\mathfrak{v} & V_0 = \mathfrak{m}^{(n)}_0\mathfrak{y}_0 + \mathfrak{n}^{(n)}_0\mathfrak{z}_0 + \cdots + \mathfrak{r}^{(n)}_0\mathfrak{v}_0
\end{array}$$

on trouvera une transformée $\mathfrak{F}$, dans la quelle le coefficient de $\mathfrak{x}\mathfrak{x}_0$ sera encore $A_{0,0}$ et où la forme $\mathfrak{G}$ analogue à G, savoir $\mathfrak{G} = A_{0,0}\mathfrak{F} - \frac{d\mathfrak{F}}{d\mathfrak{x}}\frac{d\mathfrak{F}}{d\mathfrak{x}_0}$ sera (d'après ce qui a été dit tout-à-l'heure) la transformée de G par la substitution:

$$\begin{array}{ll}
Y = \mathfrak{m}'\mathfrak{y} + \mathfrak{n}'\mathfrak{z} + \cdots + \mathfrak{r}'\mathfrak{v} & Y_0 = \mathfrak{m}'_0\mathfrak{y}_0 + \mathfrak{n}'_0\mathfrak{z}_0 + \cdots + \mathfrak{r}'_0\mathfrak{v}_0 \\
Z = \mathfrak{m}''\mathfrak{y} + \mathfrak{n}''\mathfrak{z} + \cdots + \mathfrak{r}''\mathfrak{v} & Z_0 = \mathfrak{m}''_0\mathfrak{y}_0 + \mathfrak{n}''_0\mathfrak{z}_0 + \cdots + \mathfrak{r}''_0\mathfrak{v}_0 \\
\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\
V = \mathfrak{m}^{(n)}\mathfrak{y} + \mathfrak{n}^{(n)}\mathfrak{z} + \cdots + \mathfrak{r}^{(n)}\mathfrak{v} & V_0 = \mathfrak{m}^{(n)}_0\mathfrak{y}_0 + \mathfrak{n}^{(n)}_0\mathfrak{z} + \cdots + \mathfrak{r}^{(n)}_0\mathfrak{v}_0
\end{array}$$

Mais cette substitution est la plus générale entre les n paires d'indéterminées conjuguées, et peut être employée à réduire la forme $\mathfrak{G}$; on voit donc bien qu'on peut admettre dans l'ensemble des formes dont j'ai parlé, l'existence d'une transformée remplissant la première des conditions énoncées. Quant à la seconde, on y satisfait à l'aide des entiers complexes $\mathfrak{m}, \mathfrak{n}, \ldots \mathfrak{r}$, qui restent jusqu'ici arbitraires; en désignant en effet pour un instant par $\mathfrak{a}_{0,\mu}$ les coefficients de $\mathfrak{F}$ qui correspondent à $A_{0,\mu}$, on a les relations:

$$\begin{array}{l}
\mathfrak{a}_{0,1} = \mathfrak{m}A_{0,0} + \mathfrak{m}'A_{0,1} + \mathfrak{m}''A_{0,2} + \cdots + \mathfrak{m}^{(n)}A_{0,n} \\
\mathfrak{a}_{0,2} = \mathfrak{n}A_{0,0} + \mathfrak{n}'A_{0,1} + \mathfrak{n}''A_{0,2} + \cdots + \mathfrak{n}^{(n)}A_{0,n} \\
\cdots\cdots\cdots\cdots\cdots\cdots \\
\mathfrak{a}_{0,n} = \mathfrak{r}A_{0,0} + \mathfrak{r}'A_{0,1} + \mathfrak{r}''A_{0,2} + \cdots + \mathfrak{r}^{(n)}A_{0,n}
\end{array}$$

