SUR UN MODE NOUVEAU

DE REPRÉSENTATION GÉOMÉTRIQUE

DES

FORMES QUADRATIQUES DÉFINIES OU INDÉFINIES,

PAR M. H. POINCARÉ,

Ingénieur des Mines.

Le lien qui existe entre la théorie des réseaux parallélogrammatiques de Bravais et celle des formes quadratiques a été remarqué depuis longtemps, mais on s'est restreint jusqu'ici aux formes définies; le but principal de ce Mémoire est de faire voir que rien n'est plus facile que d'appliquer la même représentation géométrique aux formes indéfinies.

J'ai dû d'abord étudier les propriétés de ces réseaux parallélogrammatiques et en ébaucher pour ainsi dire l'arithmétique. Je les ai représentés par trois notations différentes, suivant que l'une ou l'autre me semblait plus commode.

Ainsi le réseau formé par les points x, y, où

$$x = am + bn,$$
$$y = cm + dn$$

(a, b, c, d sont des constantes, m et n des indéterminées qui peuvent prendre toutes les valeurs entières positives ou négatives), peut être représenté :

1° Tantôt par la notation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix};$$

2° Tantôt par la notation

$$Am + Bn,$$

où A et B représentent les nombres complexes $a + c\sqrt{D}$, $b + d\sqrt{D}$;

3° Tantôt par la congruence

$$\alpha x + \beta y \equiv 0 \pmod{\gamma},$$

à laquelle satisfont les coordonnées de tous ses points.

Les réseaux jouissent de propriétés qui rappellent quelques-unes des propriétés des nombres; c'est ainsi qu'on est amené à considérer des réseaux entiers, fractionnaires ou incommensurables, des réseaux multiples ou diviseurs, plus petits communs multiples ou plus grands communs diviseurs d'autres réseaux, des réseaux premiers entre eux et des réseaux premiers absolus.

Après ces considérations préliminaires, je me suis occupé de la représentation des nombres complexes de la forme

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

Quand

$$D < 0,$$

le nombre est imaginaire, et on le représente ordinairement par le point dont les coordonnées sont

$$a, \quad b\sqrt{-D}.$$

Au lieu de cela, je le représente par le point dont les coordonnées sont

$$a, \quad b,$$

mode de représentation qui a l'avantage de s'appliquer au cas où

$$D > 0$$

et qu'on peut considérer comme dérivé du premier mode de représentation par projection orthogonale, de même que l'ellipse dérive du cercle.

En effet, supposons qu'un point m ait dans un plan P pour coordonnées

$$a,\ b\sqrt{-\mathrm{D}}.$$

Supposons qu'un plan Q coupe le plan P suivant l'axe des x et fasse avec lui un dièdre égal à

$$\arccos\sqrt{-\mathrm{D}}.$$

Les coordonnées de la projection du point m sur le plan Q (en conservant le même axe des x dans le plan Q) seront

$$a,\ b.$$

Toutefois, pour simplifier le langage, nous convenons que, quand nous parlerons figures égales ou semblables, il s'agira de figures égales ou semblables dans le plan P et non dans le plan Q.

Ainsi, quand nous dirons que les triangles formés par les points représentatifs des nombres complexes

$$\begin{aligned}
&\alpha+\beta\sqrt{\mathrm{D}}, \quad \gamma+\delta\sqrt{\mathrm{D}},\\
&\alpha'+\beta'\sqrt{\mathrm{D}}, \quad \gamma'+\delta'\sqrt{\mathrm{D}},\\
&\alpha''+\beta''\sqrt{\mathrm{D}}, \quad \gamma''+\delta''\sqrt{\mathrm{D}}
\end{aligned}$$

sont égaux ou semblables, il s'agira, non pas des triangles

$$(\alpha,\ \beta;\ \alpha',\ \beta';\ \alpha'',\ \beta'') \text{ et } (\gamma,\ \delta;\ \gamma',\ \delta';\ \gamma'',\ \delta''),$$

mais des triangles

$$\left(\alpha,\ \beta\sqrt{-\mathrm{D}};\ \alpha',\ \beta'\sqrt{-\mathrm{D}};\ \alpha'',\ \beta''\sqrt{-\mathrm{D}}\right)$$

et

$$\left(\gamma,\ \delta\sqrt{-\mathrm{D}};\ \gamma',\ \delta'\sqrt{-\mathrm{D}};\ \gamma'',\ \delta''\sqrt{-\mathrm{D}}\right).$$

Je remarque ensuite que les points représentatifs de tous les nombres complexes existants qui sont multiples d'un nombre complexe donné existant ou idéal forment un réseau parallélogrammatique que l'on peut

regarder comme un nouveau mode de représentation de ce nombre existant ou idéal donné.

Et il est aisé de voir que, si un nombre idéal en divise un autre, le réseau correspondant au premier divisera le réseau correspondant au second, de telle sorte que ce mode de représentation fournit un moyen d'exposer d'une manière concrète la théorie des nombres idéaux. Il conduit de plus à ce théorème :

On peut représenter, avec une approximation aussi grande qu'on voudra, un nombre complexe quelconque

$$a + b\sqrt{D},$$

où a et b peuvent être incommensurables, par une expression de la forme

$$\Sigma\lambda_m(\alpha + \beta\sqrt{D})^m,$$

où λ_m et m sont des nombres entiers, α et β des nombres fractionnaires donnés (à dénominateurs plus grands que 2).

De l'étude des nombres complexes existants ou idéaux je passe à celle des formes quadratiques.

Depuis longtemps on a représenté la forme

$$ax^2 + 2bxy + cy^2,$$

quand elle est définie, par le réseau

$$\begin{bmatrix} \frac{1}{\sqrt{a}}b & \sqrt{a} \\ \frac{\sqrt{ac-b^2}}{a} & 0 \end{bmatrix}.$$

Au lieu de cela je considère, comme plus haut, ce réseau comme placé dans le plan P, et, le projetant sur le plan Q, j'obtiens le nouveau réseau

$$\begin{bmatrix} \frac{1}{\sqrt{a}}b & \sqrt{a} \\ \frac{1}{\sqrt{a}}\varepsilon & 0 \end{bmatrix},$$

si $b^2 - ac = D\varepsilon^2$; ce nouveau mode de représentation s'applique évidemment au cas où $D > 0$, c'est-à-dire au cas des formes indéfinies.

Outre ce mode principal de représentation d'une forme par son réseau typique, il peut être avantageux de la représenter par des réseaux semblables, mais entiers, par exemple

$$\begin{bmatrix} b & a \\ \varepsilon & 0 \end{bmatrix}.$$

Cette infinité de réseaux semblables au réseau typique de la forme donnée s'appelleront les *réseaux représentatifs* de cette forme.

On sait que le mode ancien de représentation des formes définies a permis d'établir une théorie géométrique des formes réduites, de faire voir, par exemple, qu'une forme réduite correspond à un triangle fondamental acutangle, qu'une forme donnée est toujours équivalente à une forme réduite et à une seule.

