MÉMOIRE

SUR LA

RÉDUCTION SIMULTANÉE D'UNE FORME QUADRATIQUE

ET

D'UNE FORME LINÉAIRE;

PAR M. H. POINCARÉ.

Dans un Mémoire précédent (1), j'ai étudié les questions relatives à la réduction et à l'équivalence des formes cubiques ternaires. J'ai appliqué, pour cela, à ces formes la méthode qui avait conduit M. Hermite à des résultats si intéressants, en ce qui concerne les formes quadratiques et les formes décomposables en facteurs linéaires; H étant une forme algébriquement équivalente à F et la plus simple parmi ces formes; T étant une substitution linéaire telle que la forme quadratique définie

$$(x^2+y^2+z^2)\,\mathrm{T}$$

soit réduite; j'appelle forme réduite la forme HT. On reconnaît aisément que, en général, toute forme est arithmétiquement équivalente à une ou à plusieurs réduites, et que deux formes données seront équivalentes, pourvu que le système des réduites de la première soit identique au système des réduites de la seconde.

Une pareille méthode est applicable à la forme la plus générale, quels

(1) *Journal de l'École Polytechnique,* LIe Cahier.

que soient son ordre et le nombre de ces variables. En ce qui concerne les formes cubiques ternaires, j'ai fait

$H = \alpha(x^3 + y^3 + z^3) + 6\beta xyz$	quand le discriminant n'est pas nul.
$H = \alpha(x^3 + y^3) + 6\beta xyz$ ou $H = \alpha x^3 + 3\alpha xy^2 + 3\beta x^2 z + 3\beta y^2 z$	quand le discriminant est nul et que de plus $S \lesseqgtr o$, $T \lesseqgtr o$ et que la forme est indécomposable.
$H = 3x^2 y + z^3$	quand $S = T = o$ sans que la forme soit indécomposable.
$H = \alpha z^3 + 6\beta xyz$ ou $H = \alpha z^3 + 3\beta x^2 z + 3\beta y^2 z$	quand $S \lesseqgtr o$, $T \lesseqgtr o$ et que la forme se décompose en un facteur quadratique et un facteur linéaire.
$H = \alpha 3x^2 y + 3zy^2$	quand $S = T = o$ et que la forme se décompose en un facteur quadratique et un facteurlinéaire.

Quand une forme cubique ternaire n'est pas décomposable en facteurs et que S et T ne sont pas nuls à la fois, cette forme ne peut dériver de H que par un nombre fini de transformations linéaires; pour constater l'équivalence de deux pareilles formes, il suffit par conséquent de calculer les coefficients d'un nombre fini de substitutions, et de constater si ces coefficients sont entiers. La considération des réduites n'est donc pas nécessaire et on se trouve en présence, non plus d'une question d'Arithmétique, mais d'une question d'Algèbre.

Constater si deux formes F et F′, qui sont indécomposables et où S et T sont nuls à la fois, sont arithmétiquement équivalentes, c'est encore une question d'Algèbre; constater si l'on peut trouver un coefficient constant α, tel que F et αF′ soient équivalentes, c'est au contraire une question d'Arithmétique, et j'ai fait voir, dans le Mémoire dont je parle, comment on pouvait la résoudre en comparant les deux réduites extrêmes de F et de F′. Mon intention n'est pas de revenir en ce moment sur ce point.

Si maintenant on passe à l'équivalence des formes décomposables en un facteur quadratique et un facteur linéaire, on se trouve en présence d'une véritable question d'Arithmétique, sur laquelle je veux insister un peu. J'ai fait voir qu'on rencontrait dans ce cas des chaînes indéfinies de

réduites se reproduisant périodiquement ainsi qu'il arrive pour les formes quadratiques binaires indéfinies.

Remarquons d'abord que le problème de l'équivalence de deux pareilles formes se ramène à celui de l'équivalence de deux systèmes comprenant chacun une forme quadratique et une forme linéaire. Soient en effet

$$f\varphi \quad \text{et} \quad f_1\varphi_1$$

les deux formes : nous supposons que f et f_1 sont linéaires, φ et φ_1 quadratiques. Pour que ces deux formes soient équivalentes, il faut et il suffit que les deux systèmes

$$\frac{1}{\lambda}f, \quad \lambda\varphi$$

et

$$\frac{1}{\mu}f_1, \quad \mu\varphi_1,$$

où λ et μ sont des constantes choisies de telle sorte que

$$\text{discriminant de } \lambda\varphi = \text{discriminant de } \mu\varphi_1$$

soient arithmétiquement équivalents.

L'étude des formes ternaires de cette sorte est donc ramenée à celle d'un pareil système. C'est ce qui m'a déterminé à entreprendre ce travail.

INVARIANTS DU SYSTÈME.

Je dis que le système d'une forme quadratique ternaire et d'une forme linéaire a deux invariants indépendants. En effet, soient

$$f(x, y, z) \quad \text{et} \quad \varphi(x, y, z)$$

les deux formes du système; on peut toujours poser

$$\varphi = \alpha f^2 + gh,$$

où g et h sont linéaires pendant que α est une constante. Soient maintenant

$$f_1(x_1, y_1, z_1) \quad \text{et} \quad \varphi_1(x_1, y_1, z_1)$$

un nouveau système analogue : on pourra poser

$$\varphi_1 = \alpha_1 f_1^2 + g_1 h_1.$$

Il est clair que, si

$$\alpha = \alpha_1,$$

on aura

$$\varphi = \varphi_1, \qquad f = f_1,$$

pourvu que l'on ait entre $x, y, z; x_1, y_1, z_1$ les relations linéaires

$$f = f_1,$$
$$g = g_1,$$
$$h = h_1;$$

c'est-à-dire que, si δ est le déterminant des coefficients des trois fonctions linéaires f, g, h; δ_1 le déterminant des coefficients de

$$f_1, g_1, h_1;$$

le système f_1, φ, dérivera du système f, φ, par une substitution de déterminant $\frac{\delta_1}{\delta}$.

Donc, pour que les deux systèmes soient algébriquement équivalents, il faut et il suffit que

$$\alpha = \alpha_1,$$
$$\delta = \delta_1,$$

c'est-à-dire qu'il y ait deux invariants indépendants.

Pour ces deux invariants, on peut prendre :

1° Soit le discriminant de φ et l'invariant S de la forme cubique $f\varphi$;

2° Soit le discriminant de φ et celui de $\varphi + mf^2$, m étant un entier quelconque.

RÉDUCTION DU SYSTÈME.

Voici la règle que, dans le Mémoire cité, j'avais adoptée pour la réduction d'un pareil système.

On peut toujours poser

$$\varphi = \alpha f^2 + gh,$$

α étant une constante, g et h des fonctions linéaires.

Je considérais alors la forme quadratique définie

$$f^2 + \lambda^2 g^2 + \frac{1}{\lambda^2} h^2,$$

où λ est un paramètre arbitraire, et la substitution linéaire T qui réduit cette forme. Le système

$$fT, \quad \varphi T$$

était alors le système réduit équivalent à

$$f, \quad \varphi.$$

Il est clair que, λ étant arbitraire, il peut y avoir dans chaque classe plusieurs systèmes réduits. Mais je montrais que, si les coefficients de f et de φ sont entiers, ces systèmes sont toujours en nombre fini.

Je crois qu'il y a avantage à modifier un peu cette règle.

Si, en effet, g et h sont réels, on a

$$gh = k^2 - l^2,$$

en posant

$$k = \frac{g+h}{2}, \qquad l = \frac{g-h}{2},$$

et par conséquent

$$\varphi = \alpha f^2 + k^2 - l^2.$$

On aura de même

$$\varphi = \alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 - \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2,$$

où λ est arbitraire.

Supposons que α soit positif; on considérera la forme quadratique définie

$$\alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 + \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2,$$

et la substitution T qui la réduit.

Le système

$$\varphi T, \quad f T$$

sera le système réduit de φ, f.

Si, au contraire, α est négatif, on envisagera la forme quadratique définie

$$-\alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 + \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2$$

et la substitution T qui la réduit.

$\varphi T, f T$ sera encore le système réduit de φ, f.

Supposons maintenant que g et h soient imaginaires conjugués.

On pourra, d'une infinité de manières, décomposer gh en une somme de deux carrés.

Soit

$$gh = k^2 + l^2;$$

on envisagera la forme

$$\begin{aligned} &\alpha f^2 + k^2 + l^2 && \text{si } \alpha > 0, \\ &-\alpha f^2 + k^2 + l^2 && \text{si } \alpha < 0, \end{aligned}$$

ainsi que la substitution T qui la réduit.

$\varphi T, f T$ sera le système réduit de φ, f.

Voici quels avantages présente ce mode nouveau de réduction :

On sait que, si l'on envisage une forme quadratique indéfinie ternaire, cette forme peut s'écrire

$$X^2 + Y^2 - Z^2 \quad \text{ou} \quad X^2 - Y^2 - Z^2,$$

où X, Y, Z sont linéaires, et que les formes équivalentes

$$(X^2 + Y^2 - Z^2)T \quad \text{ou} \quad (X^2 - Y^2 - Z^2)T$$

sont dites réduites si la forme quadratique définie

$$(X^2 + Y^2 + Z^2)T$$

est elle-même réduite.

Cela posé, il est clair que, d'après le nouveau mode de réduction, $\varphi' T$ sera une réduite de φ quand $\varphi T, f' T$ sera un système réduit du système φ, f et, par conséquent, la nouvelle règle de réduction est plus avantageuse au point de vue des applications de la théorie qui nous occupe aux questions les plus générales relatives aux formes quadratiques indéfinies.

Soit

$$\varphi = Ax^2 + A'y^2 + A''z^2 + 2Byz + 2B'xz + 2B''xy,$$

$$f = \lambda x + \mu y + \nu z.$$

Soit φ_1 la forme adjointe de φ.

Soient a, b, c des quantités définies par les équations

$$\varphi'_x(a, b, c) = 2\lambda,$$

$$\varphi'_y(a, b, c) = 2\mu,$$

$$\varphi'_z(a, b, c) = 2\nu,$$

les quantités a, b, c seront commensurables.

Cela posé, on sait que la forme

$$\tfrac{1}{4}(a\varphi'_x + b\varphi'_y + c\varphi'_z)^2 - \varphi(a, b, c)\,\varphi(x, y, z)$$

a pour discriminant o et est, par conséquent, décomposable en deux facteurs linéaires.

De plus,

$$\tfrac{1}{2}(a\varphi'_x + b\varphi'_y + c\varphi'_z) = f.$$

On a donc

$$\varphi = \alpha f'^2 + g l,$$

où

$$\alpha = \frac{1}{\varphi(a, b, c)}.$$

Si l'on pose

$$ay - bx = z_1, \qquad cx - az = y_1, \qquad bz - cy = x_1,$$

on aura évidemment

$$ax_1 + by_1 + cz_1 = 0, \tag{2}$$

et, d'autre part, on trouve, par un calcul facile,

$$\tfrac{1}{4}(a\varphi'_x + b\varphi'_y + c\varphi'_z) - \varphi(a, b, c)\,\varphi(x, y, z) = \varphi_1(x_1, y_1, z_1).$$

On a donc

$$\varphi = \frac{1}{\varphi(a, b, c)} f'^2 + \frac{1}{\varphi(a, b, c)}\,\varphi_1(x_1, y_1, z_1).$$

Quant à $\varphi_1(x_1, y_1, z_1)$, on peut le ramener à une forme binaire à l'aide de l'identité (2) qui donne

$$\varphi_1\left(x_1, y_1, -\frac{ax_1 + by_1}{c}\right),$$

et rien n'est plus facile ensuite que de décomposer φ_1 en deux facteurs linéaires, ou bien encore de le décomposer en une somme de deux carrés ou en une différence de deux carrés.

Premier cas.

$\frac{1}{\varphi(a, b, c)} > 0$, et φ_1 se décompose en une somme de deux carrés positifs.

La forme φ est alors quadratique définie et n'a, par conséquent, en général, qu'une réduite.

Le système f, φ ne peut alors se réduire que d'une seule manière, à savoir par la substitution qui réduit φ.

Deuxième cas.

$\frac{1}{\varphi(a, b, c)} < 0$, et φ_1 se décompose en une somme de deux carrés positifs.

La substitution, qui réduit le système f, φ, est celle qui réduit la forme

$$-\varphi(x, y, z)$$

qui est quadratique définie positive.

Le système f, φ n'a donc, en général, qu'un système réduit.

Troisième cas.

φ_1 se décompose en une somme de deux carrés négatifs.

Supposons, pour fixer les idées,

$$\alpha = \frac{1}{\varphi(a, b, c)} > 0.$$

Comme on a

$$\varphi = \alpha f^2 + \alpha\varphi_1,$$

on aura

$$\varphi = \alpha f^2 - \alpha k^2 - \alpha l^2,$$

k et l étant deux fonctions linéaires, et, par définition, la substitution qui réduit le système f, φ sera celle qui réduit la forme quadratique positive

$$\alpha f^2 + \alpha k^2 + \alpha l^2.$$

Ici encore le système f, φ n'a, en général, qu'un système réduit.

Quatrième cas.

φ_1 se décompose en une différence de deux carrés, c'est-à-dire en un produit de deux fonctions linéaires réelles; ces fonctions linéaires ont des coefficients commensurables entre eux.

Dans le Mémoire cité, j'ai fait voir que, dans ce cas :

1° L'invariant $4S$ est une puissance quatrième parfaite;

2° Les systèmes réduits forment une chaîne limitée à ses deux extrémités, et, pour s'assurer de l'équivalence de deux systèmes, il suffit de constater l'identité des systèmes réduits extrêmes.