et on voit qu'on peut déterminer les entiers complexes, $\mathfrak{m}, \mathfrak{n}, \ldots \mathfrak{r}$, de manière que la partie réelle et le coefficient de $\sqrt{-1}$ dans $\mathfrak{a}_{0,1}, \mathfrak{a}_{0,2}, \ldots \mathfrak{a}_{0,n}$, soient au dessous de $\frac{1}{2}A_{0,0}$. Admettant donc l'existence de la forme F, remplissant les deux conditions précédentes, nous allons supposer que la relation (*a.*) soit vraie à l'égard des formes réduites contenant n paires d'indéterminées et nous en conclurons qu'elle a lieu nécessairement dans les formes qui en renferment $n+1$. Elle se trouvera ainsi établie dans toute sa généralité puisqu'elle a lieu comme je l'ai fait voir ailleurs (dans ce Journal T. 47) pour $n=1$. A cet effet j'observe que les coefficients de la forme G, ayant pour expression générale $B_{\mu,\nu} = A_{0,0}A_{\mu,\nu} - A_{\mu,0}A_{0,\nu}$, on trouvera lorsque les deux indices sont égaux $B_{\mu,\mu} = A_{0,0} A_{\mu,\mu} - A_{\mu,0} A_{0,\mu}$ de sorte que ces quantités peuvent alors être regardées comme les invariants de formes quadratiques à deux paires d'indéterminées $(A_{0,0}, A_{\mu,0}, A_{0,\mu}, A_{\mu,\mu})$ formes qui seront définies et réduites. Définies car nous avons supposé f et par suite F elle même définie, et réduites, par ce que le coefficient minimum $A_{0,0}$ sera au plus égal à $A_{\mu,\mu}$, et que la partie réelle comme le coefficient de $\sqrt{-1}$ dans $A_{\mu,0}$ sont au dessous de la limite $\frac{1}{2} A_{0,0}$. Donc d'après ce que j'ai établi dans le mémoire précité, on aura:

$$A_{0,0} A_{\mu,\mu} < 2 B_{\mu,\mu}$$

et par suite:

$$A_{0,0}^n A_{1,1} A_{2,2} \ldots A_{n,n} < 2^n B_{1,1} B_{2,2} \ldots B_{n,n}.$$

Mais en admettant la relation (a) pour les formes réduites G, qui contiennent n paires d'indéterminées et dont l'invariant est $A_{0,0}^{n-1} D$, on aura:

$$B_{1,1} B_{2,2} \ldots B_{n,n} < 2^{\frac{n(n-1)}{2}} A_{0,0}^{n-1} D$$

or on en conclut après avoir multiplié membre à membre par l'inégalité précédente, et supprimé le facteur $A_{0,0}^{n-1}$:

$$A_{0,0} A_{1,1} A_{2,2} \ldots A_{n,n} < 2^{\frac{n(n+1)}{2}} D$$

C'est ce résultat qui tout-à-l'heure me servira de base pour la théorie de la réduction des formes décomposables en facteurs linéaires, et qui sont à coefficients et indéterminées complexes. Mais j'indiquerai d'abord la conséquence suivante qui s'en tire immédiatement.

Concevons qu'en vue de la théorie des formes f telle que je l'envisage ici, on modifie l'idée arithmétique de *classe*, de manière à désigner ainsi l'ensemble des transformées déduites d'une forme donnée, par ces substitutions spéciales, (S, S_0) lorsqu'on attribue aux coefficients, touts les systèmes de valeurs entières complexes, pour les quelles le déterminant $\omega = 1$, on aura ce théorème: ***La totalité des formes de la même expression analytique que f, lorsqu'on les suppose définies, et à coefficients entiers tant réels que complexes, ne représente pour un invariant donné, qu'un nombre essentiellement limité de classes distinctes.*** Effectivement, dans la réduite F, touts les coefficients réels $A_{\mu,\mu}$ sont limités en vertu de la relation (a) et les modules des coefficients imaginaires $A_{\mu,\nu}$, le sont par la condition

$$A_{\mu,\mu} A_{\nu,\nu} - A_{\mu,\nu} A_{\nu,\mu} > 0$$

qui résulte comme on le voit immédiatement de ce qu'on suppose F une forme définie. On n'aura donc pour une valeur données de l'invariant qu'un nombre limité de réduites, et par conséquent un nombre limité de classes.

Je passe maintenant au second point qui me reste à traiter pour arriver à mon théorème.