De même, le mode nouveau de représentation permet d'arriver à des résultats analogues pour les formes indéfinies. Grâce à lui, je suis arrivé très facilement, dans la Partie de ce travail intitulée : *Des triangles ambigus*, à trouver à quoi correspondent géométriquement les formes réduites indéfinies et à donner une démonstration géométrique simple des principaux théorèmes qui les concernent.

J'examine de même différents autres problèmes relatifs aux formes quadratiques :

1° *Reconnaître si une forme en implique une autre.*

2° *Trouver toutes les transformations d'une forme en elle-même.*

Enfin, dans la dernière Partie de ce travail, j'étudie une opération très simple à effectuer sur les réseaux et que j'appelle *multiplication seconde* (pour la distinguer d'un autre mode de multiplication envisagé dans la première Partie).

Cette multiplication seconde correspond :

En ce qui concerne les nombres complexes idéaux, à la multiplication ordinaire;

En ce qui concerne les formes quadratiques, à la composition des formes de Gauss.

Cette considération me permet d'établir d'une façon nouvelle les théorèmes de Gauss relatifs à la composition des formes et en particulier les suivants :

Si une forme

$$Ax^2 + 2Bxy + Cy^2$$

résulte de la composition de

$$ax^2 + 2bxy + cy^2$$

et

$$a'x^2 + 2b'xy + c'y^2,$$

si M, m, m' *sont les plus grands communs diviseurs de*

$$\begin{array}{l} A,\ 2B,\ C, \\ a,\ 2b,\ c, \\ a',\ 2b',\ c', \end{array}$$

1° $\sqrt{B^2 - AC}$ *est le p. g. c. d.* (1) *de*

$$m'\sqrt{b^2 - ac} \text{ et } m\sqrt{b'^2 - a'c'};$$

2° $M = mm'$;

3° *Pour que la forme résultante soit dérivée d'une improprement primitive, il faut et il suffit que l'une des composantes soit dérivée d'une improprement primitive.*

---

(1) Pour abréger, nous écrirons souvent

p. g. c. d. et p. p. c. m.

au lieu de *plus grand commun diviseur* et *plus petit commun multiple*.

PREMIÈRE PARTIE.

ARITHMÉTIQUE DES RÉSEAUX.

Supposons que dans un plan on fasse passer par l'origine deux droites quelconques, puis qu'on mène à chacune de ces droites une série indéfinie de parallèles équidistantes. Ces parallèles diviseront le plan en une infinité de parallélogrammes égaux; nous appellerons *réseau* le système de points formé par les sommets de tous ces parallélogrammes. Les coordonnées de ces points seront données par des équations telles que

$$(1) \qquad \begin{cases} x = am + bn, \\ y = cm + dn, \end{cases}$$

où m et n peuvent prendre toutes les valeurs entières positives ou négatives.

Le réseau sera désigné par la notation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

et le déterminant $ad - bc$ s'appellera la *norme du réseau*. Ce ne sera autre chose que la surface des parallélogrammes égaux qui forment le réseau.

Commençons par énoncer différents théorèmes qui se déduisent immédiatement de ceux de Bravais.

THÉORÈME I. — *Si des points sont disposés dans le plan de telle sorte* 1° *que la distance de deux quelconques d'entre eux ne puisse devenir plus petite qu'une quantité donnée,* 2° *que si les points* x, y *et* x', y' *font partie du système de ces points il en soit de même des points* $x \pm x', y \pm y'$, *le système de ces points est un réseau.*

THÉORÈME II. — *La norme d'un réseau est la limite de la surface d'un*

cercle divisé par le nombre des points du réseau contenus dans ce cercle, quand le rayon du cercle augmente indéfiniment (BRAVAIS).

Définition. — Un réseau est entier quand a, b, c, d sont entiers. Un réseau A est multiple d'un réseau B quand tous les points du réseau A font partie du réseau B. Deux réseaux sont équivalents quand tous les points de l'un font partie de l'autre et réciproquement. Un réseau est unitaire s'il est équivalent au réseau $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

THÉORÈME III. — *Si un réseau* A *est multiple d'un réseau* B : 1° *le nombre des points du réseau* B *compris dans l'intérieur et sur deux côtés non opposés d'un des parallélogrammes qui forment le réseau* A *est le même quel que soit ce parallélogramme;* 2° *il est égal au quotient de la norme de* A *par la norme de* B, *moins* 2.

Corollaire I. — La norme d'un réseau est divisible par la norme des réseaux qui le divisent.

Corollaire II. — Les normes de deux réseaux équivalents sont égales.

Rapport de deux réseaux.

Supposons que l'on pose

$$(2)\qquad \begin{cases} m = \alpha\mu + \beta\nu, \\ n = \gamma\mu + \beta\nu; \end{cases}$$

il vient dans (1)

$$x = (a\alpha + b\gamma)\mu + (a\beta + b\delta)\nu,$$
$$y = (c\alpha + d\gamma)\mu + (c\beta + d\delta)\nu.$$

On a donc déterminé un nouveau réseau

$$\begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix} = \mathrm{A}'.$$

On dira que le réseau

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

est le rapport de ce nouveau réseau à l'ancien

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \mathrm{A}.$$

Pour trouver le rapport inverse de A à A′ il faut résoudre les équations (2), ce qui donne

$$\left.\begin{aligned} \mu &= \frac{\delta}{\Delta} m - \frac{\beta}{\Delta} n \\ \nu &= -\frac{\gamma}{\Delta} m + \frac{\alpha}{\Delta} n \end{aligned}\right\} (\Delta = \alpha\delta - \beta\gamma).$$

Le rapport cherché est donc

$$\begin{bmatrix} \frac{\delta}{\Delta} & -\frac{\beta}{\Delta} \\ -\frac{\gamma}{\Delta} & \frac{\alpha}{\Delta} \end{bmatrix}.$$

Cette opération peut être considérée comme une sorte de multiplication des réseaux, mais elle n'est pas commutative.

THÉORÈME IV. — *Si un réseau* A *est multiple d'un réseau* B, *le rapport des réseaux est entier.*

En effet, pour que m et n soient entiers toutes les fois que μ et ν le sont, il faut et il suffit que α, β, γ, δ soient entiers.

THÉORÈME V. — *Si deux réseaux sont équivalents, leur rapport est unitaire.*

En effet, il doit être entier, et, de plus, m et n doivent pouvoir prendre toutes les valeurs entières quand μ et ν prennent toutes les valeurs entières.

Réduction d'un réseau à sa plus simple expression.

Parmi tous les réseaux qui sont équivalents à un réseau donné, il en est une infinité dont l'expression est de la forme

$$\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}. \tag{3}$$

Pour amener à la forme (3) un réseau donné

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tag{4}$$

on opérera de la manière suivante.

Soit D le plus grand commun diviseur de c et de d.

Soient $\frac{c}{D} = \gamma$, $\frac{d}{D} = \delta$.

On pourra toujours résoudre l'équation

$$\alpha\delta + \gamma\beta = 1$$

par des valeurs entières de α et de β, puisque γ et δ sont premiers entre eux.