Ces résultats, démontrés pour l'ancien mode de réduction, subsistent encore pour le nouveau mode.

Cinquième cas.

φ_1 est décomposable en une différence de deux carrés ou en un produit de deux fonctions linéaires réelles dont les coefficients sont incommensurables entre eux.

J'ai fait voir que l'invariant $4S$ n'est pas puissance quatrième parfaite, et que les systèmes réduits forment une chaîne indéfinie où ils se reproduisent périodiquement, ainsi qu'il arrive pour les réduites des formes quadratiques binaires indéfinies.

Ces résultats subsistent encore avec le mode nouveau de réduction.

Ils permettent de définir des transformations semblables du système f, φ en lui-même.

Sixième cas.

φ_1 est un carré parfait.

Dans ce cas,

$$\varphi(a, b, c) = 0,$$

d'où

$$\alpha = \infty .$$

On ne peut donc plus poser

$$\varphi = \alpha f^2 + \alpha\varphi_1 ;$$

mais on pourra toujours poser, et cela d'une infinité de manières,

$$\varphi = fg + h^2,$$

g et h étant des fonctions linéaires de x, y, z.

Dans ce cas, la forme $f \times \varphi$, qui est cubique ternaire, est de la sixième famille (*voir* le Mémoire cité), et ses invariants S et T sont nuls.

Nous dirons que le système f, φ est réduit par la substitution qui réduit

$$\frac{1}{\lambda^2}\frac{f^2}{2} + \lambda^2\frac{g^2}{2} + h^2.$$

Si fT, φT est le système réduit de f, φ; φT sera l'une des réduites de φ définie à la façon ordinaire; or φ n'a qu'un nombre fini de réduites; donc le système f, φ n'aura qu'un nombre fini de systèmes réduits.

Ces systèmes formeront, non pas une chaîne, mais un réseau analogue à celui que l'on rencontre dans l'étude des réduites d'une forme quadratique ternaire indéfinie, mais moins compliqué.

Je n'ai rien à ajouter sur les trois premiers cas où le problème est ramené, comme on l'a vu, à la réduction d'une forme quadratique ternaire définie; mais je crois qu'il y a lieu de faire des trois derniers cas une étude plus approfondie.

ÉTUDE SPÉCIALE DU QUATRIÈME CAS.

Je suppose que l'on ait mis la forme φ par le procédé indiqué plus haut sous la forme

$$\alpha f^2 + gh.$$

Je suppose que α soit une constante positive et que g et h soient deux fonctions linéaires dont les coefficients soient commensurables entre eux. Le système

$$f\mathrm{T}, \quad \varphi\mathrm{T},$$

sera réduit, si la forme

$$\psi = \left(\alpha f^2 + \lambda^2\frac{g^2}{2} + \frac{1}{\lambda^2}\frac{h^2}{2}\right)\mathrm{T}$$

est réduite elle-même.

Nous dirons, avec MM. Korkine et Zolotareff, que la forme ψ est ré-

duite si elle peut se mettre sous la forme

$$\psi = \mu_1 (x + \varepsilon_1 y + \zeta_1 z)^2 + \mu_2 (y + \zeta_2 z)^2 + \mu_3 z^2,$$

où ε_1, ζ_1 et ζ_2 sont plus petits que $\frac{1}{2}$ en valeur absolue, et où μ_1 est le minimum absolu de la forme ψ et où μ_2 est le minimum absolu de la forme

$$\mu_2 (y + \zeta_2 z)^2 + \mu_3 z^2.$$

Il est clair que, si l'on fait varier λ depuis o jusqu'à l'infini, on trouvera pour les coefficients de Γ différentes valeurs qui donneront différents systèmes réduits du système f, φ. Mais nous nous bornerons à considérer les systèmes réduits qu'on obtient pour λ très grand et pour λ très petit.

Supposons donc λ très grand. Soit

$f = lx + my + nz$, l, m, n étant entiers premiers entre eux,

$g = \gamma(l_1 x + m_1 y + n_1 z)$, l_1, m_1, n_1 » »

$h = \delta(l_2 x + m_2 y + n_2 z)$, l_2, m_2, n_2 » »

Soient

$$lm_1 - ml_1 = \mathrm{DN},$$
$$mn_1 - nm_1 = \mathrm{DL},$$
$$nl_1 - ln_1 = \mathrm{DM},$$

D étant entier et L, M, N étant entiers premiers entre eux.

Je dis que le minimum absolu de la forme

$$\theta = \alpha f^2 + \lambda^2 \frac{g^2}{2} + \frac{1}{\lambda^2} \frac{h^2}{2}$$

s'obtient si λ est assez grand pour

$$x = \mathrm{L}, \qquad y = \mathrm{M}, \qquad z = \mathrm{N}.$$

En effet, on a toujours

$$\alpha f^2 > \text{ou} = \alpha,$$

à moins que

$$lx + my + nz = 0,$$

$$\lambda^2 \frac{\varepsilon^2}{2} > \text{ ou } = \lambda^2 \frac{\gamma^2}{2},$$

à moins que

$$l_1 x + m_1 y + n_1 z = 0.$$

Soit

$$\delta(l_2 \mathrm{L} + m_2 \mathrm{M} + n_2 \mathrm{N}) = \Delta,$$

et supposons que λ soit assez grand pour que

$$\alpha > \frac{1}{\lambda^2} \frac{\Delta^2}{2}$$

et

$$\lambda^2 \frac{\gamma^2}{2} > \frac{1}{\lambda^2} \frac{\Delta^2}{2}.$$

Pour

$$x = \mathrm{L}, \qquad y = \mathrm{M}, \qquad z = \mathrm{N},$$

on a

$$\theta = \frac{1}{\lambda^2} \frac{\Delta^2}{2}.$$

Si x, y, z sont entiers sans que

$$lx + my + nz = 0,$$

on a

$$\theta \geq \alpha > \frac{1}{\lambda^2} \frac{\Delta^2}{2}.$$

Si x, y, z sont entiers sans que

$$l_1 x + m_1 y + n_1 z = 0,$$

on a

$$\theta \geq \lambda^2 \frac{\gamma^2}{2} > \frac{\lambda^2}{1} \frac{\Delta^2}{2}.$$

Si x, y, z sont entiers sans être égaux à L, M, N et si l'on a

$$lx + my + nz = l_1 x + m_1 y + n_1 z = 0,$$

on aura

$$x = t\mathrm{L}, \qquad y = t\mathrm{M}, \qquad z = t\mathrm{N},$$

où t est entier et plus grand que 1.

On aura donc

$$\theta = t^2 \frac{1}{\lambda^2} \frac{\Delta^2}{2} > \frac{1}{\lambda^2} \frac{\Delta^2}{2}.$$

Donc le minimum absolu de θ s'obtient pour

$$x = \mathrm{L}, \qquad y = \mathrm{M}, \qquad z = \mathrm{N}. \qquad \text{C. Q. F. D.}$$

Poursuivons la réduction de θ.

Soient $\mathrm{L}_1, \mathrm{M}_1, \mathrm{N}_1$; $\mathrm{L}_2, \mathrm{M}_2, \mathrm{N}_2$ six nombres entiers tels que

$$(3) \qquad \begin{vmatrix} \mathrm{L} & \mathrm{L}_1 & \mathrm{L}_2 \\ \mathrm{M} & \mathrm{M}_1 & \mathrm{M}_2 \\ \mathrm{N} & \mathrm{N}_1 & \mathrm{N}_2 \end{vmatrix} = 1.$$

Posons

$$x = \mathrm{L}\xi + \mathrm{L}_1\eta + \mathrm{L}_2\zeta,$$
$$y = \mathrm{M}\xi + \mathrm{M}_1\eta + \mathrm{M}_2\zeta,$$
$$z = \mathrm{N}\xi + \mathrm{N}_1\eta + \mathrm{N}_2\zeta,$$

et appelons T, la transformation

$$\begin{vmatrix} \mathrm{L} & \mathrm{L}_1 & \mathrm{L}_2 \\ \mathrm{M} & \mathrm{M}_1 & \mathrm{M}_2 \\ \mathrm{N} & \mathrm{N}_1 & \mathrm{N}_2 \end{vmatrix};$$

on aura

$$\theta\mathrm{T}_1 = \frac{1}{\lambda^2}\frac{h^2}{2} + \alpha \left[(l\,\mathrm{L}_1 + m\,\mathrm{M}_1 + n\,\mathrm{N}_1)\eta + (l\,\mathrm{L}_2 + m\,\mathrm{M}_2 + n\,\mathrm{N}_2)\zeta\right]^2$$
$$+ \frac{\lambda^2\gamma^2}{2}\left[(l_1\mathrm{L}_1 + m_1\mathrm{M}_1 + n_1\mathrm{N}_1)\eta + (l_1\mathrm{L}_2 + m_1\mathrm{M}_2 + n_1\mathrm{N}_2)\zeta\right]^2.$$

Les deux derniers carrés ne contiennent plus que η et ζ; ils forment

donc une forme binaire. Réduisons cette forme binaire et pour cela cherchons son minimum absolu.

Soient

$$l_1 L_1 + m_1 M_1 + n_1 N_1 = \quad Q,$$
$$l_1 L_2 + m_1 M_2 + n_1 N_2 = -P.$$

Je dis que les nombres P et Q sont premiers entre eux ; en effet, puisque

$$l_1 L + m_1 M + n_1 N = 0,$$

et que le déterminant (3) est égal à 1, le plus grand commun diviseur de P et de Q diviserait l_1, m_1, n_1 qui sont premiers entre eux.

Je dis que le minimum de la forme binaire

$$\alpha[(lL_1 + mM_1 + nN_1)\eta + (lL_2 + mM_2 + nN_2)\zeta]^2 + \frac{\lambda^2\gamma^2}{2}(Q\eta - P\zeta)^2 = \theta$$

s'obtient si λ est suffisamment grand, pour

$$\eta = P, \qquad \zeta = Q.$$

Je dis que

$$(lL_1 + mM_1 + nN_1)P + (lL_2 + mM_2 + nN_2)Q = \pm D,$$

car un calcul très simple montre que cette expression est égale au déterminant

$$D\begin{vmatrix} L & M & N \\ L_1 & M_1 & N_1 \\ L_2 & M_2 & N_2 \end{vmatrix} = \begin{vmatrix} nm_1 - mn_1 & ln_1 - nl_1 & ml_1 - lm_1 \\ L_1 & M_1 & N_1 \\ L_2 & M_2 & N_2 \end{vmatrix},$$

ou à ce déterminant changé de signe.

Donc, pour

$$\eta = P, \qquad \zeta = Q,$$

on a

$$\theta_1 = \alpha D^2.$$

Supposons que λ soit assez grand pour que

$$\frac{\lambda^2\gamma^2}{2} > \alpha D^2.$$

Si l'on n'a pas

$$Q\eta - P\zeta = 0;$$

on a

$$Q\eta - P\zeta \geq 1,$$

puisque η et ζ, P et Q sont entiers et par conséquent

$$\theta_1 \geq \frac{\lambda^2\gamma^2}{2} > \alpha D^2.$$

Si l'on a

$$Q\eta - P\zeta = 0,$$

sans avoir

$$\eta = P, \qquad \zeta = Q,$$

on a

$$\eta = Pt, \qquad \zeta = Qt,$$

t étant un entier plus grand que 1 et, par conséquent,

$$\theta_1 = \alpha t^2 D^2 > \alpha D^2.$$

Donc αD^2 est le minimum absolu de θ_1 et, si l'on pose

$$\eta = P\eta_1 + P_1\zeta_1,$$
$$\zeta = Q\eta_1 + Q_1\zeta_1,$$

où P_1 et Q_1 sont tels que

$$PQ_1 - P_1Q = 1,$$

si l'on appelle T_2 la substitution

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & P & P_1 \\ 0 & Q & Q_1 \end{vmatrix},$$

la forme $\theta T_1 T_2$ pourra s'écrire

$$\mu_1(\xi + \varepsilon_1\eta_1 + \varepsilon'_1\zeta_1)^2 + \mu_2(\eta_1 + \varepsilon_2\zeta_1)^2 + \mu_3\zeta_1^2,$$

où μ_1 est le miuimum absolu de la forme ternaire pendant que μ_2 est le minimum absolu de la forme binaire

$$\mu_2(\eta_1 + \varepsilon_2\zeta_1)^2 + \mu_3\zeta_1^2.$$

Posons

$$\begin{aligned} \xi_1 &= \xi_2 + \delta_1\eta_1 + \delta'_1\zeta_2, \\ \eta_1 &= \eta_2 + \delta_2\zeta_2, \\ \zeta_1 &= \zeta_2, \end{aligned}$$

où δ_1, δ'_1, δ_2 sont des nombres entiers déterminés, de telle façon que

$$\begin{aligned} -\tfrac{1}{2} < \delta_2 + \varepsilon_2 < \tfrac{1}{2}, \\ -\tfrac{1}{2} < \delta'_1 + \varepsilon_1\delta_2 + \varepsilon'_1 < \tfrac{1}{2}, \\ -\tfrac{1}{2} < \delta_1 + \varepsilon_1 < \tfrac{1}{2}, \end{aligned}$$

ce qui est toujours possible ; appelons T_3 la substitution

$$\begin{vmatrix} 1 & \delta_1 & \delta'_1 \\ 0 & 1 & \delta_2 \\ 0 & 0 & 1 \end{vmatrix}.$$

Il est clair que la forme quadratique définie

$$\theta T_1 T_2 T_3$$

sera réduite, et que, par conséquent, le système réduit cherché sera

$$\varphi T_1 T_2 T_3, \quad f T_1 T_2 T_3.$$

On peut simplifier ce calcul. Supposons, en effet, que la substitution

$$T_1 T_2 T_3$$

équivaille à la suivante

$$\begin{aligned} l_1 x + m_1 y + n_1 z &= \mathrm{H}_1 \zeta_2, \\ lx + my + nz &= \mathrm{H}\eta_2 + \varepsilon_1 \zeta_2, \\ l_2 x + m_2 y + n_2 z &= \mathrm{H}_2 \xi_2 + \varepsilon_1 \eta_2 + \varepsilon'_1 \zeta_2, \end{aligned}$$

il est clair que l'on devra avoir

$$\mathrm{H}_1 = 1, \qquad \mathrm{H} = \mathrm{D}, \qquad \mathrm{H}_2 = \frac{\Delta}{\delta},$$

et, pour que les coefficients de la substitution soient entiers, il faut et il suffit que l'on ait

$$l - \varepsilon_2 l_1 \equiv m - \varepsilon_2 m_1 \equiv n - \varepsilon_2 n_1 \equiv 0 \pmod{\mathrm{D}}$$

et

$$\left.\begin{aligned} l_2 - \frac{\varepsilon_1}{\mathrm{D}} l + \left(\frac{\varepsilon_1 \varepsilon_2}{\mathrm{D}} - \varepsilon'_1\right) l_1 &\equiv m_2 - \frac{\varepsilon_1}{\mathrm{D}} m + \left(\frac{\varepsilon_1 \varepsilon_2}{\mathrm{D}} - \varepsilon'_1\right) m_1 \\ &\equiv n_2 - \frac{\varepsilon_1}{\mathrm{D}} n + \left(\frac{\varepsilon_1 \varepsilon_2}{\mathrm{D}} - \varepsilon'_1\right) n_1 \equiv 0 \end{aligned}\right\} \left(\mathrm{mod}\,\frac{\Delta}{\delta}\right).$$

Je dis que les trois premières congruences peuvent toujours être résolues.