Soit φ une forme à n indéterminées imaginaires, $x, y, \ldots u$, à coefficients complexes, et décomposable en n facteurs linéaires, savoir:

$$\begin{aligned} A &= ax + a'y + \cdots + a^{(n-1)}u \\ B &= bx + b'y + \cdots + b^{(n-1)}u \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ L &= lx + l'y + \cdots + l^{(n-1)}u \end{aligned}$$

de sorte qu'on ait $\varphi = AB \ldots L$. Ces quantités $A, B, \ldots L$, ne se trouveront point complétement déterminées par la forme donnée φ, car il est clair qu'on peut multiplier par un facteur constant chacune d'elle, pourvu que le produit de touts ces facteurs constants soit l'unité. J'observe cependant que le déterminant Δ, relatif au système de ces fonctions linéaires, ne subira aucun changement par l'introduction de ces multiplicateurs arbitraires, car en remplaçant $A, B, \ldots L$, par $t_1 A, t_2 B, \ldots t_n L$ le déterminant relatif aux nouvelles fonctions sera $t_1 t_2 \ldots t_n \Delta$, et on doit faire comme nous l'avons dit: $t_1 t_2 \ldots t_n = 1$. Nous pouvons donc désormais, regarder Δ, comme absolument déterminé par la forme proposée φ. Cela posé, j'introduis encore les facteurs linéaires conjugués de $A, B, \ldots L$, qui seront en suivant la notation déjà employée:

$$\begin{aligned} A_0 &= a_0 x_0 + a'_0 y_0 + \cdots + a_0^{(n-1)} u_0 \\ B_0 &= b_0 x_0 + b'_0 y_0 + \cdots + b_0^{(n-1)} u_0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ L_0 &= l_0 x_0 + l'_0 y_0 + \cdots + l_0^{(n-1)} u_0 \end{aligned}$$

et dont le déterminant sera désigné par Δ_0. Puis je compose avec ces deux groupes de fonctions, la forme quadratique suivante, de la nature de celles qui nous ont occupé précédemment, savoir:

$$f = AA_0 + BB_0 + \cdots + LL_0$$

Cette forme dépendra essentiellement, des multiplicateurs arbitraires que l'on peut introduire dans les fonctions linéaires, A, B, etc., mais quelque soient ces multiplicateurs, son invariant D sera la quantité entièrement connue $D = \Delta\Delta_0$, de plus elle sera toujours définie, et on pourra lui appliquer la méthode de réduction exposée plus haut. Concevons donc que pour un système déterminé, des facteurs linéaires, $A, B, \ldots L$, on ait obtenu la substitution propre à effectuer cette réduction, et que je continuerai de représenter par la notation (S, S_0). En effectuant la partie de cette substitution désignée par S, dans $A, B, \ldots L$, je supposerai qu'ils deviennent:

$$\begin{aligned}
\mathfrak{A} &= \mathfrak{a}X + \mathfrak{a}'Y + \cdots + \mathfrak{a}^{(n-1)}U \\
\mathfrak{B} &= \mathfrak{b}X + \mathfrak{b}'Y + \cdots + \mathfrak{b}^{(n-1)}U \\
&\cdots\cdots\cdots\cdots\cdots \\
\mathfrak{L} &= \mathfrak{l}X + \mathfrak{l}'Y + \cdots + \mathfrak{l}^{(n-1)}U
\end{aligned}$$

tandis que par la substitution S_0, les facteurs conjugués $A_0, B_0, \ldots L_0$, se changent en:

$$\begin{aligned}
\mathfrak{A}_0 &= \mathfrak{a}_0X_0 + \mathfrak{a}'_0Y_0 + \cdots + \mathfrak{a}_0^{(n-1)}U_0 \\
\mathfrak{B}_0 &= \mathfrak{b}_0X_0 + \mathfrak{b}'_0Y_0 + \cdots + \mathfrak{b}_0^{(n-1)}U_0 \\
&\cdots\cdots\cdots\cdots\cdots \\
\mathfrak{L}_0 &= \mathfrak{l}_0X_0 + \mathfrak{l}'_0Y_0 + \cdots + \mathfrak{l}_0^{(n-1)}U_0.
\end{aligned}$$