On multipliera alors le réseau (4) par le rapport

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

qui est unitaire, et il viendra

$$\begin{bmatrix} a\beta + b\alpha, & a\delta - b\gamma \\ c\beta + d\alpha, & c\delta - d\gamma \end{bmatrix},$$

où

$$c\delta - d\gamma = 0.$$

Le réseau (4) est donc réduit à la forme (3). Cette réduction a déjà été indiquée par Eisenstein dans ses *Mathematische Abhandlungen*.

Conditions d'équivalence de deux réseaux.

Pour que deux réseaux

$$R = \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \quad \text{et} \quad R' = \begin{bmatrix} a' & b' \\ c' & 0 \end{bmatrix}$$

soient équivalents, il faut et il suffit que

$$c = c', \quad b = b',$$
$$a \equiv a' \pmod{b}.$$

Conditions de divisibilité.

Pour que R′ divise R, il faut et il suffit que

$$c \equiv 0 \pmod{c'}, \quad b \equiv 0 \pmod{b'},$$
$$a \equiv a' \frac{c}{c'} \pmod{b'}.$$

Plus grand commun diviseur et plus petit commun multiple.

Le plus petit commun multiple de R et de R′ est le système des points communs à ces deux réseaux.

Leur plus grand commun diviseur est le système des points

$$x = am + bn + a'm' + b'n',$$
$$y = cm + c'm',$$

où m, n, m', n' prennent toutes les valeurs entières positives et négatives.

D'après le théorème I, si les deux réseaux sont entiers, ces deux systèmes de points sont des réseaux. Le premier est un commun multiple de R et R′ et celui dont la norme est la plus petite; le second est un de leurs communs diviseurs et celui dont la norme est la plus grande.

Problème. — *Si le p. p. c. m. et le p. g. c. d. de* R *et de* R′ *sont respectivement*

$$R'_1 = \begin{bmatrix} A' & B' \\ C' & 0 \end{bmatrix}, \quad R_1 = \begin{bmatrix} A & B \\ C & 0 \end{bmatrix},$$

calculer A, B, C, A′, B′, C′.

Soient

C_1 le p. g. c. d. de c et c',

$$\gamma = \frac{c}{C_1}, \quad \gamma' = \frac{c'}{C_1};$$

B_1 le p. g. c. d. de

$$b,\ b' \text{ et } a\gamma' - a'\gamma;$$

β le p. g. c. d. de

$$b \text{ et } b';$$

α et α' deux nombres entiers tels que

$$\alpha\gamma + \alpha'\gamma' = 1.$$

Pour que R_1 divise R et R', il faut et il suffit que

$$c \equiv c' \equiv 0 \pmod{C}, \quad b \equiv b' \equiv 0 \pmod{B},$$
$$a \equiv A\frac{c}{C} \pmod{B}, \quad a' \equiv A\frac{c'}{C} \pmod{B}.$$

Or les deux premières congruences peuvent se remplacer par

$$C_1 \equiv 0 \pmod{C},$$

les deux dernières par

$$a\gamma' - a'\gamma \equiv 0 \pmod{B}, \quad a\alpha + a'\alpha' \equiv A\frac{C_1}{C} \pmod{B}.$$

Donc, pour que R_1 divise R et R', il faut et il suffit que

$$C_1 \equiv 0 \pmod{C}, \quad b \equiv b' \equiv a\gamma' - a'\gamma \equiv 0 \pmod{B},$$
$$a\alpha + a'\alpha' \equiv A\frac{C_1}{C} \pmod{B}$$

ou que

$$C_1 \equiv 0 \pmod{C}, \quad B_1 \equiv 0, \quad a\alpha + a'\alpha' \equiv A\frac{C_1}{C} \pmod{B},$$

c'est-à-dire qu'il divisera R et R', pourvu qu'il divise le réseau

$$\begin{bmatrix} a\alpha + a'\alpha' & B_1 \\ C_1 & 0 \end{bmatrix}.$$

Mais la norme de R_1 doit être aussi grande que possible; on a donc

$$B = B_1, \quad C = C_1, \quad A \equiv a\alpha + a'\alpha' \pmod{B}.$$

Cherchons maintenant A', B', C'.

Pour que R et R′ divisent R'_1, il faut et il suffit que

$$C' \equiv 0 \pmod{c}, \quad C' \equiv 0 \pmod{c'}, \quad B' \equiv 0 \pmod{b}, \quad B' \equiv 0 \pmod{b'},$$

$$A' \equiv a\frac{C'}{c} \pmod{b}, \quad A' \equiv a'\frac{C'}{c'} \pmod{b'}$$

ou bien que

$$C' \equiv 0 \left(\mathrm{mod.}\ \frac{cc'}{C_1}\right), \quad B' \equiv 0 \left(\mathrm{mod.}\ \frac{bb'}{\beta}\right),$$

$$A' \equiv a\frac{C'}{c} \pmod{b}, \quad A' \equiv a'\frac{C'}{c'} \pmod{b'}.$$

Posons

$$C' \equiv \frac{cc'}{C_1}\lambda;$$

les deux dernières congruences deviendront

$$A' \equiv a\gamma'\lambda \pmod{b}, \quad A' \equiv a'\gamma\lambda \pmod{b'}, \tag{5}$$

d'où

$$(a\gamma' - a'\gamma)\lambda \equiv 0 \pmod{\beta},$$

ou

$$\frac{a\gamma' - a'\gamma}{B_1}\lambda \equiv 0 \left(\mathrm{mod.}\ \frac{\beta}{B_1}\right),$$

ou

$$\lambda \equiv 0 \left(\mathrm{mod.}\ \frac{\beta}{B_1}\right).$$

Soit A'_1 un nombre entier qui satisfasse aux congruences

$$A'_1 \equiv a\gamma'\frac{\beta}{B_1} \pmod{b}, \quad A'_1 \equiv a'\gamma\frac{\beta}{B_1} \pmod{b'}.$$

Les deux congruences (5) pourront se remplacer par les deux congruences

$$\lambda \equiv 0 \left(\mathrm{mod.}\ \frac{\beta}{B_1}\right), \quad A' \equiv A'_1\frac{\lambda B_1}{\beta} \left(\mathrm{mod.}\ \frac{bb'}{\beta}\right).$$

Donc, pour que R'_1 soit multiple de R et de R′, il faut et il suffit que

$$C' \equiv 0 \left(\mathrm{mod.}\ \frac{cc'}{C_1}\frac{\beta}{B_1}\right), \quad B' \equiv 0 \left(\mathrm{mod.}\ \frac{bb'}{\beta}\right), \quad A' \equiv A'_1\frac{C'C_1B_1}{cc'\beta} \left(\mathrm{mod.}\ \frac{bb'}{\beta}\right),$$

c'est-à-dire qu'il soit multiple du réseau

$$\begin{bmatrix} A'_1 & \frac{bb'}{\beta} \\ \frac{cc'\beta}{C_1B_1} & 0 \end{bmatrix}.$$

Mais la norme de R'_1 doit être aussi petite que possible; on a donc

$$A' = A'_1, \quad B' = \frac{bb'}{\beta}, \quad C' = \frac{cc'\beta}{C_1B_1}.$$

THÉORÈME VI. — *Le produit des normes de deux réseaux est égal au produit des normes de leur p. g. c. d. et de leur p. p. c. m.*

En effet, on a

$$B = B_1, \quad C = C_1, \quad B' = \frac{bb'}{\beta}, \quad C' = \frac{cc'\beta}{B_1C_1};$$

on a donc, en multipliant,

$$BCB'C' = bcb'c'. \qquad \text{C. Q. F. D.}$$

THÉORÈME VII. — *Tout diviseur commun à deux réseaux divise leur plus grand commun diviseur.*

THÉORÈME VIII. — *Tout multiple commun à deux réseaux est multiple de leur p. p. c. m.*

Il suffit d'énoncer ces deux résultats pour que l'on saisisse immédiatement leur évidence.