Les trois nombres l_1, m_1, n_1 étant premiers entre eux, on pourra toujours trouver trois nombres λ_1, μ_1, ν_1, tels que

$$l_1 \lambda_1 + m_1 \mu_1 + n_1 \nu_1 = 1.$$

Les trois congruences donnent alors

$$\varepsilon_2 \equiv l\lambda_1 + m\mu_1 + n\nu_1 \pmod{\mathrm{D}}.$$

On trouvera aisément un nombre ε_2 satisfaisant à cette condition, ainsi qu'aux inégalités

$$-\frac{\mathrm{D}}{2} < \varepsilon_2 < \frac{\mathrm{D}}{2}.$$

Je dis que ce nombre satisfera aux trois congruences

$$l - \varepsilon_2 l_1 \equiv m - \varepsilon_2 m_1 \equiv n - \varepsilon_2 n_1 \equiv 0 \pmod{\mathrm{D}}.$$

On a, en effet,

$$l - \varepsilon_2 l_1 \equiv l - (l\lambda_1 + m\mu_1 + n\nu_1) l_1 \pmod{D}$$

ou

$$l - \varepsilon_2 l_1 \equiv l - l(l_1\lambda_1 + m_1\mu_1 + n_1\nu_1) + \mu_1(ml_1 - lm_1) + \nu_1(nl_1 - ln_1)$$

ou

$$l - \varepsilon_2 l_1 \equiv l - l - \mu_1 DN + \nu_1 DM \equiv 0 \pmod{D}.$$

Soit donc

$$l - \varepsilon_2 l_1 = l_3 D, \qquad m - \varepsilon_2 m_1 = m_3 D, \qquad n - \varepsilon_2 n_1 = n_3 D.$$

Je dis que les nombres l_3, m_3, n_3 sont premiers entre eux ; en effet, leur plus grand commun diviseur devrait diviser L, M, N, qui sont premiers entre eux.

Les trois dernières congruences deviennent

$$(4) \qquad \left\{ \begin{array}{l} l_2 - \varepsilon_1 l_3 - \varepsilon'_1 l_1 \equiv m_2 - \varepsilon_1 m_3 - \varepsilon'_1 m_1 \\ \qquad\qquad \equiv n_2 - \varepsilon_1 n_3 - \varepsilon'_1 n_1 \equiv 0 \end{array} \right\} \left(\mathrm{mod}\,\frac{\Delta}{\delta}\right).$$

On pourra toujours trouver trois nombres λ_3, μ_3, ν_3 satisfaisant aux conditions

$$\lambda_3 l_1 + \mu_3 m_1 + \nu_3 n_1 = 0,$$
$$\lambda_3 l_3 + \mu_3 m_3 + \nu_3 n_3 = 1,$$

d'où

$$\lambda_3 l + \mu_3 m + \nu_3 n = D.$$

Les trois congruences (4) donnent alors

$$(5) \qquad (\lambda_3 l_2 + \mu_3 m_2 + \nu_3 n_2) \equiv \varepsilon_2,$$

$$(6) \quad (\lambda_1 l_2 + \mu_1 m_2 + \nu_1 n_2) - \varepsilon_1(\lambda_1 l_3 + \mu_1 m_3 + \nu_1 n_3) \equiv \varepsilon'_1 \quad \left(\mathrm{mod}\,\frac{\Delta}{\delta}\right).$$

La congruence (5) donnera ε_1, et la congruence (6) ε'_1 ; on aura soin de choisir ces deux nombres de telle façon que leur valeur absolue soit plus petite que la moitié de $\frac{\Delta}{\delta}$.

Cela posé, le système réduit s'écrira

$$\alpha(D\eta_2+\varepsilon_2\zeta_2)^2+\gamma\delta\left(\frac{\Delta}{\delta}\xi_2+\varepsilon_1\eta_2+\varepsilon'_1\zeta_2\right)\zeta_2,$$

$$D\eta_2+\varepsilon_2\zeta_2.$$

Les calculs de réduction du système se partagent donc en trois parties :

1° Calcul de α, γ, δ, l, m, n, l_1, m_1, n_1, l_2, m_2, n_2, Δ, D, où l'on se borne à des opérations purement algébriques et à des recherches de plus grand commun diviseur;

2° Calcul de λ_1, μ_1, ν_1, λ_3, μ_3, ν_3, où l'on a à résoudre des congruences linéaires très simples ;

3° Calcul de ε_2, ε_1, ε'_1, où l'on n'a qu'à chercher les restes de trois divisions de nombres entiers.

Dans tout ce qui précède, nous avons supposé que α était positif et que l, m, n étaient premiers entre eux.

Si α était négatif, on changerait le signe de φ.

Si l, m, n avaient un plus grand commun diviseur D, on poserait

$$f=f'D,$$

d'où

$$\varphi=\alpha D^2f'^2+gh,$$

et de toutes façons on serait ramené au cas que nous avons étudié.

Remarque. — Les considérations qui précèdent montrent suffisamment qu'un pareil système n'est reproduit par aucune substitution linéaire.

Exemple. — Soit à réduire le système

$$\varphi=x^2+y^2-4z^2,$$

$$f=x+3y-2z.$$

Ici l'on a

$$l=1,\qquad m=3,\qquad n=-2;$$

d'où

$$a=1,\qquad b=6,\qquad c=1.$$

On trouve aisément

$$9\varphi - f^2 = +(x - 2z)(8x - 6y + 20z);$$

d'où

$$\alpha = \tfrac{1}{9}, \qquad \gamma\delta = \tfrac{2}{9};$$

$$l_1 = 1, \qquad m_1 = 0, \qquad n_1 = -2,$$

$$l_2 = 4, \qquad m_2 = -3, \qquad n_2 = 10;$$

$$L = -2, \qquad M = 0, \qquad N = -1, \qquad D = 3;$$

$$\frac{\Delta}{\delta} = -18.$$

La transformation $T_1 T_2 T_3$ s'écrira alors

$$\begin{aligned} l_1 x + m_1 y + n_1 z &= \zeta_2, \\ lx + my + nz &= 3\eta_2 + \varepsilon_2 \zeta_2, \\ l_2 x + m_2 y + n_2 z &= -18\xi_2 + \varepsilon_1 \eta_2 + \varepsilon_1' \zeta_2; \end{aligned}$$

ε_2 sera déterminé par les trois congruences

$$\left.\begin{aligned} l - \varepsilon_2 l_1 &= 1 - \varepsilon_2 \equiv 0 \\ m - \varepsilon_2 m_1 &= 3 \equiv 0 \\ n - \varepsilon_2 n_1 &= -2 + 2\varepsilon_2 \equiv 0 \end{aligned}\right\} \pmod 3.$$

Il n'est pas besoin ici de chercher les nombres λ_1, μ_1, ν_1, pour voir que ces congruences se réduisent à

$$\varepsilon_2 \equiv 1 \pmod 3,$$

ou

$$\varepsilon_2 = 1.$$

Quant à l_3, m_3, n_3, on trouve immédiatement

$$l_3 = 0, \qquad m_3 = 1, \qquad n_3 = 0,$$

d'où les trois congruences

$$\left.\begin{aligned} 4 - \quad \varepsilon_1 &\equiv 0 \\ -3 - \quad \varepsilon'_1 &\equiv 0 \\ 10 + 2\varepsilon'_1 &\equiv 0 \end{aligned}\right\} \pmod{18},$$

d'où

$$\varepsilon'_1 = 4, \qquad \varepsilon_1 = -3.$$

Le système réduit cherché est alors

$$\alpha(D\eta_2 + \varepsilon_2\zeta_2)^2 + \gamma\delta\zeta_2\left(\frac{\Delta}{\delta}\xi_2 + \varepsilon_1\eta_2 + \varepsilon'_1\zeta_2\right)$$

$$D\eta_2 + \varepsilon_2\zeta_2,$$

c'est-à-dire

$$\tfrac{1}{9}(3\eta_2 + \zeta_2)^2 + \tfrac{2}{9}\zeta_2(-18\xi_2 + 3\eta_2 + 4\zeta_2)$$

$$3\eta_2 + \zeta_2,$$

ou, revenant aux variables x, y, z, c'est-à-dire changeant ξ_2 en x, η_2 en y, ζ_2 en z,

$$-4xz + y^2 + z^2$$

$$3y + z;$$

on trouverait de même le système réduit extrême qui correspond aux valeurs très petites du paramètre arbitraire λ et l'on arriverait au résultat suivant :

Pour que deux systèmes se composant chacun d'une fonction linéaire et d'une forme quadratique, ayant mêmes invariants et rentrant tous deux dans le quatrième cas, soient arithmétiquement équivalents, il faut et il suffit que les deux systèmes réduits extrêmes de l'un (trouvés comme il a été dit plus haut, l'un pour les valeurs très petites de λ, l'autre pour les valeurs très grandes de ce paramètre) soient identiques aux deux systèmes réduits extrêmes de l'autre.

ÉTUDE SPÉCIALE DU CINQUIÈME CAS.

Supposons que φ se mette sous la forme

$$af^2 + gh,$$

où g et h sont des fonctions linéaires dont les coefficients sont réels, mais non commensurables entre eux.

Pour réduire le système f, φ, on cherche la transformation qui réduit la forme définie

$$\alpha f^2 + \frac{\lambda^2}{2} g^2 + \frac{1}{2\lambda^2} h^2 = \theta; \tag{6}$$

et pour cela il faut d'abord chercher le minimum absolu de cette forme.

Je dis que, quels que soient λ, g, h, et f, on peut toujours choisir α assez petit pour que ce minimum absolu s'obtienne en faisant

$$g = h = 0$$

ou bien, si

$$a = \lambda_1 \delta, \qquad b = \mu_1 \delta, \qquad c = \nu_1 \delta$$

(où λ_1, μ_1, ν_1 sont des entiers premiers entre eux), en faisant

$$x = \lambda_1, \qquad y = \mu_1, \qquad z = \nu.$$

Si en effet

$$f = lx + my + nz,$$

$$l\lambda_1 + m\mu_1 + n\nu_1 = \Delta, \quad l\lambda_2 + m\mu_2 + n\nu_2 = \Delta_2, \quad l\lambda_3 + m\mu_3 + n\nu_3 = \Delta_3,$$

la valeur de la forme (6) pour

$$x = \lambda_1, \qquad y = \mu_1, \qquad z = \nu_1$$

sera

$$\alpha \Delta^2.$$

Supposons maintenant que le plus grand commun diviseur des coefficients de gh soit E. Le produit gh ne peut devenir nul pour des valeurs

entières de g et de h que si g et h s'annulent à la fois, et si cela n'a pas lieu, il est au moins égal à E.

Donnons donc à x, y, z des valeurs entières différentes de λ_1, μ_1 et ν_1; si g et h ne s'annulent pas à la fois, on aura

$$\theta > \frac{\lambda^2}{2} g^2 + \frac{1}{2\lambda^2} h^2 > gh > \mathrm{E}.$$

Si g et h s'annulent à la fois, on aura

$$x = \lambda_1 t, \qquad y = \mu_1 t, \qquad z = \nu_1 t,$$

où t est entier et > 2, d'où

$$\theta = \alpha \Delta^2 t^2 > \alpha \Delta^2.$$

Si donc α est assez petit pour que

$$\alpha \Delta^2 < \mathrm{E},$$

le minimum de θ sera $\alpha \Delta^2$.

Cela posé, prenons un système f, φ quelconques; il pourra se présenter deux cas :

Premier cas.

$$\alpha \Delta^2 < \mathrm{E}.$$

Dans ce cas le minimum de θ se trouve immédiatement, ainsi qu'on vient de le voir.

Deuxième cas.

$$\alpha \Delta^2 > \mathrm{E} \quad \text{ou} \quad = \mathrm{E}.$$

Dans ce cas on remarquera que l'on peut remplacer le système donné f, φ par le système

$$f, \ \varphi + \mu f^2,$$

où μ est un nombre quelconque.