De là résultera pour la transformée de φ, par la substitution S, l'expression: $\Phi = \mathfrak{A}.\mathfrak{B}\ldots\mathfrak{L}$, et pour la transformée réduite de f, par la substitution (S, S_0) la suivante:

$$F = \mathfrak{A}\mathfrak{A}_0 + \mathfrak{B}\mathfrak{B}_0 + \cdots + \mathfrak{L}\mathfrak{L}_0.$$

Cela étant, je vais démontrer, qu'en supposant la forme donnée φ, à coefficients entiers complexes, et irréductible, dans ce sens que l'équation $\varphi = 0$, n'admette d'autres solutions entières que $x = 0$, $y = 0$, $\ldots$ $u = 0$, les coefficients de Φ, qui seront aussi des entiers complexes, auront tous des valeurs finies et limitées par l'invariant $D = \Delta\Delta_0$.

Soient à cet effet, $\sigma, \sigma_1, \ldots \sigma_{n-1}$, les coefficients de XX_0, YY_0, $\ldots$ UU_0, dans la forme réduite F, à savoir:

$$\begin{aligned}
\sigma &= \mathfrak{a}\mathfrak{a}_0 + \mathfrak{b}\mathfrak{b}_0 + \cdots + \mathfrak{l}\mathfrak{l}_0 \\
\sigma_1 &= \mathfrak{a}'\mathfrak{a}'_0 + \mathfrak{b}'\mathfrak{b}'_0 + \cdots + \mathfrak{l}'\mathfrak{l}'_0 \\
&\cdots\cdots\cdots\cdots\cdots \\
\sigma_{n-1} &= \mathfrak{a}^{(n-1)}\mathfrak{a}_0^{(n-1)} + \mathfrak{b}^{(n-1)}\mathfrak{b}_0^{(n-1)} + \cdots + \mathfrak{l}^{(n-1)}\mathfrak{l}_0^{(n-1)}
\end{aligned}$$

Ces relations peuvent s'écrire de la manière suivante:

$$\begin{aligned}
1 &= \bmod^2\frac{\mathfrak{a}}{\sqrt{\sigma}} + \bmod^2\frac{\mathfrak{b}}{\sqrt{\sigma}} + \cdots + \bmod^2\frac{\mathfrak{l}}{\sqrt{\sigma}} \\
1 &= \bmod^2\frac{\mathfrak{a}'}{\sqrt{\sigma_1}} + \bmod^2\frac{\mathfrak{b}'}{\sqrt{\sigma_1}} + \cdots + \bmod^2\frac{\mathfrak{l}'}{\sqrt{\sigma_1}} \\
&\cdots\cdots\cdots\cdots\cdots \\
1 &= \bmod^2\frac{\mathfrak{a}^{(n-1)}}{\sqrt{\sigma_{n-1}}} + \bmod^2\frac{\mathfrak{b}^{(n-1)}}{\sqrt{\sigma_{n-1}}} + \cdots + \bmod^2\frac{\mathfrak{l}^{(n-1)}}{\sqrt{\sigma_{n-1}}}
\end{aligned}$$

et montrent alors que les modules des quantités $\frac{\mathfrak{a}}{\sqrt{\sigma}}$, $\frac{\mathfrak{b}}{\sqrt{\sigma}}$ etc. sont tous inférieurs à l'unité. Il en résulte qu'en représentant par Ψ, le produit des facteurs:

$$\begin{gathered}
\frac{\mathfrak{a}}{\sqrt{\sigma}}X+\frac{\mathfrak{a}'}{\sqrt{\sigma_1}}Y+\cdots+\frac{\mathfrak{a}^{(n-1)}}{\sqrt{\sigma_{n-1}}}U,\\
\frac{\mathfrak{b}}{\sqrt{\sigma}}X+\frac{\mathfrak{b}'}{\sqrt{\sigma_1}}Y+\cdots+\frac{\mathfrak{b}^{(n-1)}}{\sqrt{\sigma_{n-1}}}U,\\
\dots\dots\dots\dots\dots\dots\\
\frac{\mathfrak{l}}{\sqrt{\sigma}}X+\frac{\mathfrak{l}'}{\sqrt{\sigma_1}}Y+\cdots+\frac{\mathfrak{l}^{(n-1)}}{\sqrt{\sigma_{n-1}}}U,
\end{gathered}$$