Définitions. — On appelle *réseau premier* un réseau dont la norme est un nombre premier, *réseau second* un réseau dont la norme est une puissance d'un nombre premier.

THÉORÈME IX. — *Un réseau quelconque peut être considéré comme le p. p. c. m. d'un certain nombre de réseaux seconds premiers entre eux.*

Soit en effet

$$p^\alpha q^\beta r^\gamma$$

la norme du réseau donné décomposée en facteurs premiers.

Ce réseau aura un diviseur de norme p^α.

Soit en effet

$$R = \begin{bmatrix} A & p^{\alpha-\alpha'} q^{\beta-\beta'} r^{\gamma-\gamma'} \\ p^{\alpha'} q^{\beta'} r^{\gamma'} & 0 \end{bmatrix};$$

on pourra toujours choisir a de telle façon que

$$aq^{\beta'} r^{\gamma'} \equiv A \pmod{p^{\alpha-\alpha'}},$$

et par conséquent que le réseau

$$P_\alpha = \begin{bmatrix} a & p^{\alpha-\alpha'} \\ p^{\alpha'} & 0 \end{bmatrix}$$

divise R.

Le réseau P_α qui divise R a pour norme p^α; on trouverait de même des réseaux Q_β, R_γ divisant R et ayant pour norme q^β et r^γ.

Donc R est multiple de

$$H = \text{p. p. c. m. de } P_\alpha, Q_\beta, R_\gamma.$$

Mais P_α, Q_β, R_γ étant premiers deux à deux, on a

$$\text{norme } H = \text{norme } P_\alpha \times \text{norme } Q_\beta \times \text{norme } R_\gamma = p^\alpha q^\beta r^\gamma = \text{norme R}.$$

Donc

$$R = H. \qquad \text{C. Q. F. D.}$$

Notation nouvelle. — Considérons le système des points dont les coordonnées sont définies par les équations

$$x = \alpha_1 m_1 + \alpha_2 m_2 + \alpha_3 m_3 + \alpha_4 m_4,$$
$$y = \beta_1 m_1 + \beta_2 m_2 + \beta_3 m_3 + \beta_4 m_4,$$

où les α et les β sont des quantités données et les m des variables qui peuvent prendre toutes les valeurs entières positives ou négatives.

Si les α et les β ont une commune mesure, ce système de points est un réseau; nous le représenterons par la notation

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix}.$$

Par exemple, le p. g. c. d. de

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ et } \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$$

sera

$$\begin{bmatrix} a & b & a' & b' \\ c & d & c' & d' \end{bmatrix}.$$

THÉORÈME X. — *La norme de*

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{bmatrix}$$

est le p. g. c. d. des normes de

$$\begin{bmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{bmatrix}, \quad \begin{bmatrix} \alpha_1 & \alpha_3 \\ \beta_1 & \beta_3 \end{bmatrix} \text{ et } \begin{bmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{bmatrix}.$$

En effet, soit δ la plus grande commune mesure de

$$\beta_1, \ \beta_2, \ \beta_3;$$

soient $\beta_1 = \lambda_1 \delta$, $\beta_2 = \lambda_2 \delta$, $\beta_3 = \lambda_3 \delta$.

Soit δ_1 la plus grande commune mesure de

$$\alpha_1 \lambda_2 - \alpha_2 \lambda_1, \quad \alpha_1 \lambda_3 - \alpha_3 \lambda_1, \quad \alpha_2 \lambda_3 - \alpha_3 \lambda_2.$$

Les nombres λ_1, λ_2, λ_3 seront des entiers premiers entre eux; il existera donc trois nombres μ_1, μ_2, μ_3 tels que

$$\mu_1 \lambda_1 + \mu_2 \lambda_2 + \mu_3 \lambda_3 = 1.$$

Posons maintenant

$$(\alpha) \qquad \begin{cases} m_1 = \mu_1 M_1 + 0 + N_2 \lambda_3 + N_3 \lambda_2, \\ m_2 = \mu_2 M_1 + N_1 \lambda_3 + 0 - N_3 \lambda_1, \\ m_3 = \mu_3 M_1 - N_1 \lambda_2 - N_2 \lambda_1 + 0 ; \end{cases}$$

à tout système de valeurs entières de M_1, N_1, N_2, N_3 correspondra un

système de valeurs entières de m_1, m_2, m_3; de même on pourra choisir un système de valeurs entières de M_1, N_1, N_2, N_3 tel que m_1, m_2, m_3 prennent des valeurs entières quelconques.

Car les déterminants dont le complexe est représenté par

$$\begin{vmatrix} \mu_1 & 0 & \lambda_3 & \lambda_2 \\ \mu_2 & \lambda_3 & 0 & -\lambda_1 \\ \mu_3 & -\lambda_2 & -\lambda_1 & 0 \end{vmatrix}$$

sont premiers entre eux, puisqu'il est aisé de voir que ceux que l'on obtient en supprimant la deuxième, la troisième et la quatrième colonne sont égaux respectivement à λ_1, λ_2, λ_3.

Donc le réseau proposé est équivalent à celui qu'on en déduit par la substitution (α) et qui s'écrit

$$\begin{bmatrix} \alpha_1\mu_1+\alpha_2\mu_2+\alpha_3\mu_3 & \alpha_1\lambda_2-\alpha_2\lambda_1 & \alpha_1\lambda_3-\alpha_3\lambda_1 & \alpha_2\lambda_3-\alpha_3\lambda_2 \\ \beta_1\mu_1+\beta_2\mu_2+\beta_3\mu_3 & \beta_1\lambda_2-\beta_2\lambda_1 & \beta_1\lambda_3-\beta_3\lambda_1 & \beta_2\lambda_3-\beta_3\lambda_2 \end{bmatrix}$$

ou

$$\begin{bmatrix} \alpha_1\mu_1+\alpha_2\mu_2+\alpha_3\mu_3 & \alpha_1\lambda_2-\alpha_2\lambda_1 & \alpha_1\lambda_3-\alpha_3\lambda_1 & \alpha_2\lambda_3-\alpha_3\lambda_2 \\ \delta & 0 & 0 & 0 \end{bmatrix},$$

qui est évidemment équivalent à

$$\begin{bmatrix} \alpha_1\mu_1+\alpha_2\mu_2+\alpha_3\mu_3 & \delta_1 \\ \delta & 0 \end{bmatrix},$$

c'est-à-dire que la norme du réseau proposé est égale à $\delta\delta_1$, c'est-à-dire à la plus grande commune mesure de

$$(\alpha_1\lambda_2-\alpha_2\lambda_1)\delta, \quad (\alpha_2\lambda_3-\alpha_3\lambda_2)\delta, \quad (\alpha_1\lambda_3-\alpha_3\lambda_1)\delta$$

ou de

$$\alpha_1\beta_2-\alpha_2\beta_1, \quad \alpha_2\beta_3-\alpha_3\beta_2, \quad \alpha_1\beta_3-\alpha_3\beta_1. \qquad \text{C. Q. F. D.}$$

Remarque I. — Le même raisonnement s'applique dans le cas de quatre variables.