En effet :

1° Pour que deux systèmes f, φ et f_1, φ_1, soient équivalents, il faut et il suffit que les deux systèmes

$$f,\ \varphi + \mu f^2 \quad \text{et} \quad f_1,\ \varphi_1 + \mu f_1^2$$

soient équivalents.

2° Les transformations linéaires que reproduisent le système f, φ sont les mêmes que celles qui reproduisent le système, f et $\varphi + \mu f^2$; de sorte que, au double point de vue de l'équivalence des systèmes et des transformations semblables, il est indifférent d'envisager le système f, φ ou bien le système f et $\varphi + \mu f^2$.

On choisira alors μ de telle sorte que

$$(\alpha + \mu)\Delta^2 < \mathrm{E},$$

et l'on sera ramené au premier cas.

Revenons donc au premier cas :

Le minimum absolu de θ s'obtient pour

$$x = \lambda_1, \qquad y = \mu_1, \qquad z = \nu_1.$$

Soient donc λ_2, μ_2, ν_2, λ_3, μ_3, ν_3 six entiers tels que

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix} = 1.$$

Posons

$$\begin{aligned} x &= \lambda_1 \xi + \lambda_2 \eta + \lambda_3 \zeta, \\ y &= \mu_1 \xi + \mu_2 \eta + \mu_3 \zeta, \\ z &= \nu_1 \xi + \nu_2 \eta + \nu_3 \zeta, \end{aligned}$$

et appelons T_1 cette transformation linéaire.

On aura

$$\theta\,\mathrm{T}_1 = \alpha\left[\Delta\xi + (\lambda_2 l + \mu_2 m + \nu_2 n)\eta + (\lambda_3 l + \mu_3 m + \nu_3 n)\zeta^3\right] + \left(\frac{\lambda^2}{2} g^2 + \frac{1}{\lambda^2} a^2\right)\mathrm{T}_1$$

et

$$\varphi T_1 = \alpha\left[\Delta\xi + (\lambda_2 l + \mu_2 m + \nu_2 n)\eta + (\lambda_3 l + \mu_3 m + \nu_3 n)\zeta\right]^2 + gh'T_1.$$

Les formes

$$\left(\frac{\lambda^2}{2}g^2 + \frac{1}{\lambda^2}h^2\right)T_1 \quad \text{et} \quad ghT_1$$

ne contiennent que η et ζ et sont par conséquent binaires.

Pour achever la réduction, il faut :

1° Chercher une transformation T_2 de la forme

$$\begin{aligned}\xi &= \xi_1 + k_0\eta_1 + k'_0\zeta_1,\\ \eta &= \quad k_1\eta_1 + k'_1\zeta_1,\\ \zeta &= \quad k_2\eta_1 + k'_2\zeta_1,\end{aligned}$$

telle que la forme

$$\left(\frac{\lambda^2}{2}g^2 + \frac{1}{\lambda^2}h^2\right)T_1T_2,$$

soit réduite, et que

$$\begin{aligned}-\frac{\Delta}{2} < \Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0 < \frac{\Delta}{2},\\ -\frac{\Delta}{2} < \Delta_2 k'_1 + \Delta_3 k'_2 + \Delta k'_0 < \frac{\Delta}{2},\end{aligned}$$

ce qui est toujours possible;

2° Appliquer cette transformation T_2 au système

$$fT_1, \quad \varphi T_1.$$

Cherchons donc la substitution T_2.

Pour calculer k_0, il suffit de chercher un nombre entier qui soit égal à

$$-\frac{\Delta_2 k_1 + \Delta_3 k_2}{\Delta}$$

à $\pm\frac{1}{2}$ près. On calculerait de même k'_0.

Il reste à calculer les quatre coefficients

$$\begin{vmatrix} k_1 & k'_1 \\ k_2 & k'_2 \end{vmatrix},$$

qui forment une substitution linéaire binaire entre η, ζ et η_1, ζ_1; cette substitution, nous l'appellerons τ.

Elle doit être telle que la forme binaire définie

$$\left(\frac{\lambda^2}{2} g^2 + \frac{1}{\lambda^2} h^2\right) \Gamma_1 \tau$$

soit réduite, c'est-à-dire que la forme binaire indéfinie

$$gh\Gamma_1\tau$$

soit réduite.

Le problème de la réduction du système f, φ est donc ramené à celui de la réduction de la forme binaire

$$gh\Gamma_1,$$

et l'on trouve

système réduit du système f, φ

$= $ le système formé de $\Delta\xi_1 + (\Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0)\eta_1$

$+ (\Delta_2 k'_1 + \Delta_3 k'_2 + \Delta k'_0)\zeta_1$ et de $\alpha[\Delta\xi_1 + (\Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0)\eta_1$

$+ (\Delta_2 k'_1 + \Delta_3 k'_2 + \Delta k'_0)\zeta_1]^2$

$+$ réduite de $gh\Gamma_1$.

CALCUL DE $g.h.\Gamma$.

Le calcul de α, de λ_1, μ_1, ν_1, λ_2, μ_2, ν_2, λ_3, μ_3, ν_3, k_0, k'_0 ne présentant pas de difficulté, je passe immédiatement au calcul des coefficients de la forme binaire $gh\Gamma$.

Soient

$$\varphi = Ax^2 + A'y^2 + A''z^2 + 2Byz + 2B'xz + 2B''xy$$

et

$$\varphi_1 = \text{forme adjointe de } \varphi,$$
$$\varphi_1 = A_1 x^2 + A'_1 y^2 + A''_1 z^2 + 2B_1 yz + 2B'_1 xz + 2B''_1 xy;$$

d'où

$$A_1 = A'A'' - B^2, \qquad A'_1 = AA'' - B'^2, \qquad A''_1 = AA' - B''^2,$$
$$B_1 = B'B'' - AB, \qquad B'_1 = B''B - A'B', \qquad B''_1 = BB' - A''B''.$$

On sait que nous avons défini a, b, c par les conditions

$$\varphi'_x(a, b, c) = 2l,$$
$$\varphi'_y(a, b, c) = 2m,$$
$$\varphi'_z(a, b, c) = 2n;$$

on en tire aisément, pour les valeurs de a, b, c, les expressions suivantes, en appelant H le discriminant de φ,

$$aH = A_1 l + B''_1 m + B'_1 n,$$
$$bH = B''_1 l + A'_1 m + B_1 n,$$
$$cH = B'_1 l + B_1 m + A''_1 n.$$

Si δ_1 est le plus grand commun diviseur de aH, bH et cH, on aura

$$\lambda_1 = \frac{aH}{\delta_1}, \qquad \mu_1 = \frac{bH}{\delta_1}, \qquad \nu_1 = \frac{cH}{\delta_1},$$

et les valeurs de λ_2, μ_2, ν_2, λ_3, μ_3, ν_3 s'en déduiront aisément.

On sait que la forme

$$(lx + my + nz)^2 - \varphi(x, y, z)\,\varphi(a, b, c)$$

se décompose en deux facteurs linéaires et est égale à

$$-gh\,\varphi(a, b, c).$$

Or, d'autre part, cette forme s'écrit

$$\begin{aligned}&A_1(bz-cy)^2+A_1'(cx+az)^2+A_1''(ay+bx)^2\\&\qquad+2B(ay-bz)(cx-az)\\&\qquad+2B'(ay-bx)(bz-cy)+2B''(bz-cy)(cx-az),\end{aligned}$$

ainsi qu'on l'a vu plus haut, ou bien

$$\varphi_1[(bz-cy),(cx-az),(ay-bx)];$$

d'où l'on tire

$$\begin{aligned}gh&=-\frac{\varphi_1[(bz-cy),(cx-az),(ay-bx)]}{\varphi(a,b,c)}\\&=-\frac{\varphi_1[(\mu_1 z-\nu_1 y),(\nu_1 x-\lambda_1 z),(\lambda_1 y-\mu_1 x)]}{\varphi(\lambda_1,\mu_1,\nu_1)}.\end{aligned}$$

Une première remarque importante, c'est que

$$\varphi(\lambda_1,\mu_1,\nu_1)=\frac{\varphi_1(l,m,n)H}{\delta_1^2}.$$

Posons donc

$$-\frac{1}{\varphi(\lambda_1,\mu_1,\nu_1)}=\gamma.$$

Considérons la transformation

$$T_1=\begin{vmatrix}\lambda_1&\lambda_2&\lambda_3\\ \mu_1&\mu_2&\mu_3\\ \nu_1&\nu_2&\nu_3\end{vmatrix},$$

et appelons L_1, M_1, N_1 les mineurs qui correspondent à λ_1, μ_1, ν_1, de telle sorte que

$$\begin{aligned}\lambda_1L_1+\mu_1M_1+\nu_1N_1&=1,\\ \lambda_2L_1+\mu_2M_1+\nu_2N_1&=0,\\ \lambda_3L_1+\mu_3M_1+\nu_3N_1&=0.\end{aligned}$$

Appelons de même L_2, M_2, N_2; L_3, M_3, N_3 les mineurs, tels que

$$\lambda_1 L_2 + \mu_1 M_2 + \nu_1 N_2 = 0, \qquad \lambda_1 L_3 + \mu_1 M_3 + \nu_1 N_3 = 0,$$
$$\lambda_2 L_2 + \mu_2 M_2 + \nu_2 N_2 = 1, \qquad \lambda_2 L_3 + \mu_2 M_3 + \nu_2 N_3 = 0,$$
$$\lambda_3 L_2 + \mu_3 M_2 + \nu_3 N_2 = 0, \qquad \lambda_3 L_3 + \mu_3 M_3 + \nu_3 N_3 = 1.$$

On aura évidemment

$$\mu_1 z - \nu_1 y = L_3 \eta_1 - L_2 \zeta,$$
$$\nu_1 x - \lambda_1 z = M_3 \eta_1 - M_2 \zeta,$$
$$\lambda_1 y - \mu_1 x = N_3 \eta_1 - N_2 \zeta;$$

d'où

$$gh T_1 = \gamma \varphi_1 [(L_3 \eta_1 - L_2 \zeta), (M_3 \eta_1 - M_2 \zeta), (N_3 \eta_1 - N_2 \zeta)].$$

Supposons que

$$gh T_1 = P \eta_1^2 + 2 Q \eta_1 \zeta + R \zeta^2,$$

il viendra

$$P = \gamma \varphi_1 (L_3, M_3, N_3),$$
$$R = \gamma \varphi_1 (L_2, M_2, N_2),$$
$$2Q = \gamma [L_3 \varphi'_{1x}(L_2, M_2, N_2) + M_3 \varphi'_{1y}(L_2, M_2, N_2) + N_3 \varphi'_{1z}(L_2, M_2, N_2)].$$

CALCUL DU DISCRIMINANT $Q^2 - RP$.

On a

$$\frac{1}{\gamma^2}(Q^2 - RP) = \frac{1}{4}(L_3 \varphi'_{1x} + M_3 \varphi'_{1y} + N_3 \varphi'_{1z})^2 - \varphi_1 (L_3, M_3, N_3) \varphi_1 (L_2, M_2, N_2).$$

Remarquons que l'on a identiquement

$$\text{forme adjointe de } \varphi_1 = \varphi H.$$

On a donc, d'après une remarque déjà faite,

$$\frac{1}{\gamma^2}(Q^2 - RP) = H \varphi [(N_3 M_2 - N_2 M_3), (L_3 N_2 - L_2 N_3), (M_3 L_2 - M_2 L_3)]$$

ou

$$\frac{1}{\gamma^2}(Q^2 - RP) = H\varphi(\lambda_1, \mu_1, \nu_1) = \frac{H^2}{\delta_1^2}\varphi_1(l, m, n)$$

ou enfin

$$Q^2 - RP = -\gamma H = \frac{\delta_1^2}{G}$$

si $\varphi_1(l, m, n) = G$.

Calculons maintenant le plus grand commun diviseur de P, Q, R. Si E est le plus grand commun diviseur des trois nombres entiers

$$\varphi_1(L_3, M_3, N_3), \quad \varphi_1(L_2, M_2, N_2),$$
$$\tfrac{1}{2}\left[L_2\varphi'_{1x}(L_3, M_3, N_3) + M_2\varphi'_{1y}(L_3, M_3, N_3) + N_2\varphi'_{1z}(L_3, M_3, N_3)\right],$$

γE sera le plus grand commun diviseur de P, Q, R, de sorte que le déterminant de la forme primitive ψ de laquelle ghT_1 est dérivée s'écrira

$$\frac{-H}{\gamma E^2} = \frac{H^2 G}{\delta_1^2 E^2}.$$

Ce déterminant doit être un nombre entier.

Une fois les coefficients de ghT_1 connus, les procédés ordinaires de réduction des formes binaires donnent immédiatement les coefficients de la substitution τ, ce qui permet d'achever complètement la réduction du système.

TRANSFORMATIONS SEMBLABLES.

L'un des problèmes les plus intéressants que permet de résoudre la réduction des formes ou des systèmes de formes est la recherche des substitutions semblables.