c. à d. ce que devient Φ, lorsqu'on y remplace, $X, Y, \ldots U$ par: $\frac{1}{\sqrt{\sigma}}X$, $\frac{1}{\sqrt{\sigma_1}}Y, \ldots \frac{1}{\sqrt{\sigma_{n-1}}}U$, les modules des coefficients de cette transformée sont eux mêmes limités. En effet, si pour fixer les idées, nous considérons le coefficient d'un quelconque des termes de Ψ, que nous représenterons par: $X^p Y^q \ldots U^s$, les exposants étant des entiers dont la somme est n, on trouve sans peine que la vàleur *maximum* de son module est donnée par le facteur numérique qui multiplie le même terme $X^p Y^q \ldots U^s$ dans la puissance polynomiale: $\frac{1}{n^{\frac{1}{2}n}}(X+Y+\cdots+U)^n$. Cela posé, convenons de désigner par lès expressions symboliques suivantes: $\{X^p Y^q \ldots U^s\}$ et: $[X^p Y^q \ldots U^s]$, les modules des coefficients de $X^p Y^q \ldots U^s$ dans Φ et Ψ. Il est clair qu'on aura d'après la relation qui lie les deux formes:

$$(1.)\qquad \{X^p Y^q \ldots U^s\} = [X^p Y^q \ldots U^s]\sqrt{\sigma^p \sigma_1^q \ldots \sigma_{n-1}^s}$$

et en particulier pour les coefficients des puissances les plus élevées des indéterminées:

$$(2.)\qquad \begin{cases} \{X^n\} = [X^n]\sqrt{\sigma^n}\\ \{Y^n\} = [Y^n]\sqrt{\sigma_1^n}\\ \dots\dots\dots\dots\\ \{U^n\} = [U^n]\sqrt{\sigma_{n-1}^n} \end{cases}$$

Or en multipliant ces équations membre à membre, il vient:

$$\{X^n\}\{Y^n\}\cdots\{U^n\} = [X^n][Y^n]\cdots[U^n]\sqrt{(\sigma\sigma_1\ldots\sigma_{n-1})^n}$$

mais d'après la relation caractéristique pour les formes quadratiques réduites, et la valeur de l'invariant de F, que nous avons trouvé précédemment égal à $\Delta\Delta_0$, on a:

$$\sigma\sigma_1\ldots\sigma_{n-1} < 2^{\frac{1}{2}n(n-1)}\Delta\Delta_0$$

il en résulte donc que:

$$\{X^n\}\{Y^n\}\cdots\{U^n\} < [X^n][Y^n]\cdots[U^n]\cdot 2^{\frac{1}{2}n(n-1)}\Delta\Delta_0$$

et finalement, en ayant égard aux limites des quantités $[X^n]$, $[Y^n]$ etc.:

$$\{X^n\}\{Y^n\}\cdots\{U^n\} < \frac{2^{\frac{1}{2}n^2(n-1)}}{n^{\frac{1}{2}n^2}}\cdot(\Delta\Delta_0)^{\frac{1}{2}n}$$

Voiçi donc déjà les coefficients des puissances les plus élevées dans la forme Φ, limitées au moyen de l'invariant $\Delta\Delta_0$. Et c'est en ce moment que nous employons la condition d'irréductibilité de cette forme telle qu'elle a été posée plus haut, de manière qu'aucun de ces coefficients ne puisse être supposé s'évanouir. N'ayant obtenu en effet qu'une limite de leur produit, dans le cas ou l'un d'eux serait nul, on ne pourrait plus rien conclure sur les autres. Maintennant et à l'aide des valeurs de ces quantités: $\{X^n\}$, $\{Y^n\}$ etc., nous obtiendrons des limites pour les coefficients des autres termes, en déduisant des équations (1.) et (2.), la suivante:

$$\{X^pY^q\ldots U^s\}\{X^n\}^{1-\frac{p}{n}}\{Y^n\}^{1-\frac{q}{n}}\cdots\{U^n\}^{1-\frac{s}{n}}$$
$$= [X^pY^q\ldots U^s][X^n]^{1-\frac{p}{n}}[Y^n]^{1-\frac{q}{n}}\cdots[U^n]^{1-\frac{s}{n}}\sqrt{(\sigma\sigma_1\ldots\sigma_{n-1})^n}$$