La norme du réseau

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix}$$

est alors la plus grande commune mesure de

$$\alpha_1\beta_2 - \beta_1\alpha_2, \quad \alpha_1\beta_3 - \beta_1\alpha_3, \quad \alpha_1\beta_4 - \beta_1\alpha_4,$$
$$\alpha_2\beta_3 - \beta_2\alpha_3, \quad \alpha_2\beta_4 - \beta_2\alpha_4, \quad \alpha_3\beta_4 - \beta_3\alpha_4.$$

Remarque II. — Cette méthode peut servir à la recherche du p. g. c. d. de deux réseaux.

Notation nouvelle. — Les points dont les coordonnées sont entières et satisfont à la congruence

$$ax + by \equiv 0 \pmod{c}, \tag{15}$$

où a, b et c sont entiers, forment un réseau.

En effet, on peut supposer a et b premiers entre eux, car, s'ils ne l'étaient pas, soit D le p. g. c. d. de a, de b et de c, soit D′ le p. g. c. d. de $\frac{a}{D}$ et $\frac{b}{D}$, on pourrait remplacer la congruence (15) par celle-ci :

$$\frac{a}{DD'}x + \frac{b}{DD'}y \equiv 0 \left(\text{mod. } \frac{c}{D}\right).$$

Or, a et b étant premiers entre eux, soit δ le p. g. c. d. de a et de c, on doit avoir

$$y \equiv 0 \pmod{\delta},$$

d'où

$$y = \delta m.$$

Il vient alors

$$\frac{a}{\delta}x + bm \equiv 0 \left(\text{mod. } \frac{c}{\delta}\right),$$

d'où, si k est le nombre des nombres premiers avec $\frac{c}{\delta}$ et plus petits que lui,

$$x + bm\left(\frac{a}{\delta}\right)^{k-1} \equiv 0 \left(\text{mod. } \frac{c}{\delta}\right),$$

d'où

$$x \equiv -b\left(\frac{a}{\delta}\right)^{k-1} m + \frac{c}{\delta} n.$$

Les points en question forment donc le réseau

$$\begin{bmatrix} -b\left(\frac{a}{\delta}\right)^{k-1} & \frac{c}{\delta} \\ \delta & 0 \end{bmatrix},$$

d'où l'on conclut aisément que :

THÉORÈME XI. — *La norme du réseau défini par la congruence* (15), *où a et b sont premiers entre eux, est égale à c.*

THÉORÈME XII. — *Pour qu'un réseau*

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

puisse être représenté par une congruence telle que (15), *il faut et il suffit que* α, β, γ *soient des nombres entiers premiers entre eux.*

En effet, le réseau défini par la congruence (15) s'écrivant

$$\begin{bmatrix} -b\left(\frac{a}{\delta}\right)^{k-1} & \frac{c}{\delta} \\ \delta & 0 \end{bmatrix},$$

je dis d'abord que

(16) $$\delta, \ \frac{c}{\delta}, \ b\left(\frac{a}{\delta}\right)^{k-1}$$

sont premiers entre eux.

En effet :

1° δ, $\frac{c}{\delta}$ et b sont premiers entre eux, car tout nombre qui diviserait δ et b diviserait a et b, qui sont premiers entre eux.

2° δ, $\frac{c}{\delta}$ et $\frac{a}{\delta}$ sont premiers entre eux, parce que $\frac{c}{\delta}$ et $\frac{a}{\delta}$ sont premiers entre eux.

Donc les nombres (16) sont premiers entre eux. C. Q. F. D.

Je dis réciproquement que, si α, β et γ sont premiers entre eux, le réseau

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

peut être représenté par une congruence telle que (15).

Soit en effet Δ le p. g. c. d. de α et de β; soient ξ et n deux nombres tels que

$$\alpha\xi + \beta n = \Delta.$$

Soit

$$\xi_1 = \xi + \lambda\frac{\beta}{\Delta},$$

$$n_1 = n - \lambda\frac{\alpha}{\Delta},$$

d'où

$$\alpha\xi_1 + \beta n_1 = \Delta.$$

ξ et $\frac{\beta}{\Delta}$ étant premiers entre eux, nous choisirons λ de telle façon que ξ_1 soit un nombre premier plus grand que Δ, ce qui est toujours possible, ainsi que Lejeune-Dirichlet l'a démontré, puisque ξ et $\frac{\beta}{\Delta}$ sont premiers entre eux.

Puisque γ et ξ_1 sont premiers avec Δ, il en sera de même de $\gamma\xi_1$.

Cela posé, multiplions les deux équations

$$x = \alpha m + \beta n,$$
$$y = \gamma m$$

respectivement par

$$-\gamma\xi_1 \text{ et } \alpha\xi_1 + \beta n_1 = \Delta$$

et ajoutons; il viendra

$$(\alpha\xi_1 + \beta n_1)y - \gamma\xi_1 x = \beta\gamma(m\xi_1 - n_1 n),$$

d'où

$$(17) \qquad (\alpha\xi_1 + \beta n_1)y - \gamma\xi_1 x \equiv 0 \pmod{\beta\gamma}.$$

Donc le réseau représenté par la congruence (17) divise le réseau donné; mais ils ont même norme $\beta\gamma$, puisque $\alpha\xi_1 + \beta n_1$ et $\gamma\xi_1$ sont premiers entre eux. Donc ils sont équivalents. C. Q. F. D.

Corollaire. — Pour qu'un réseau

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

puisse être représenté par une congruence telle que (15), il faut et il suffit que α, β, γ, δ soient des nombres entiers premiers entre eux.

THÉORÈME XIII. — *Pour qu'un réseau*

$$ax + by \equiv 0 \pmod{c}$$

soit divisible par le réseau

$$a'x + b'y \equiv 0 \pmod{c'},$$

il faut et il suffit que

$$ab' - ba' \equiv c \equiv 0 \pmod{c'}.$$

En effet :

1° Je dis que ces conditions sont suffisantes.

En effet, supposons qu'elles soient remplies; je vais faire voir que deux nombres x et y qui satisfont à la première congruence satisfont également à la seconde.