Soit f, φ un système de formes quelconques, algébriquement équivalent à un système canonique quelconque F, Φ, de telle sorte que

$$f = F\tau, \qquad \varphi = \Phi\tau.$$

Dans certains cas, les seuls qui soient intéressants au point de vue arithmé-

tique, on pourra trouver une infinité de substitutions τ qui permettent de passer du système F, Φ au système f, φ; supposons donc qu'on ait à la fois

$$f = \mathrm{F}\tau_1, \qquad \varphi = \Phi\tau_1,$$
$$f = \mathrm{F}\tau_2, \qquad \varphi = \Phi\tau_2.$$

Soient T_1 et T_2 deux substitutions à coefficients entiers, telles que les formes quadratiques définies

$$(x^2+y^2+z^2)\,\tau_1\mathrm{T}_1,$$
$$(x^2+y^2+z^2)\,\tau_2\mathrm{T}_2$$

soient réduites; les systèmes

$$f\mathrm{T}_1, \quad \varphi\mathrm{T}_1,$$
$$f\mathrm{T}_2, \quad \varphi\mathrm{T}_2$$

seront par définition des systèmes réduits du système f, φ.

Si ces deux systèmes sont identiques, de telle sorte que

$$f\mathrm{T}_1 = f\mathrm{T}_2, \qquad \varphi\mathrm{T}_1 = \varphi\mathrm{T}_2,$$

il est clair que

$$f\mathrm{T}_1\mathrm{T}_2^{-1} = f, \qquad \varphi\mathrm{T}_1\mathrm{T}_2^{-1} = \varphi,$$

de telle sorte que

$$\mathrm{T}_1\mathrm{T}_2^{-1}$$

sera une substitution semblable du système f, φ.

Si donc, dans la réduction successive d'un système, on rencontre deux systèmes réduits identiques, on pourra en déduire une substitution semblable.

Je dis que, réciproquement, on obtiendra ainsi toutes les substitutions semblables. En effet, soit S une pareille substitution; on a, par hypothèse,

$$f\mathrm{S} = f, \qquad \varphi\mathrm{S} = \varphi.$$

Soit

$$f = \mathrm{F}\tau_1, \qquad \varphi = \Phi\tau_1$$

et

$$\text{forme } (x^2 + y^2 + z^2)\,\tau, \mathrm{T}_1 = \text{réduite},$$

de telle sorte que $f\mathrm{T}_1$, $\varphi\mathrm{T}_1$ soit un système réduit de f, φ.

On aura évidemment

$$f = \mathrm{F}\tau_1\mathrm{S}, \qquad \varphi = \Phi\tau_1\mathrm{S};$$

la forme

$$(x^2 + y^2 + z^2)\,\tau_1\mathrm{S}.\mathrm{S}^{-1}\mathrm{T}_1$$

sera réduite, et, par conséquent, le système

$$f\mathrm{S}^{-1}\mathrm{T}_1, \quad \varphi\mathrm{S}^{-1}\mathrm{T}_1$$

sera réduit. De plus, il est clair qu'il sera identique à $f\mathrm{T}_1$, $\varphi\mathrm{T}_1$, c'est-à-dire que la substitution S pourra s'obtenir par le procédé exposé plus haut.

Appliquons donc ce procédé au cas qui nous occupe. Soient

$$f\mathrm{T}_2, \quad \varphi\mathrm{T}_2,$$
$$f\mathrm{T}_3, \quad \varphi\mathrm{T}_3$$

deux systèmes réduits de f, φ. Le premier de ces systèmes réduits s'écrira, en conservant les anciennes notations,

$$\Delta\xi_1 + (\Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0)\,\tau_{12} + (\Delta_2 k'_1 + \Delta_3 k'_2 + \Delta k'_0)\,\zeta_1$$

et

$$[\Delta\xi_1 + (\Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0)\,\tau_{12} + (\Delta_2 k'_1 + \Delta_3 k'_2 + \Delta k'_0)\,\zeta_1]^2 + gh\mathrm{T}_1\tau,$$

$gh\mathrm{T}_1\tau$ étant une des réduites de $gh\mathrm{T}_1$; le second s'écrirait d'une façon analogue

$$\Delta\xi_2 + (\Delta_2 k''_1 + \Delta_3 k''_2 + \Delta k''_0)\,\tau_{12} + (\Delta_2 k'''_1 + \Delta_3 k'''_2 + \Delta k'''_0)\,\zeta_2$$

et

$$[\Delta\xi_2 + (\Delta_2 k''_1 + \Delta_3 k''_2 + \Delta k''_0)\,\tau_{12} + (\Delta_2 k'''_1 + \Delta_3 k'''_2 + \Delta k'''_0)\,\zeta_2]^2 + gh\mathrm{T}_1\tau\tau_1,$$

$gh\mathrm{T}_1\tau\tau_1$ étant une autre réduite de $gh\mathrm{T}_1$, telle que la substitution s'écrive

$$\eta_1 = k_1''\eta_2 + k_1'''\zeta_2,$$
$$\zeta = k_2''\eta_2 + k_2'''\zeta_2.$$

Pour que ces deux systèmes réduits soient identiques, il faut et il suffit que

$$(gh)\,\mathrm{T}_1\tau = (gh)\,\mathrm{T}_1\tau\tau_1,$$
$$\Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0 = \Delta_2 k_1'' + \Delta_3 k_2'' + \Delta k_0'',$$
$$\Delta_2 k_1' + \Delta_3 k_2' + \Delta k_0' = \Delta_2 k_1''' + \Delta_3 k_2''' + \Delta k_0''';$$

d'où

$$\left.\begin{aligned}\Delta_2 k_1 + \Delta_3 k_2 &\equiv \Delta_2 k_1'' + \Delta_3 k_2''\\ \Delta_2 k_1' + \Delta_3 k_2' &\equiv \Delta_2 k_1''' + \Delta_3 k_2'''\end{aligned}\right\} \pmod{\Delta}.$$

Cherchons d'abord les substitutions qui reproduisent $(gh)\,\mathrm{T}_1\tau$.

$(gh)\,\mathrm{T}_1\tau$ est une forme binaire indéfinie; supposons qu'elle soit égale à un coefficient constant multiplié par une forme primitive

$$\psi = p\eta_1^2 + 2q\eta_1\zeta_1 + r\zeta_1^2.$$

Il est clair que la forme ψ, et par conséquent la forme $(gh)\,\mathrm{T}_1\tau$, sera reproduite par la substitution

$$\eta_1 = (t - qu)\,\eta_2 - ru\zeta_2,$$
$$\zeta_1 = pu\eta_2 + (t + qu)\,\zeta_2,$$

où t et u sont des entiers satisfaisant à

$$t^2 - (q^2 - rp)\,u^2 = 1,$$

si la forme ψ est proprement primitive, et où $2t$ et $2u$ sont des entiers satisfaisant à

$$4t^2 - 4\,(q^2 - rp)\,u^2 = 4,$$

si la forme ψ est improprement primitive.

Si l'on applique cette substitution à

$$(\Delta_2 k_1 + \Delta_3 k_2)\,\tau_1 + (\Delta_2 k'_1 + \Delta_3 k'_2)\,\zeta_1,$$

il vient

$$\begin{aligned}&[(\Delta_2 k_1 + \Delta_3 k_2)\,(t - qu) + (\Delta_2 k'_1 + \Delta_3 k'_2)\,pu]\,\tau_2\\ &+ [(\Delta_2 k'_1 + \Delta_3 k''_2)\,(t + qu) - (\Delta_2 k_1 + \Delta_3 k_2)\,ru]\,\zeta_2;\end{aligned}$$

d'où

$$\left.\begin{aligned}(\Delta_2 k_1 + \Delta_3 k_2)\,(t - qu) + (\Delta_2 k'_1 + \Delta_3 k'_2)\,pu &\equiv \Delta_2 k''_1 + \Delta_3 k''_2\\ (\Delta_2 k'_1 + \Delta_3 k''_2)\,(t + qu) - (\Delta_2 k_1 + \Delta_3 k_2)\,ru &\equiv \Delta_2 k'''_1 + \Delta_3 k'''_2\end{aligned}\right\} \pmod{\Delta}$$

ou, posant

$$\Delta_2 k_1 + \Delta_3 k_2 = v, \qquad \Delta_2 k'_1 + \Delta_3 k'_2 = w,$$

on doit avoir

$$\left.\begin{aligned}vt + u\,(pw - qv) &\equiv v\\ wt + u\,(qw - rv) &\equiv w\end{aligned}\right\} \pmod{\Delta}.$$

Soit ρ le plus grand commun diviseur de v, w et Δ; soit σ celui de v et de w. Ces deux congruences pourront être remplacées par les suivantes :

$$\left.\begin{aligned}\frac{v}{\sigma}(t - qu) + \frac{w}{\sigma}\,pu &\equiv \frac{v}{\sigma}\\ \frac{v}{\sigma}\,ru + \frac{w}{\sigma}\,(t + qu) &\equiv \frac{w}{\sigma}\end{aligned}\right\} \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

Multiplions la première par ru, la seconde par $t - qu$ et ajoutons; multiplions de même la première par $t + qu$, la seconde par $-pu$, et ajoutons. En remarquant que

$$t^2 - (q^2 - rp)\,u^2 = 1,$$

nous aurons

$$\left.\begin{aligned}\frac{v}{\sigma}\,ru + \frac{w}{\sigma}\,(t - qu) &\equiv \frac{w}{\sigma}\\ \frac{v}{\sigma}(t + qu) - \frac{w}{\sigma}\,pu &\equiv \frac{v}{\sigma}\end{aligned}\right\} \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right),$$

d'où

$$2u\frac{rv-qw}{\sigma}\equiv 2u\frac{qv-pw}{\sigma}\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

Soit θ le plus grand commun diviseur de

$$\frac{rv-qw}{\sigma}, \quad \frac{qv-pw}{\sigma} \quad \text{et} \quad \frac{\Delta}{\rho}.$$

Ces deux congruences se réduiront à

$$2u\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho\theta}\right).$$

Premier cas.

La forme $px^2+2qxy+ry^2$ est proprement primitive; $\frac{\Delta}{\rho\theta}$ est impair, u et t doivent être entiers. Dans ce cas les congruences se réduisent à

$$u\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho\theta}\right),$$

d'où

$$u\frac{rv-qw}{\sigma}\equiv u\frac{qv-pw}{\sigma}\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right),$$

$$\left.\begin{aligned} t\frac{w}{\sigma}&\equiv\frac{w}{\sigma}\\ t\frac{v}{\sigma}&\equiv\frac{v}{\sigma}\end{aligned}\right\}\left(\mathrm{mod}\,\frac{\Delta}{\rho}\right)$$

ou

$$t\equiv 1 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

Deuxième cas.

La forme $px^2+2qxy+ry^2$ est proprement primitive; $\frac{\Delta}{\rho\theta}$ est pair.

Dans ce cas, u et t doivent être entiers, et l'on doit avoir

$$u\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{2\rho\theta}\right);$$

d'où

$$u\frac{rv-qw}{\sigma}\equiv u\frac{qv-pw}{\sigma}\equiv 0 \pmod{\frac{\Delta}{2\rho}}$$

et

$$t\equiv 1 \pmod{\frac{\Delta}{2\rho}}.$$

De plus

$$\frac{2\rho}{\Delta}(t-1)\frac{w}{\sigma} \quad \text{et} \quad \frac{2\rho\theta}{\Delta}u\frac{rv-qw}{\sigma\theta}$$

et, d'autre part,

$$\frac{2\rho}{\Delta}(t-1)\frac{v}{\sigma} \quad \text{et} \quad \frac{2\rho\theta}{\Delta}u\frac{qv-pw}{\sigma\theta}$$

doivent être de même parité.

Or $\frac{v}{\sigma}$ et $\frac{w}{\sigma}$ ne peuvent être pairs tous deux ; de même $\frac{rv-qw}{\sigma\theta}$ et $\frac{qv-pw}{\sigma\theta}$ ne peuvent être pairs tous deux.

Cela posé, il peut se présenter deux cas :

1° $\frac{w}{\sigma}$ et $\frac{rv-qw}{\sigma\theta}$

et, d'autre part,

$$\frac{v}{\sigma} \quad \text{et} \quad \frac{qv-pv}{\sigma\theta}$$

sont de même parité, et alors les congruences se réduisent à

$$t-1\equiv u\theta\equiv 0 \pmod{\frac{\Delta}{2\rho}}, \qquad t-1\equiv u\theta \pmod{\frac{\Delta}{\rho}};$$

2° Ou bien les nombres

$$\frac{w}{\sigma} \quad \text{et} \quad \frac{rv-qw}{\sigma\theta},$$

ou les nombres

$$\frac{v}{\sigma} \quad \text{et} \quad \frac{qv-pv}{\sigma\theta}$$

ne sont pas de même parité, et alors les congruences se réduisent à

$$t-1\equiv u\theta\equiv 0 \pmod{\frac{\Delta}{\rho}}.$$

Troisième cas.

La forme $px^2 + 2qxy + ry^2$ est improprement primitive. Dans ce cas, $2u$ et $2t$ sont entiers, et l'on trouve immédiatement

$$2u\theta \equiv 2(t-1) \equiv 0 \pmod{\frac{\Delta}{\rho}},$$

$$\theta \equiv 1 \pmod 2, \qquad q^2 - rp \equiv 1 \pmod 2.$$

Mais cela n'est pas suffisant, il faut encore que les parités de $2u$ et de $2t$ satisfassent à certaines conditions.