et remplaçant dans le second membre, $[X^nY^n\ldots U^n]$, $[X^n]$, $[Y^n]$ etc. et le produit $\sigma\sigma_1\ldots\sigma_{n-1}$ par leurs limites supérieures. Il vient ainsi en désignant par $(p, q, \ldots s)$ le coefficient de $X^pY^q\ldots U^s$ dans la puissance $(X+Y+\cdots+U)^n$:

$$\{X^pY^q\ldots U^s\}\{X^n\}^{1-\frac{p}{n}}\{Y^n\}^{1-\frac{q}{n}}\cdots\{U^n\}^{1-\frac{s}{n}} < (p,q,\ldots s)\frac{2^{\frac{1}{2}n^2(n-1)}}{n^{\frac{1}{2}n^2}}(\Delta\Delta_0)^{\frac{1}{2}n}.$$

Nous sommes ainsi parvenus à la proposition annoncée sur la réduction des formes décomposables en facteurs linéaires, et qui nous autorise à donner aux transformées telles que Φ, le nom de formes reduites. Mon théorème sur les racines des équations algébriques à coefficients entiers complexes, en est une conséquence immédiate comme Vous allez voir.

Soit: $Pv^n+Qv^{n-1}+\cdots+Rv+S=0$ une équation de cette nature. En désignant ses racines par $a, b, c \ldots k, l$ le discriminant, ou déterminant de *Gaufs*, sera le nombre entier complexe:

$$\mathfrak{D} = P^{2(n-1)}(a-b)^2(a-c)^2\cdots(k-l)^2$$

Cela posé, faisons dépendre de cette équation une forme φ à coefficients entiers complexes, que nous définirons de cette manière:

$$\varphi = P^{n-1}(x+ay+a^2z+\cdots+a^{n-1}u)(x+by+b^2z+\cdots+b^{n-1}u)\cdots$$
$$(x+ly+l^2z+\cdots+l^{n-1}u)$$

Nous remarquerons d'abord, que pour cette forme, la quantité $\varDelta$, est précisément $\sqrt{\mathfrak{D}}$. Soit en effet:

$$A = x+ay+\cdots+a^{n-1}u$$
$$B = x+by+\cdots+b^{n-1}u$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$L = x+ly+\cdots+l^{n-1}u,$$

d'aprés sa définition même, $\varDelta$ sera le produit de P^{n-1} multiplié par le déterminant relatif au système des facteurs linéaires $A, B, \ldots L$. Or on sait que ce déterminant, est la fonction alternée égale au produit des différences des racines $a, b, \ldots l$, de sorte qu'on a bien $\varDelta = \sqrt{\mathfrak{D}}$. Je dis maintenant que les racines de deux équations différentes, aux quelles correspondent des formes φ, arithmétiquement équivalentes, doivent être regardées comme présentant les mêmes irrationalités. Soit en effet:

$$\mathfrak{P}v^n+\mathfrak{Q}v^{n-1}+\cdots+\mathfrak{R}v+\mathfrak{S} = 0$$

et:

$$\Phi = \mathfrak{P}^{n-1}(X+\mathfrak{a}Y+\cdots+\mathfrak{a}^{n-1}U)(X+\mathfrak{b}Y+\cdots+\mathfrak{b}^{n-1}U)\cdots$$
$$(X+\mathfrak{l}Y+\cdots+\mathfrak{l}^{n-1}U)$$

une seconde équation, ayant pour racines $\mathfrak{a}, \mathfrak{b}, \ldots \mathfrak{l}$, avec la forme correspondante. S'il est possible de déduire Φ de φ, par une substitution à coefficients entiers complexes et au déterminant un, c. à d. d'avoir identiquement: $\varphi = \Phi$, en prenant

$$x = \alpha X+\alpha' Y+\cdots+\alpha^{(n-1)}U$$
$$y = \beta X+\beta' Y+\cdots+\beta^{(n-1)}U$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$u = \varkappa X+\varkappa' Y+\cdots+\varkappa^{(n-1)}U$$