On a, en effet,

$$(18) \qquad \begin{cases} a'(ax + by) - a(a'x + b'y) = y(a'b - b'a), \\ b'(ax + by) - b(a'x + b'y) = x(b'a - a'b). \end{cases}$$

Or, par hypothèse,

$$ax + by \equiv a'b - b'a \equiv 0 \pmod{c'}.$$

Donc c' divise

$$a(a'x + b'y) \text{ et } b(a'x + b'y).$$

Donc, puisque a et b sont premiers entre eux, il divise $a'x + b'y$.

C. Q. F. D.

2° Je dis que ces conditions sont nécessaires.

En effet, si le second réseau divise le premier, la norme du second

réseau doit diviser celle du premier, c'est-à-dire que

$$c \equiv 0 \pmod{c'}.$$

De plus, soient x et y les coordonnées d'un point du premier réseau qui appartient, par hypothèse, également au second; on aura

$$ax + by \equiv a'x + b'y \equiv 0 \pmod{c'}.$$

Or, on aura pu choisir x et y de telle façon que ces deux nombres soient premiers entre eux (*voir* la démonstration du théorème XII).

Et d'après les équations (18), on aura

$$y(a'b - b'a) \equiv x(a'b - b'a) \equiv 0 \pmod{c'}$$

ou, puisque x et y sont premiers entre eux,

$$a'b - b'a \equiv 0 \pmod{c'}. \qquad \text{C. Q. F. D.}$$

Corollaire I. — Pour que deux réseaux

$$ax + by \equiv 0 \pmod{c},$$
$$a'x + b'y \equiv 0 \pmod{c'}$$

soient équivalents, il faut et il suffit que

$$c = c', \quad ab' - ba' \equiv 0 \pmod{c}.$$

Corollaire II. — Un réseau

$$ax + by \equiv 0 \pmod{c}$$

n'a jamais qu'un diviseur ayant pour norme un diviseur donné de c, γ par exemple.

En effet, soit

$$\alpha x + \beta y \equiv 0 \pmod{\gamma}$$

un diviseur de c ayant pour norme γ; on devra avoir, comme condition de divisibilité,

$$a\beta - \alpha b \equiv 0 \pmod{\gamma},$$

c'est-à-dire que le réseau diviseur serait équivalent à

$$ax + by \equiv 0 \pmod{\gamma}.$$ C. Q. F. D.

Remarque. — Ce corollaire ne serait plus vrai dans le cas où le réseau donné ne pourrait être représenté par une congruence telle que (15).

THÉORÈME XIV. — *Les deux réseaux*

$$ax + by \equiv 0 \pmod{c},$$
$$a'x + b'y \equiv 0 \pmod{c'}$$

ont pour p. g. c. d.

$$ax + by \equiv 0 \pmod{\gamma},$$

où γ est le p. g. c. d. de

$$c, \ c' \text{ et } ab' - ba'.$$

En effet, le p. g. c. d. cherché divisant

$$ax + by \equiv 0 \pmod{c}$$

peut se mettre sous la forme

$$ax + by \equiv 0 \pmod{\gamma},$$

où γ divise c.

Et pour qu'un pareil réseau divise

$$a'x + b'y \equiv 0 \pmod{c'}$$

et

$$ax + by \equiv 0 \pmod{c},$$

il faut et il suffit que

$$c \equiv c' \equiv ab' - ba' \equiv 0 \pmod{\gamma'},$$

c'est-à-dire que la plus grande valeur que l'on puisse donner à γ est le p. g. c. d. de

$$c, \ c' \text{ et } ab' - ba'.$$ C. Q. F. D.

DEUXIÈME PARTIE.

REPRÉSENTATION DES NOMBRES COMPLEXES PAR DES POINTS.

On peut supposer que le point dont les coordonnées sont x et y représente le nombre complexe

$$x + y\sqrt{D};$$

cette représentation est analogue à celle du nombre imaginaire $x + y\sqrt{-1}$. On sait que, dans ce cas, on nomme *module* et *argument* de $x + y\sqrt{-1}$ les quantités

$$\sqrt{x^2 + y^2}, \quad \text{arc tang}\frac{y}{x}.$$

Par analogie, nous nommerons *module* et *argument* de $x + y\sqrt{D}$ les quantités

$$\sqrt{x^2 - y^2 D} \quad \text{et} \quad \frac{1}{\sqrt{-D}}\text{arc tang}\frac{y}{x}\sqrt{-D}.$$

Si D est négatif, ces quantités sont toujours réelles et leur signification géométrique est facile à trouver.

Le module est (si ξ et η sont les coordonnées courantes) le rapport du rayon vecteur qui va de l'origine au point (x, y) au segment déterminé sur ce rayon par l'ellipse

$$\xi^2 - \eta^2 D = 1.$$

L'argument est le double de l'aire comprise entre ce rayon vecteur, cette ellipse et l'axe des x.

Si O (*fig.* 1) est l'origine, OA et OB les axes, C le point (x, y), ABD l'ellipse

$$\xi^2 - \eta^2 D = 1,$$

on a

$$\text{mod C} = \frac{\text{OC}}{\text{OD}},$$

$$\text{arg C} = 2 \times \text{aire ODA}.$$

Supposons maintenant que D soit positif; le module ne sera réel que si

$$x^2 - y^2 D > 0.$$

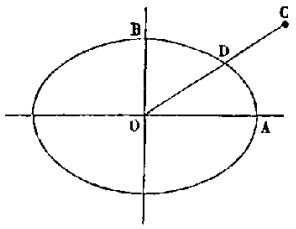
Il sera alors égal au rapport du vecteur OC au segment déterminé sur ce vecteur par l'hyperbole

$$\xi^2 - \eta^2 D = 1.$$

Si $x^2 - y^2 D < 0$, le module sera imaginaire et égal à $\sqrt{-1}$ multiplié par le rapport du vecteur OC au segment déterminé sur ce vecteur par l'hyperbole

$$\xi^2 - \eta^2 D = -1.$$

Fig. 1.



Soit λ l'argument; on aura

$$\frac{y}{x}\sqrt{-D} = \frac{1}{\sqrt{-1}}\,\frac{e^{\lambda\sqrt{D}} - e^{-\lambda\sqrt{D}}}{e^{\lambda\sqrt{D}} + e^{-\lambda\sqrt{D}}},$$

ou, posant $\frac{y}{x}\sqrt{+D} = m$,

$$e^{2\lambda\sqrt{D}} = \frac{1+m}{1-m},$$

ou

$$\lambda = \frac{1}{2\sqrt{D}}\left[L(1+m) - L(1-m)\right].$$

Si m est compris entre -1 et $+1$, λ a une valeur réelle A et une infinité de valeurs imaginaires

$$A + \frac{k\pi}{\sqrt{D}}\sqrt{-1} \quad (k \text{ entier positif ou négatif});$$

on conviendra de donner à λ la valeur réelle quand x sera positif et la

valeur

$$A + \frac{\pi}{\sqrt{-D}}$$

quand x sera négatif.