D'abord $2u$ et $2t$ doivent être de même parité; car

$$4t^2 - 4(q^2 - rp)u^2 = 4 \equiv 0 \pmod 2;$$

d'où

$$4t^2 \equiv 4u^2 \quad \text{et} \quad 2t \equiv 2u.$$

Deux cas à considérer :

1° Si $\frac{\Delta}{\rho}$ est pair, $2u$ et $2t$ doivent être pairs, à cause des congruences

$$2u\theta \equiv 2(t-1) \equiv 0 \pmod{\frac{\Delta}{\rho}},$$

et ces congruences se réduisent à

$$u\theta \equiv t - 1 \equiv 0 \pmod{\frac{\Delta}{2\rho}}.$$

Envisageons maintenant les congruences

$$(\zeta) \qquad \left\{ \begin{array}{l} \frac{v}{\sigma}(t-1) + u\theta\frac{pw - qv}{\sigma\jmath} \equiv 0 \\ \frac{w}{\sigma}(t-1) + u\theta\frac{qw - rv}{\sigma\theta} \equiv 0 \end{array} \right\} \pmod{\frac{\Delta}{\rho}}.$$

Puisque

$$p \equiv r \equiv 0 \pmod 2, \qquad q \equiv 1 \pmod 2,$$

$$\frac{v}{\sigma} \equiv \frac{pw - qv}{\sigma\theta}, \qquad \frac{w}{\sigma} \equiv \frac{qw - rv}{\sigma\jmath} \pmod 2.$$

Posons donc

$$t - 1 = \frac{\Delta}{2\rho}\tau, \qquad u\theta = \frac{\Delta}{2\rho}\upsilon,$$

ces congruences se réduiront à

$$\frac{\nu}{\sigma}(\tau + \upsilon) \equiv \frac{w}{\sigma}(\tau + \upsilon) \equiv 0 \pmod 2$$

ou, puisque $\frac{\nu}{\sigma}$ et $\frac{w}{\sigma}$ sont premiers entre eux,

$$\tau \equiv \upsilon \pmod 2$$

ou

$$t - 1 \equiv u\theta \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

2° Si $\frac{\Delta}{\rho}$ est impair, $2t$ et $2u$ peuvent être pairs ou impairs, et par conséquent t et u peuvent être entiers ou fractionnaires.

Les congruences

$$2u\theta \equiv 2(t-1) \equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right)$$

équivalent aux suivantes

$$\left.\begin{aligned} 2(t-1)\frac{\nu}{\sigma} + 2u\theta\,\frac{pw - q\nu}{\sigma\theta} &\equiv 0 \\ 2(t-1)\frac{w}{\sigma} + 2u\theta\,\frac{qw - r\nu}{\sigma\theta} &\equiv 0 \end{aligned}\right\} \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right),$$

lesquelles équivalent aux congruences (ζ), pourvu que les nombres

$$(t-1)\frac{\nu}{\sigma} + u\theta\,\frac{pw - q\nu}{\sigma\theta},$$

$$(t-1)\frac{w}{\sigma} + u\theta\,\frac{qw - r\nu}{\sigma\vartheta}$$

soient entiers, ce qui exige que

$$2(t-1)\frac{\nu}{\sigma} + 2u\theta\,\frac{pw - q\nu}{\sigma\vartheta} \equiv 0,$$

$$2(t-1)\frac{\nu}{\sigma} + 2u\theta\,\frac{qw - r\nu}{\sigma\vartheta} \equiv 0 \pmod 2,$$

ou

$$\frac{\nu}{\sigma}\left[2(t-1)+2u\theta\right]\equiv\frac{\omega}{\sigma}\left[2(t-1)+2u\theta\right]\equiv 0 \pmod 2$$

ou

$$2(t-1)\equiv 2u\theta \pmod 2.$$

Résumons-nous. Le problème des transformations semblables se ramène au calcul de nombres t et u satisfaisant à certaines conditions. Cinq cas peuvent se présenter, puisque le deuxième et le troisième cas se subdivisent. Soit

$$q^2 - rp = \Omega.$$

Premier cas.

t et u sont entiers :

$$t^2 - \Omega u^2 = 1, \qquad u\equiv 0 \pmod{\frac{\Delta}{\rho\theta}}, \qquad t\equiv 1 \pmod{\frac{\Delta}{\rho}}.$$

Deuxième cas.

t et u sont entiers :

$$t^2 - \Omega u^2 = 1, \qquad t-1\equiv u\theta\equiv 0 \pmod{\frac{\Delta}{2\rho}},$$

$$t-1\equiv u\theta \pmod{\frac{\Delta}{\rho}}.$$

Troisième cas.

t et u sont entiers :

$$t^2 - \Omega u^2 = 1, \qquad t-1\equiv u\theta\equiv 0 \pmod{\frac{\Delta}{\rho}}.$$

Quatrième cas.

t et u sont entiers :

$$t^2 - \Omega u^2 = 1, \qquad t-1\equiv u\theta\equiv 0 \pmod{\frac{\Delta}{2\rho}},$$

$$t-1\equiv u\theta \pmod{\frac{\Delta}{\rho}}.$$

Cinquième cas.

$2t$ et $2u$ sont entiers et de même parité :

$$4t^2 - 4\Omega u^2 = 4, \qquad 2(t-1) \equiv 2u\theta \equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

Nous allons maintenant discuter ces conditions.

Considérons les nombres complexes de la forme

$$a + b\sqrt{\Omega}.$$

On sait que les nombres entiers de cette forme, qui satisfont à la condition

$$a^2 - b^2\Omega = 1,$$

sont les puissances d'un certain nombre entier complexe

$$a_1 + b_1\sqrt{\Omega}.$$

Dans le cas particulier où Ω est impair, il peut arriver aussi qu'un nombre complexe fractionnaire

$$\frac{c + d\sqrt{\Omega}}{2},$$

où c et d sont entiers, mais impairs, satisfasse à la condition

$$c^2 + d^2\Omega = 4.$$

Dans ce cas, tous les nombres complexes entiers de la forme $a + b\sqrt{\omega}$, ou fractionnaires de la forme $\frac{c + d\sqrt{\Omega}}{2}$, sont les puissances d'un même nombre fractionnaire

$$\frac{c_1 + d_1\sqrt{\Omega}}{2}.$$

Nous retrouvons, en passant, une remarque déjà faite autrefois par Eisentein. Je dis qu'en supposant que ce nombre $\frac{c_1 + d_1\sqrt{\Omega}}{2}$ existe, il est la

racine cubique de $a_1 + b_1\sqrt{\Omega}$. En effet, $a_1 + b_1\sqrt{\Omega}$ est une puissance de $\frac{c_1 + d_1\sqrt{\Omega}}{2}$, et c'est la plus petite de ses puissances qui soit un entier complexe.

Or, puisque $\frac{r_1 + d_1\sqrt{\Omega}}{2}$ est fractionnaire et que

$$c_1^2 - d_1^2\Omega = 4, \qquad \Omega \equiv 1 \pmod 2,$$

on aura

$$c_1 \equiv d_1 \equiv 1 \pmod 2.$$

De plus

$$\left(\frac{c_1 + d_1\sqrt{\Omega}}{2}\right)^2 = \frac{c_1^2 + d_1^2\Omega}{4} + \frac{c_1 d_1}{2}\sqrt{\Omega};$$

or

$$c_1 d_1 \equiv 1 \pmod 2;$$

donc la deuxième puissance est fractionnaire.

Au contraire,

$$\left(\frac{c_1 + d_1\sqrt{\Omega}}{2}\right)^3 = \frac{c_1^3 + 3c_1 d_1^2\Omega}{8} + \frac{3c_1^2 d_1 + d_1^3\Omega}{8}\sqrt{\Omega};$$

cette valeur se simplifie à cause de

$$c_1^2 = 4 + d_1^2\Omega,$$

ce qui donne

$$\frac{c_1(1 + d_1^2\Omega)}{2} + \frac{d_1(3 + d_1^2\Omega)}{2}\sqrt{\Omega}.$$

Or il est clair que

$$1 + d_1^2\Omega \equiv 3 + d_1^2\Omega \equiv 0 \pmod 2;$$

donc la troisième puissance est entière. Donc elle est égale à $a_1 + b_1\sqrt{\Omega}$.

C. Q. F. D.

Cette remarque permettra toujours de reconnaître si le nombre $\frac{c_1 + d_1\sqrt{\Omega}}{2}$ existe.

En résumé, les nombres t et u seront tels que le nombre complexe

$$t + u\sqrt{\Omega}$$

soit une puissance suivant les cas de

$$a_1 + b_1\sqrt{\Omega} \quad \text{ou de} \quad \frac{c_1 + d_1\sqrt{\Omega}}{2}.$$

Nous allons voir comment la théorie des congruences complexes permet de trouver toutes celles de ces puissances qui remplissent les autres conditions auxquelles sont assujettis les nombres t et u.

DES CONGRUENCES COMPLEXES.

Nous dirons que deux nombres complexes $a + b\sqrt{\Omega}$ et $c + d\sqrt{\Omega}$ sont congrus, par rapport au double module $\alpha + \beta\sqrt{\Omega}$ et $\gamma + \delta\sqrt{\Omega}$, et nous écrirons

$$a + b\sqrt{\Omega} \equiv c + d\sqrt{\Omega} \quad \left[\mathrm{mod}\left(\alpha + \beta\sqrt{\Omega}, \gamma + \delta\sqrt{\Omega}\right)\right]$$

quand on aura

$$a = c + \alpha m + \gamma n,$$
$$b = d + \beta m + \delta n,$$

m et n étant des entiers.

Si l'on représente le nombre complexe $a + b\sqrt{\Omega}$ par un point dont les coordonnées sont a et b, si l'on divise le plan en parallélogrammes ayant pour sommets

$$\alpha m + \gamma n, \quad \beta m + \delta n,$$

à des nombres congrus correspondront des points correspondants de ce réseau parallélogrammatique.

Représentons ce réseau par la notation

$$\begin{vmatrix} \alpha & \gamma \\ \beta & \delta \end{vmatrix},$$

de manière à pouvoir écrire

$$a + b\sqrt{\Omega} \equiv c + d\sqrt{\Omega} \quad \left(\mathrm{mod}\left|\begin{array}{cc}\alpha & \gamma\\ \beta & \delta\end{array}\right|\right),$$

ce réseau peut être remplacé par un réseau équivalent, et, parmi les réseaux équivalents, il y en a toujours un plus simple que les autres et qui est de la forme

$$\left|\begin{array}{cc}\alpha & \gamma\\ \beta & 0\end{array}\right| \quad (0 < \alpha < \gamma)$$

[*voir* mon Mémoire *Sur un mode nouveau de représentation des formes quadratiques définies ou indéfinies* (XLVII^{e} Cahier du *Journal de l'École Polytechnique*)].

Par rapport à un réseau quelconque, les nombres entiers complexes se répartissent en un nombre fini de classes.

Deux congruences complexes peuvent toujours être additionnées si elles ont lieu par rapport au même réseau.

Si une congruence complexe a lieu par rapport à deux réseaux différents, elle a lieu par rapport à leur plus petit commun multiple.

Telles sont les ressemblances des congruences complexes et des congruences ordinaires; voici une différence importante : une congruence complexe ne pourra pas toujours être multipliée par un nombre entier complexe. Il faut, pour cela, que le réseau qui sert de module soit un nombre complexe idéal.

De même, pour que l'on puisse diviser une congruence complexe par un nombre entier complexe, il faut et il suffit que le module soit un nombre complexe idéal et soit premier avec le nombre entier complexe par lequel on veut diviser la congruence.

Pour toutes ces propositions, je renvoie au Mémoire cité plus haut.

Donc, en résumé, si le module est un nombre complexe idéal, le calcul des congruences complexes est le même que celui des congruences ordinaires.

Rappelons enfin les conditions pour qu'un réseau

$$\begin{vmatrix} \alpha & \gamma \\ \beta & 0 \end{vmatrix}$$

soit un nombre complexe idéal; ces conditions sont

$$\alpha \equiv \gamma \equiv 0 \pmod{\beta}, \qquad \frac{\alpha^2}{\beta^2} \equiv \Omega \pmod{\frac{\gamma}{\beta}}.$$

Une proposition importante :

Puisque le calcul des congruences complexes ayant pour module un nombre complexe idéal est le même que celui des congruences ordinaires, les résidus des puissances d'un nombre entier complexe (par rapport à un nombre complexe idéal premier avec lui) se reproduisent périodiquement.

CALCUL DE t ET DE u.

Nous pouvons maintenant calculer t et u; nous savons que

$$t + u\sqrt{\Omega} = (a_1 + b_1\sqrt{\Omega})^m \qquad \text{ou} \qquad t + u\sqrt{\Omega} = (c_1 + d_1\sqrt{\Omega})^m,$$

m étant un entier, et cet entier va être déterminé par une congruence complexe. Examinons successivement les cinq cas qui peuvent se présenter et que nous avons énumérés plus haut :

Premier et troisième cas.

On a

$$t - 1 \equiv u\theta \equiv 0 \pmod{\frac{\Delta}{\rho}}.$$

On peut donc écrire la congruence complexe

$$t + u\sqrt{\Omega} \equiv 1 \pmod{\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}}.$$

Le module de cette congruence est un nombre complexe idéal; car θ di-

vise Ω, et, si $a_1 + b_1\sqrt{\Omega}$ est le plus petit nombre entier complexe dont la norme soit l'unité, on aura

$$t + u\sqrt{\Omega} = \left(a_1 + b_1\sqrt{\Omega}\right)^m;$$

d'où la congruence

$$\left(a_1 + b_1\sqrt{\Omega}\right)^m \equiv 1.$$

Si l'on fait varier m par valeurs entières, on verra les résidus de $\left(a_1 + b_1\sqrt{\Omega}\right)^m$ se reproduire périodiquement ; si k est le plus petit nombre, tel que

$$\left(a_1 + b_1\sqrt{\Omega}\right)^k \equiv 1,$$

la condition nécessaire et suffisante pour que

$$\left(a_1 + b_1\sqrt{\Omega}\right)^m \equiv 1$$

sera

$$m \equiv 0 \pmod{k}.$$

De plus, on verrait, comme pour les congruences ordinaires, que k est un diviseur du nombre des résidus premiers avec le nombre idéal

$$\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}.$$

De même on sait que, si a est premier avec b ; si k est le plus petit nombre, tel que

$$a^k \equiv 1 \pmod{b},$$

k est un diviseur du nombre des résidus (pris par rapport à b) et qui sont premiers avec b. Nous avons ici un résultat analogue qui se démontrerait identiquement de la même façon.