on pourra en désignant par $t_1, t_2, \ldots t_n$ des constantes poser les relations:

$$x+ay+\cdots+a^{n-1}u = t_1(X+\mathfrak{a}Y+\cdots+\mathfrak{a}^{n-1}U)$$
$$x+by+\cdots+b^{n-1}u = t_2(X+\mathfrak{b}Y+\cdots+\mathfrak{b}^{n-1}U)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x+ly+\cdots+l^{n-1}u = t_n(X+\mathfrak{l}Y+\cdots+\mathfrak{l}^{n-1}U).$$

Or en effectuant la substitution et désignant pour abréger la fonction entière à coefficients entiers complexes $\alpha^{(i)}+\beta^{(i)}v+\cdots+\varkappa^{(i)}v^{n-1}$ par $\theta_i(v)$ ces relations donneront:

$$\begin{array}{lcl}
X\theta(a)+Y\theta_1(a)+\cdots+U\theta_{n-1}(a) & = & t_1(X+\mathfrak{a}Y+\cdots+\mathfrak{a}^{n-1}U) \\
X\theta(b)+Y\theta_1(b)+\cdots+U\theta_{n-1}(b) & = & t_2(X+\mathfrak{b}Y+\cdots+\mathfrak{b}^{n-1}U) \\
\cdots & & \cdots \\
X\theta(l)+Y\theta_1(l)+\cdots+U\theta_{n-1}(l) & = & t_n(X+\mathfrak{l}Y+\cdots+\mathfrak{l}^{n-1}U)
\end{array}$$

On en conclura les expressions suivantes des racines $\mathfrak{a}, \mathfrak{b}, \ldots \mathfrak{l}$ par $a, b, \ldots l$:

$$\begin{array}{llll}
\mathfrak{a}=\dfrac{\theta_1(a)}{\theta(a)} & \mathfrak{a}^2=\dfrac{\theta_2(a)}{\theta(a)} & \ldots & \mathfrak{a}^{n-1}=\dfrac{\theta_{n-1}(a)}{\theta(a)} \\
\mathfrak{b}=\dfrac{\theta_1(b)}{\theta(b)} & \mathfrak{b}^2=\dfrac{\theta_2(b)}{\theta(b)} & \ldots & \mathfrak{b}^{n-1}=\dfrac{\theta_{n-1}(b)}{\theta(b)} \\
\cdots & & & \\
\mathfrak{l}=\dfrac{\theta_1(l)}{\theta(l)} & \mathfrak{l}^2=\dfrac{\theta_2(l)}{\theta(l)} & \ldots & \mathfrak{l}^{n-1}=\dfrac{\theta_{n-1}(l)}{\theta(l)}
\end{array}$$

et il est visible qu'en partant de la substitution inverse, pour déduire φ de Φ, on arrivera à des expressions toutes semblables qui donneront les racines $a, b, \ldots l$, au moyen de $\mathfrak{a}, \mathfrak{b}, \ldots \mathfrak{l}$. Nous sommes donc bien autorisés par là à regarder les racines des deux équations, comme présentant les mêmes irrationalités.

Cela posé, considérons l'ensemble des équations de degré n, ayant même discriminant, avec la série des formes φ, qui correspondent à chacune d'elles. Ces formes en nombre infini, ayant toutes le même invariant $\Delta\Delta_0$, à savoir le module du discriminant, seront réductibles à un nombre limité de réduites Φ. Or les équations dont les racines pourront présenter des irrationalités distinctes seront celles là seules aux quelles correspondent des formes ayant des transformées réduites différentes.*) Elles seront donc bien essentiellement comme je l'ai annoncé, en nombre fini.

---

*) En effet, des formes ayant même réduite, sont arithmétiquement équivalentes, et il a été expliqué plus haut, comment les racines des équations dont elles dépendent offrent déslors les mêmes irrationalités. Voyez au reste sur cette question de l'équivalence des formes décomposables en facteurs linéaires, mon premier mémoire sur la théorie des formes quadratiques, Tome 47 de ce Journal.