La valeur de A est positive ou négative selon que m ou $\frac{y}{x}$ est positif ou négatif. Elle est encore égale au double de l'aire comprise entre l'axe des x, le rayon vecteur OC et l'hyperbole $\xi^2 - \eta^2 D = 1$.

Si m n'est pas compris entre -1 et $+1$, c'est-à-dire si

$$x^2 - y^2 D < 0,$$

λ est égal à

$$A + \frac{2k+1}{2}\,\frac{\pi\sqrt{-1}}{\sqrt{D}},$$

où A est réel, k entier, positif ou négatif.

On conviendra de choisir la valeur

$$A + \frac{\pi}{2\sqrt{-D}}$$

quand y sera positif et la valeur

$$A - \frac{\pi}{2\sqrt{-D}}$$

quand y sera négatif.

Le module d'un produit est le produit des modules des facteurs.

L'argument d'un produit est la somme des arguments des facteurs.

En effet, soit

$$\left(x + y\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right) = \left[xx_1 + yy_1 D + \sqrt{D}(xy_1 + yx_1)\right];$$

on a

$$\left[xx_1 + yy_1 D + \sqrt{D}(xy_1 + yx_1)\right] = \frac{1}{\sqrt{-D}}\operatorname{arc\,tang}\frac{xy_1 + yx_1}{xx_1 + yy_1 D} = \frac{1}{\sqrt{-D}}\varphi,$$

d'où

$$\operatorname{tang}\varphi = \frac{(xy_1 + yx_1)\sqrt{-D}}{xx_1 + yy_1 D}.$$

Soit de même

$$\arg\left(x + y\sqrt{D}\right) = \frac{1}{\sqrt{-D}}\psi, \quad \arg\left(x_1 + y_1\sqrt{D}\right) = \frac{1}{\sqrt{-D}}\psi_1,$$

d'où

$$\operatorname{tang}\psi = \frac{y\sqrt{-D}}{x}, \quad \operatorname{tang}\psi_1 = \frac{y_1\sqrt{-D}}{x_1},$$

d'où

$$\operatorname{tang}\varphi = \frac{\frac{y_1\sqrt{-D}}{x_1} + \frac{y}{x}\sqrt{-D}}{1 - \frac{y_1\sqrt{-D}}{x_1}\,\frac{y\sqrt{-D}}{x}} = \frac{\operatorname{tang}\psi + \operatorname{tang}\psi_1}{1 - \operatorname{tang}\psi \operatorname{tang}\psi_1},$$

d'où

$$\varphi = \psi + \psi_1 + m\pi. \qquad \text{C. Q. F. D.}$$

Cette démonstration, où m est entier, positif ou négatif, s'étend au cas où D est positif, et il est facile de voir que, si l'on s'en tient aux conventions faites précédemment, m est toujours égal à 0, à 2 ou à -2.

THÉORÈME XV. — *Tous les nombres entiers complexes dont le module est égal à* 1 *sont les puissances positives et négatives d'un même nombre entier complexe.*

En effet, soient A et B deux nombres entiers complexes de module 1; le nombre complexe

$$A^m B^n,$$

où m et n sont des entiers positifs et négatifs, est entier et de module 1.

L'argument de $A^m B^n$ est égal à

$$m \arg A + n \arg B.$$

Si les arguments de A et de B n'avaient pas de commune mesure, cette expression pourrait prendre toutes les valeurs possibles, c'est-à-dire que tous les points de l'hyperbole

$$x^2 - Dy^2 = 1$$

représenteraient des nombres complexes entiers, *ce qui est absurde*. Donc ces deux arguments ont une commune mesure, et l'expression

$$m \arg A + n \arg B$$

peut être égalée à tous les multiples positifs et négatifs de cette commune mesure.

Si A est celui des nombres entiers complexes de module 1 dont l'argument est positif et le plus petit possible, son argument sera cette commune mesure, de sorte que l'argument de B sera un multiple de celui de A; de sorte que B, qui est un nombre entier complexe *quelconque* de module 1, sera une puissance positive ou négative de A. C. Q. F. D.

Notation nouvelle. — Soient

$$\begin{aligned} A_1 &= a_1 + b_1\sqrt{D}, \\ A_2 &= a_2 + b_2\sqrt{D}, \\ A_3 &= a_3 + b_3\sqrt{D}, \\ A_4 &= a_4 + b_4\sqrt{D} \end{aligned}$$

une série de nombres complexes; nous représenterons le réseau

$$\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{bmatrix}$$

par la notation

$$A_1 m_1 + A_2 m_2 + A_3 m_3 + A_4 m_4.$$

Si l'on a alors (par exemple)

$$C = c + d\sqrt{D},$$

le réseau

$$(c + d\sqrt{D})(A_1 m_1 + A_2 m_2 + A_3 m_3 + A_4 m_4)$$

ne sera autre que le réseau qui avec les anciennes notations s'écrirait

$$\begin{bmatrix} a_1 c + D b_1 d & a_2 c + D b_2 d & a_3 c + D b_3 d & a_4 c + D b_4 d \\ a_1 d + b_1 c & a_2 d + b_2 c & a_3 d + b_3 c & a_4 d + b_4 c \end{bmatrix}.$$

PROBLÈME I. — *Quelle est la norme du réseau*

$$A_1 m_1 + A_2 m_2,$$

où A_1 *et* A_2 *sont deux nombres complexes dont les modules et les arguments sont respectivement* ρ_1 *et* ρ_2, φ_1 *et* φ_2 ?

Cette norme est évidemment égale à

$$\frac{1}{\sqrt{-D}}\rho_1\rho_2\sin\left[\sqrt{-D}(\varphi_1-\varphi_2)\right].$$

PROBLÈME II. — *Trouver les trois coefficients de la forme quadratique*

$$\text{norme}(A_1m_1+A_2m_2).$$

Soit

$$\text{norme}(A_1m_1+A_2m_2)=am_1^2+2bm_1m_2+cm_2^2;$$

on aura évidemment

$$a=\rho_1^2,$$
$$c=\rho_2^2,$$
$$b=\rho_1\rho_2\cos\left[\sqrt{-D}(\varphi_1-\varphi_2)\right].$$

REPRÉSENTATION DES NOMBRES COMPLEXES PAR DES SÉRIES.

Soit α un nombre complexe fractionnaire dont le dénominateur est plus grand que 2 et qui ne peut, par conséquent, satisfaire à une équation de la forme

$$(\psi)\qquad \alpha^m+A_{m-1}\alpha^{m-1}+A_{m-2}\alpha^{m-2}+\ldots+A_1\alpha+A_0=0,$$

où les A sont entiers.

Soit R_m le réseau

$$n_0+\alpha n_1+\alpha^2n_2+\ldots+\alpha^{m-1}n_{m-1}+\alpha^m n_m,$$

où n_0, n_1, n_2, ..., n_m sont les indéterminées, et qui ne peut être équivalent au réseau R_{m-1}, sans quoi une équation de la forme (ψ) se trouverait satisfaite.

Soit

$$R_m=\begin{bmatrix} a_m & b_m \\ c_m & 0 \end{bmatrix}.$$

1° On peut prendre m assez grand pour que $b_m c_m$ soit aussi petit que l'on veut.