Deuxième et quatrième cas.

On a

$$t - 1 \equiv u\theta \equiv 0 \pmod{\frac{\Delta}{2\rho}}, \qquad t - 1 \equiv u\theta \pmod{\frac{\Delta}{\rho}},$$

ce qui équivaut à la congruence complexe

$$t + u\sqrt{\Omega} \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right).$$

Le module est-il un nombre complexe idéal?

Les conditions énoncées plus haut se réduisent ici à

$$\theta^2 \equiv \Omega \pmod{2\theta}$$

ou

$$\theta \equiv \frac{\Omega}{\theta} \pmod 2.$$

Dans le quatrième cas, la forme $px^2 + 2qxy + ry^2$ est improprement primitive : son discriminant Ω est donc impair ; donc θ et $\frac{\Omega}{\theta}$ sont tous deux impairs, c'est-à-dire que la condition est remplie.

Résumons les hypothèses relatives au deuxième cas :

La forme $px^2 + 2qxy + ry^2$ est proprement primitive ;

$\frac{\Delta}{\rho\theta}$ est pair ;

$\frac{w}{\sigma}$ et $\frac{rv - qw}{\sigma\theta}$ sont de même parité ;

$\frac{v}{\sigma}$ et $\frac{qv - pw}{\sigma\theta}$ sont de même parité.

On peut faire sur les parités de p, q, r les hypothèses suivantes :

$$p \equiv q \equiv r \equiv 1 \pmod 2,$$

$$p \equiv r \equiv 1, \qquad q \equiv 0 \pmod 2,$$

$$p \equiv q \equiv 1, \qquad r \equiv 0 \pmod 2,$$

$$q \equiv r \equiv 1, \qquad p \equiv 0 \pmod 2,$$

$$p \equiv 1, \qquad q \equiv r \equiv 0 \pmod 2,$$

$$r \equiv 1, \qquad q \equiv p \equiv 0 \pmod 2.$$

Dans les hypothèses 2, 3, 4, on a

$$\Omega \equiv 1 \pmod 2;$$

d'où

$$1 \equiv \theta \equiv \frac{\Omega}{\theta} \pmod 2.$$

Dans l'hypothèse 1, on peut supposer

$$\frac{w}{\sigma} \equiv 1, \qquad \frac{\nu}{\sigma} \equiv 0 \pmod 2;$$

mais alors

$$\frac{q\nu - pw}{\sigma} \equiv 1 \pmod 2,$$

et, par conséquent, $\frac{\nu}{\sigma}$ et $\frac{q\nu - pw}{\sigma\theta}$ ne seraient pas de même parité.

Cette hypothèse doit donc être rejetée, ainsi que

$$\frac{w}{\sigma} \equiv 1, \quad \frac{\nu}{\sigma} \equiv 0 \pmod 2.$$

On doit donc supposer

$$\frac{w}{\sigma} \equiv \frac{\nu}{\sigma} \equiv 1 \pmod 2;$$

d'où

$$\frac{r\nu - qw}{\sigma} \equiv \frac{q\nu - pw}{\sigma} \equiv 0 \pmod 2;$$

d'où, puisque $\frac{r\nu - qw}{\sigma} \equiv 1 \pmod 2$,

$$\theta \equiv 0 \pmod 2.$$

Dans l'hypothèse 5, on a

$$\frac{q\nu - pw}{\sigma} \equiv \frac{w}{\sigma} \pmod 2$$

et

$$\frac{r\nu - qw}{\sigma} \equiv 0 \pmod 2.$$

On ne peut donc supposer

$$\frac{w}{\sigma} \equiv 1, \qquad \frac{\nu}{\sigma} \equiv 0 \pmod 2.$$

Soit

$$\frac{\nu}{\tau} \equiv 1, \qquad \frac{w}{\tau} \equiv 0 \pmod 2.$$

On aura

$$\frac{q\nu - pw}{\tau} \equiv 0, \qquad \frac{q\nu - pw}{\tau\theta} \equiv 1 \pmod 2,$$

d'où

$$\theta \equiv 0 \pmod 2.$$

Soit maintenant

$$\frac{\nu}{\tau} \equiv \frac{w}{\tau} \equiv 1 \pmod 2.$$

On aura

$$\frac{r\nu - qw}{\tau} \equiv 0, \qquad \frac{q\nu - pw}{\tau} \equiv 1 \pmod 2.$$

Cette hypothèse doit donc être rejetée.

D'ailleurs, il est clair que l'hypothèse va se traiter comme l'hypothèse 5.

D'où il résulte que deux cas peuvent se présenter :

Première hypothèse :

$$\theta \equiv \frac{\Omega}{\theta} \pmod 2;$$

Seconde hypothèse :

$$\theta \equiv 0, \qquad \frac{\Omega}{\theta} \equiv 1 \pmod 2.$$

Dans la première hypothèse, le module de la congruence complexe étant un nombre idéal, tout se passera comme dans le premier et le troisième cas.

Dans la seconde hypothèse, il s'agit de résoudre une congruence complexe

$$\left(a_1 + b_1\sqrt{\Omega}\right)^m = t + u\sqrt{\Omega} \equiv 1 \mod \begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho'} & 0 \end{vmatrix},$$

dont le module n'est pas un nombre idéal.

Soit

$$t + u\sqrt{\Omega} \equiv 1, \qquad t' + u'\sqrt{\Omega} \equiv 1.$$

Quelle est la condition pour que

$$\left(t+u\sqrt{\Omega}\right)\left(t'+u'\sqrt{\Omega}\right)\equiv 1\,?$$

On aura

$$u\theta\equiv u'\theta\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{2\rho}\right),$$

$$t-1\equiv u\theta, \qquad t'-1\equiv u'\theta \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

Soient

$$\frac{\Delta}{2\rho\theta}=\alpha, \qquad u=\alpha\lambda, \qquad u'=\alpha\lambda', \qquad \Omega=\omega\theta.$$

Pour que

$$\left(t+u\sqrt{\Omega}\right)\left(t'+u'\sqrt{\Omega}\right)\equiv 1,$$

il faut et il suffit que

$$t'u\theta+u't\theta\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{2\rho}\right)$$

et

$$\mathrm{A}=tt'+uu'\Omega-t'u\theta-tu'\theta-1\equiv 0 \quad \left[\mathrm{mod}\left(\frac{\Delta}{\rho}=2\alpha\theta\right)\right].$$

Or

$$\mathrm{A}=t(t'-1)+(t-1)+\alpha^2\lambda\lambda'\omega\theta-\alpha\theta(t'\lambda+t\lambda')$$

ou

$$\left.\begin{aligned}&\mathrm{A}\equiv\alpha\theta\lambda' t+\alpha\theta\lambda+\alpha^2\lambda\lambda'\omega\theta-\alpha\theta(t'\lambda+t\lambda'),\\&\mathrm{A}\equiv\alpha\theta\lambda(1-t'+\alpha\lambda'\omega\theta)\equiv\alpha^2\theta\lambda\lambda'(\omega-\theta)\end{aligned}\right\}\ (\mathrm{mod}\,2\alpha\theta),$$

de sorte que la condition cherchée

$$\mathrm{A}\equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right)$$

se réduit à

$$\alpha\lambda\lambda'(\omega-\theta)\equiv 0 \quad (\mathrm{mod}\,2).$$

Or, par hypothèse,

$$\omega-\theta\equiv 1 \quad (\mathrm{mod}\,2).$$

Il faut donc et il suffit que l'un des trois nombres α, λ, λ' soit pair. Or, si

λ est pair, on aura

$$t + u\sqrt{\Omega} \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}\right).$$

En résumé, si deux nombres complexes sont congrus à 1 par rapport au module

$$\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}$$

[où

$$\frac{\Omega}{\theta} \equiv \theta + 1 \pmod 2,$$

de telle façon que le module ne soit pas un nombre idéal], pour que leur produit soit également congru à 1, il faut et il suffit que $\frac{\Delta}{2\rho\theta}$ soit pair ou que l'un des deux nombres donnés soit congru à 1 par rapport au module

$$\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}.$$

Cela posé, nous pourrons, dans l'hypothèse qui nous occupe, distinguer deux cas :

1° $\frac{\Delta}{2\rho\theta}$ est pair.

Alors le produit de deux nombres congrus à 1 est toujours congru à 1.

Si donc k est le plus petit des nombres m qui satisfassent à la congruence

$$(a_1 + b_1\sqrt{\Omega})^m \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right),$$

tous les autres sont des multiples de k, c'est-à-dire que tout se passe comme si le module était un nombre complexe idéal.

Nous devons toutefois faire une distinction importante. Dans le cas où le module était un nombre complexe idéal, les nombres

$$\left(a_1+b_1\sqrt{\Omega}\right)^m \quad \text{et} \quad \left(a_1+b_1\sqrt{\Omega}\right)^{m+k}$$

étaient congrus entre eux quel que soit m.

Ici cela n'aura plus lieu en général, à moins que

$$\left(a_1+b_1\sqrt{\Omega}\right)^k \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}\right);$$

mais on aura toujours

$$\left(a_1+b_1\sqrt{\Omega}\right)^m \equiv \left(a_1+b_1\sqrt{\Omega}\right)^{m+2k} \quad \left(\mathrm{mod}\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right),$$

de sorte que la période sera, en général, non pas k, mais $2k$. De plus, k est un diviseur du nombre des résidus pris par rapport au nombre idéal

$$\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}$$

et premiers par rapport à ce nombre idéal.

2^o $\frac{\Delta}{2\rho\theta}$ est impair.

Soit

$$(25) \qquad \left(a_1+b_1\sqrt{\Omega}\right)^m \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right)$$

une solution quelconque de la congruence. Cette solution nous fournira

une substitution semblable du système f, φ. Le carré de cette substitution sera également une substitution semblable, de sorte qu'on devra avoir

$$(a_1 + b_1\sqrt{\Omega})^{2m} \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right).$$

Or, d'après ce qu'on a vu plus haut, cela ne peut avoir lieu que si l'on a

$$(26) \qquad (a_1 + b_1\sqrt{\Omega})^{m} \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}\right).$$

On peut donc remplacer la congruence (25) par la congruence (26) dont le module est un nombre idéal; on est donc ainsi ramené aux cas déjà examinés.

Cinquième cas.

$2t$ et $2u$ sont entiers et de même parité.

$$4t^2 - 4u^2\Omega = 4, \qquad 2(t-1) \equiv 2u\theta \quad \left(\mathrm{mod}\,\frac{\Delta}{\rho}\right).$$

Ici le nombre $t + u\sqrt{\Omega}$ peut ne plus être entier complexe; mais les nombres de la forme $a + b\sqrt{\Omega}$, tels que $2a$ et $2b$ soient entiers et de même parité, jouissent de propriétés qui les rapprochent des nombres entiers. Nous les appellerons, pour cette raison, *nombres intègres*.

La somme ou le produit de deux nombres intègres est un nombre intègre.

Cela posé, on devra avoir

$$t + u\sqrt{\Omega} \equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right),$$

cette congruence pouvant être résolue, soit en nombres entiers, soit en nombres intègres.

Je dis qu'une congruence prise en nombres intègres par rapport au module

$$\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}$$

peut être multipliée par un nombre intègre quelconque. Il suffit, en effet, de faire voir qu'on peut la multiplier par

$$\sqrt{\Omega} \quad \text{et} \quad \frac{1+\sqrt{\Omega}}{2}.$$

Soit, en effet,

$$a + b\sqrt{\Omega} \equiv 0;$$

on aura

$$a = \alpha\frac{\Delta}{2\rho}, \qquad b = \beta\frac{\Delta}{2\rho\theta},$$

α et β étant entiers pendant que $\alpha\frac{\Delta}{\rho}$ et $\beta\frac{\Delta}{\rho\theta}$ sont de même parité.

En multipliant par $\sqrt{\Omega}$, il vient

$$\beta\frac{\Delta}{2\rho\theta}\Omega + \alpha\frac{\Delta}{2\rho}\sqrt{\Omega} \equiv 0.$$

Je dis que cette congruence est vérifiée; en effet,

$$\beta\frac{\Delta}{2\rho\theta}\Omega \equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{2\rho}\right),$$

puisque β et $\frac{\Omega}{\theta}$ sont entiers; de même

$$\alpha\frac{\Delta}{2\rho} \equiv 0 \quad \left(\mathrm{mod}\,\frac{\Delta}{2\rho\theta}\right),$$

puisque α et θ sont entiers.

En multipliant par $\frac{1+\sqrt{\Omega}}{2}$, il vient

$$\frac{\Delta}{2\rho}\left(\frac{\beta\Omega}{2\theta} + \frac{\alpha}{2}\right) + \frac{\Delta}{2\rho\theta}\left(\frac{\beta}{2} + \frac{\alpha\theta}{2}\right)\sqrt{\Omega} \equiv 0.$$

Pour que cette congruence soit vérifiée, il faut et il suffit que

$$\varrho\frac{\Omega}{\theta}+\alpha\equiv\beta+\alpha\theta\equiv 0 \pmod 2;$$

or, puisque

$$\frac{\Omega}{\theta}\equiv\theta\equiv 1 \pmod 2,$$

il faut et il suffit que

$$\beta+\alpha\equiv 0 \pmod 2.$$

Or, puisque, dans le cinquième cas, $\frac{\Delta}{\rho}$ est impair, et que l'on doit supposer

$$\beta\frac{\Delta}{\rho\theta}=\alpha\frac{\Delta}{\rho} \pmod 2,$$

cette condition sera toujours remplie.

C'est dire que toute congruence en nombres intègres, prise par rapport au module

$$\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix},$$

peut être multipliée par un nombre intègre quelconque, c'est-à-dire qu'elle jouit des mêmes propriétés que les congruences complexes en nombres entiers prises par rapport à un nombre idéal.

Cela posé, la congruence qu'il s'agit de résoudre pour avoir t et u s'écrit

$$t+u\sqrt{\Omega}=\left(\frac{c_1+d_1\sqrt{\Omega}}{2}\right)^m\equiv 1 \quad \left(\mathrm{mod}\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right).$$

La discussion de cette congruence est absolument la même que celle que nous avons faite dans le premier et dans le troisième cas.

Si k est le plus petit nombre qui, substitué à m, satisfasse à cette congruence, les autres seront ses multiples.

De plus, on aura, quel que soit m,

$$\left(\frac{c_1+d_1\sqrt{\Omega}}{2}\right)^{m+k}\equiv\left(\frac{c_1+d_1\sqrt{\Omega}}{3}\right)^{m}.$$

Une fois m connu, on aura sans peine t et u, et la connaissance de t et de u permettra d'écrire immédiatement les substitutions semblables du système f, φ.

Remarque. — Au commencement de ce travail, j'avais défini de la façon suivante les systèmes réduits formés d'une forme linéaire et d'une forme quadratique :

« On dit que le système f, φ est réduit, si l'on peut écrire

$$\pm\varphi=\alpha f^2+gh,$$

g et h étant linéaires et α positif, et si l'on peut choisir λ de telle sorte que la forme définie

$$\alpha f^2+\left(\frac{\lambda g+\frac{1}{\lambda}h}{2}\right)^2+\left(\frac{\lambda g-\frac{1}{\lambda}h}{2}\right)^2$$

soit réduite. »

On a vu que, si α est suffisamment petit, cette définition revient à la suivante :

On dit que le système f, φ est réduit quand gh est une forme binaire réduite en y et en z et quand les coefficients de y et de z dans f sont plus petits en valeur absolue que la moitié du coefficient de x.

De plus, on a vu qu'une transformation très simple permet de rendre α aussi petit que l'on veut. Il est donc plus logique et plus simple de s'en tenir, quel que soit α, à cette seconde définition; c'est ce que nous ferons toujours.

Mais ce n'est pas tout. Dans cette seconde définition, j'ai dit que gh doit être une forme binaire réduite et j'ai entendu par là une forme telle que

$$\left(\frac{\lambda g+\frac{1}{\lambda}h}{2}\right)^2+\left(\frac{\lambda g-\frac{1}{\lambda}h}{2}\right)^2$$

soit réduite.

Mais il y a une infinité de manières de définir les formes binaires réduites indéfinies, et à chacune d'elles va correspondre une façon nouvelle de définir les systèmes réduits tels que f, φ.

Cette définition nouvelle conviendra aussi bien que celles qui précèdent à l'objet que nous nous proposons, c'est-à-dire à la recherche des conditions d'équivalence des systèmes et de leurs substitutions semblables. On pourra donc choisir dans chaque cas particulier celle qui conduira aux calculs les plus rapides.

Par exemple, on pourra appeler *forme réduite* toute forme binaire indéfinie dont les coefficients extrêmes sont de signe contraire. On peut alors, par un calcul très simple, déduire d'une forme réduite une forme réduite équivalente et contiguë, de sorte qu'on arrive très rapidement à écrire toutes les réduites d'une forme donnée.

C'est de cette dernière définition que nous ferons usage dans l'exemple numérique qui va suivre.

Exemple numérique. — Soit

$$f = x + y + z,$$
$$\varphi = x^2 + 4y^2 - z^2 + 2xy + 2xz + 2yz.$$

On a

$$l = m = n = 1;$$

d'où les trois équations

$$a + b + c = 1,$$
$$a + 4b + 5c = 1,$$
$$a - 5b - 13c = 1;$$

d'où l'on tire

$$a = 1, \qquad b = c = 0$$

et, par conséquent,

$$\delta_1 = 1,$$
$$\lambda_1 = 1, \qquad \mu_1 = 0, \qquad \nu_1 = 0,$$
$$\lambda_2 = 0, \qquad \mu_2 = 1, \qquad \nu_2 = 0,$$
$$\lambda_3 = 0, \qquad \mu_3 = 0, \qquad \nu_3 = 1,$$
$$\Delta = \Delta_2 = \Delta_3 = 1.$$

On a, d'autre part,

$$\varphi(a, b, c) = 1;$$

d'où

$$-gh = \varphi - f^2 = 3y^2 - 2z^2.$$

Le problème est donc ramené à la réduction successive de la forme

$$3y^2 - 2z^2;$$

$3y^2 - 2z^2$ est elle-même une réduite, et l'on trouve immédiatement que la série des réduites de cette forme s'écrit comme il suit :

$$\begin{aligned}
&3y^2 - 2z^2,\\
&y^2 - 4yz - 2z^2,\\
&y^2 - 2yz - 5z^2,\\
&y^2 - 6z^2,\\
&y^2 + 2yz - 5z^2,\\
&y^2 + 4yz - 2z^2,\\
&3y^2 - 2z^2,
\end{aligned}$$

et se reproduisent ensuite périodiquement. Dans ce tableau, chaque réduite se déduit de la précédente par l'une des substitutions

$$\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \quad \text{ou} \quad \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}.$$

Elles se déduisent de $3y^2 - 2z^2$ par les substitutions

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix}, \quad \begin{vmatrix} 1 & 3 \\ 1 & 4 \end{vmatrix},$$

$$\begin{vmatrix} 1 & 4 \\ 1 & 5 \end{vmatrix}, \quad \begin{vmatrix} 5 & 4 \\ 6 & 5 \end{vmatrix}.$$

Soit

$$\begin{vmatrix} k_1 & k'_1 \\ k_2 & k'_2 \end{vmatrix}$$

l'une de ces substitutions.

La substitution correspondante

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & k_1 & k'_1 \\ 0 & k_2 & k'_2 \end{vmatrix},$$

qui réduira le système f, φ, devra satisfaire à la condition

$$-\frac{\Delta}{2} < \Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0 < \frac{\Delta}{2}$$

ou

$$-\tfrac{1}{2} < k_1 + k_2 + k_0 < \tfrac{1}{2},$$

d'où

$$k_0 = -(k_1 + k_2).$$

De même

$$k'_0 = -(k'_1 + k'_2),$$

de sorte que la suite des substitutions qui réduisent f, φ est

$$\begin{vmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -3 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{vmatrix},$$

$$\begin{vmatrix} 1 & -2 & -5 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -7 \\ 0 & 1 & 3 \\ 0 & 1 & 4 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -9 \\ 0 & 1 & 4 \\ 0 & 1 & 5 \end{vmatrix};$$

$$\begin{vmatrix} 1 & -11 & -9 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix};$$

d'où, pour les systèmes réduits de f, φ, le tableau suivant :

$$\begin{aligned}
&x, \quad && x^2 - 3y^2 + 2z^2,\\
&x, \quad && x^2 - y^2 + 4yz + 2z^2,\\
&x, \quad && x^2 - y^2 + 2yz + 5z^2,\\
&x, \quad && x^2 - y^2 + 6z^2,\\
&x, \quad && x^2 - y^2 - 2yz + 5z^2,\\
&x, \quad && x^2 - y^2 - 4yz + 2z^2,\\
&x, \quad && x^2 - 3y^2 + 2z^2.
\end{aligned}$$

De plus, si

$$T = \begin{vmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \qquad T_1 = \begin{vmatrix} 1 & -11 & -9 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix},$$

les substitutions semblables du système f, φ seront les puissances de

$$T_1 T^{-1} = \begin{vmatrix} 1 & -10 & -8 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix}.$$

On aurait pu arriver au même résultat directement.

En effet, ici

$$\Omega = 6,$$

et l'équation

$$t^2 - \Omega u^2 = 1$$

admet, pour sa solution la plus simple,

$$t = 5, \qquad u = 2,$$

ce qui conduit, pour la substitution semblable la plus simple de gh, à

$$\begin{vmatrix} 5 & 4 \\ 6 & 5 \end{vmatrix};$$

d'un autre côté, les congruences auxquelles sont assujettis les nombres t et u ayant pour module $\frac{\Delta}{\rho}$, qui est ici l'unité, sont toujours satisfaites. Donc les nombres

$$t = 5, \qquad u = 2$$

sont bien ceux qui correspondent à la substitution semblable la plus simple du système f, φ; c'est dire que cette substitution est de la forme

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix},$$

et, comme elle doit reproduire

$$x + y + z,$$

elle aura pour coefficients

$$k_0 = -10, \qquad k'_0 = -8.$$

C. Q. F. D.

Deuxième exemple. — Soit à trouver les substitutions semblables du système

$$14x + y + 2z,$$
$$y^2 - 6z^2.$$

On a

$$\Omega = 6,$$

et les substitutions semblables devront être de la forme

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & t & 6u \\ 0 & u & t \end{vmatrix},$$

où

$$(t + u\sqrt{6}) = (5 + 2\sqrt{6})^m;$$

puisque

$$t = 5,$$

$u = 2$ est la solution la plus simple de

$$t^2 - 6u^2 = 1.$$

On est donc conduit aux congruences suivantes

$$\begin{aligned} t \quad + 2u &\equiv 1 \pmod{14}. \\ 6u + 2t &\equiv 2. \end{aligned}$$

Ici

$$\begin{gathered} \nu = 1, \qquad \omega = 2, \\ \sigma = 1, \qquad \rho = 1, \qquad \frac{\Delta}{\rho} = 14, \\ \frac{r\nu - q\omega}{\sigma} = -6, \qquad \frac{q\nu - p\omega}{\sigma} = -2, \qquad \theta = 2, \\ \frac{\Delta}{\rho\theta} = 7 \equiv 1 \pmod{2}. \end{gathered}$$

De plus, la forme est proprement primitive, de sorte qu'on est dans le premier cas et que les congruences se réduisent à

$$\begin{aligned} t &\equiv 1 \pmod{14}, \\ u &\equiv 0 \pmod{7}. \end{aligned}$$

On peut d'ailleurs retrouver ces congruences directement.

Reprenons

$$\left.\begin{aligned} t \quad + 2u &\equiv 1 \\ 6u + 2t &\equiv 2 \end{aligned}\right\} \pmod{14}.$$

Multiplions la première par $-6u$, la seconde par t et ajoutons; il vient

$$2(t^2 - 6u^2) \equiv 2t - 6u \pmod{14}.$$

Multiplions de même la première par t, la seconde par $-u$; il vient

$$t^2 - 6u^2 \equiv t - 2u \pmod{14}.$$

A cause de la relation

$$t^2 - 6u^2 = 1,$$

ces congruences se réduisent à

$$\left.\begin{aligned} 2t - 6u &\equiv 2 \\ t - 2u &\equiv 1 \end{aligned}\right\} \pmod{14},$$

qui, jointes aux premières, donnent

$$12u \equiv 4u \equiv 0 \pmod{14}$$

ou

$$\begin{aligned} u &\equiv 0 \pmod{7}, \\ 2u &\equiv 0 \pmod{14}, \\ t &\equiv 1 \pmod{14}. \end{aligned}$$

La recherche de t et de u se ramène donc à la résolution de la congruence complexe

$$t + u\sqrt{6} = \left(5 + 2\sqrt{6}\right)^m \equiv 1, \qquad \mod \begin{vmatrix} 0 & 14 \\ 7 & 0 \end{vmatrix}.$$

Or on trouve que, par rapport à ce module qui est un nombre complexe idéal,

$$\begin{aligned} \left(5 + 2\sqrt{6}\right)^2 &\equiv \quad 7 + 6\sqrt{6}, \\ \left(5 + 2\sqrt{6}\right)^3 &\equiv \quad 9 + 2\sqrt{6}, \\ \left(5 + 2\sqrt{6}\right)^4 &\equiv -1, \\ \left(5 + 2\sqrt{6}\right)^5 &\equiv -5 - 2\sqrt{6}, \\ \left(5 + 2\sqrt{6}\right)^6 &\equiv -7 - 6\sqrt{6}, \\ \left(5 + 2\sqrt{6}\right)^7 &\equiv -9 - 2\sqrt{6}, \\ \left(5 + 2\sqrt{6}\right)^8 &\equiv \quad 1, \end{aligned}$$

et que par conséquent on aura, si m et μ sont des entiers quelconques,

$$\left(5 + 2\sqrt{6}\right)^{m+8\mu} \equiv \left(5 + 2\sqrt{6}\right)^m.$$

Les valeurs de $t + u\sqrt{6}$ nous est donc donnée par

$$(5 + 2\sqrt{6})^8 = 46099201 + 18819920\sqrt{6}.$$

La substitution semblable la plus simple du système est donc de la forme

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & 46099201 & 112919520 \\ 0 & 18819920 & 46099201 \end{vmatrix},$$

et, comme elle doit reproduire

$$14x + y + 2z,$$

on aura

$$1 = 14k_0 + 83739041,$$
$$2 = 14k'_0 + 205117922;$$

d'où

$$k_0 = 5981360,$$
$$k'_0 = 14651280.$$

Donc, les substitutions semblables du système

$$14x + y + 2z, \qquad y^2 - 6z^2$$

sont les puissances de

$$\begin{vmatrix} 1 & 5918360 & 14651280 \\ 0 & 46099201 & 112919520 \\ 0 & 18819920 & 46099201 \end{vmatrix}.$$