En effet, R_m divisant R_{m-1}, on a

$$b_{m-1} c_{m-1} \equiv 0 \pmod{b_m c_m}.$$

Comme d'ailleurs R_m et R_{m-1} ne sont pas équivalents, on a

$$b_m c_m < b_{m-1} c_{m-1} \quad \text{ou} \quad b_m c_m \leq \frac{1}{2} b_{m-1} c_{m-1},$$

ou enfin

$$b_m c_m \leq \frac{1}{2^{m-1}} b_1 c_1,$$

inégalité dont le second membre peut évidemment devenir plus petit que toute quantité donnée.

2° On peut prendre m assez grand pour que c_m soit aussi petit que l'on veut.

En effet, on a évidemment

$$c_m \equiv 0 \pmod{c_{m+1}}.$$

Donc, si c_m ne pouvait pas devenir plus petit que toute quantité donnée, on aurait, à partir d'une certaine valeur de m,

$$\gamma = c_m = c_{m+1} = c_{m+2} = \dots.$$

Or, le réseau R_{m+1} peut s'écrire

$$\begin{bmatrix} a_m & b_m & a_m\lambda + c_m\mu D & b_m\lambda \\ c_m & 0 & a_m\mu + c_m\lambda & b_m\mu \end{bmatrix}$$

si

$$\alpha = \lambda + \mu\sqrt{D}.$$

Donc on a

$$b_m\mu \equiv 0 \pmod{c_{m+1}}.$$

Donc, si l'on suppose que c_m ne peut pas devenir plus petit que γ, on aura

$$c_m \equiv 0 \pmod{\gamma}, \quad b_m\mu \equiv 0 \pmod{\gamma},$$

d'où

$$b_m c_m \equiv 0 \left(\text{mod.} \frac{\gamma^2}{\mu}\right) \quad \text{ou} \quad b_m c_m \geq \frac{\gamma^2}{\mu},$$

ce qui est impossible, puisque $b_m c_m$ peut devenir plus petit que toute quantité donnée.

3° On peut toujours prendre m assez grand pour que l'équidistance des parallèles menées par chacun des points du réseau R_m à la droite $\alpha x + \beta y = 0$ soit aussi petite que l'on veut. En effet, si $\frac{\alpha}{\beta}$ est incommensurable, cette équidistance est nulle; il suffit donc d'envisager le cas où α et β sont commensurables. Soit $\frac{\gamma}{\sqrt{\alpha^2+\beta^2}}$ l'équidistance cherchée pour le réseau

$$R_{m+1} = \begin{bmatrix} a_m & b_m & a_m\lambda + c_m\mu D & b_m\lambda \\ c_m & 0 & a_m\mu + c_m\lambda & b_m\mu \end{bmatrix};$$

γ sera la plus grande commune mesure des quatre quantités

$$\alpha a_m + \beta c_m,\quad \alpha b_m,\quad (\alpha\lambda + \beta\mu) b_m$$

et

$$(\alpha\lambda + \beta\mu) a_m + (\alpha\mu D + \beta\lambda) c_m,$$

de sorte qu'on aura

$$\begin{aligned} \alpha a_m + \beta c_m &\equiv 0 \pmod{\gamma}, \\ \alpha b_m &\equiv 0 \pmod{\gamma}, \\ (\alpha\lambda + \beta\mu) b_m &\equiv 0 \pmod{\gamma}, \\ (\alpha\lambda + \beta\mu) a_m + (\alpha\mu D + \beta\lambda) c_m &\equiv \pmod{\gamma}. \end{aligned}$$

Multipliant la première congruence par la deuxième, la troisième par la quatrième, il vient

$$\begin{aligned} \alpha^2 a_m b_m + \alpha\beta b_m c_m &\equiv 0 \pmod{\gamma^2}, \\ (\alpha\lambda + \beta\mu)^2 a_m b_m + (\alpha\lambda + \beta\mu)(\alpha\mu D + \beta\lambda) b_m c_m &\equiv 0 \pmod{\gamma^2}, \end{aligned}$$

ou, si A et B sont les quotients de α^2 et $(\alpha\lambda + \beta\mu)^2$ par leur plus grande commune mesure,

$$[\alpha\beta B - (\alpha\lambda + \beta\mu)(\alpha\mu D + \beta\lambda) A] b_m c_m \equiv 0 \pmod{\gamma^2}.$$

Donc, puisque $b_m c_m$ tend vers zéro quand m tend vers l'infini, le premier membre de cette congruence, et par conséquent le module γ^2, tendra également vers zéro. C. Q. F. D.

4° Soit γ_m l'équidistance des parallèles menées par chacun des points du réseau R_m à la droite $\alpha x + \beta y = 0$.

On a

$$\gamma_m = f_m\left(\frac{\alpha}{\beta}\right),$$

$f_m\left(\frac{\alpha}{\beta}\right)$ représentant une fonction discontinue et toujours finie de $\frac{\alpha}{\beta}$. Soit Γ_m la plus grande valeur de $f_m\left(\frac{\alpha}{\beta}\right)$. Je dis qu'on peut prendre m assez grand pour que Γ_m soit aussi petit qu'on voudra, plus petit que ε, par exemple.

En effet, soit d'abord $m = 1$; $f_1\left(\frac{\alpha}{\beta}\right)$ ne pourra prendre une valeur supérieure à ε que pour un nombre fini de valeurs de $\frac{\alpha}{\beta}$, à savoir $\frac{\alpha_1}{\beta_1}$, $\frac{\alpha_2}{\beta_2}$, $\ldots$, $\frac{\alpha_n}{\beta_n}$ par exemple.

On peut toujours, d'après ce qu'on vient de voir, prendre m assez grand pour que

$$f_m\left(\frac{\alpha_1}{\beta_1}\right) < \varepsilon, \quad f_m\left(\frac{\alpha_2}{\beta_2}\right) < \varepsilon, \quad \ldots, \quad f_m\left(\frac{\alpha_n}{\beta_n}\right) < \varepsilon.$$

D'ailleurs, si $\frac{\alpha}{\beta}$ n'est égal ni à $\frac{\alpha_1}{\beta_1}$, ni à $\frac{\alpha_2}{\beta_2}$, $\ldots$, ni à $\frac{\alpha_n}{\beta_n}$, on aura

$$f_m\left(\frac{\alpha}{\beta}\right) < f_1\left(\frac{\alpha}{\beta}\right) < \varepsilon.$$

Donc

$$F_m < \varepsilon. \qquad \text{C. Q. F. D.}$$

5° On peut toujours choisir m assez grand pour qu'un point quelconque du plan soit aussi voisin que l'on voudra d'un point du réseau R_m, car la distance d'un point quelconque du plan au point le plus rapproché du réseau R_m est au plus égale à $\frac{2}{3}\Gamma_m$.

Donc un nombre complexe quelconque existant (entier, fractionnaire ou incommensurable) peut être représenté, avec une approximation aussi grande qu'on voudra, par l'expression

$$n_0 + n_1\alpha + n_2\alpha^2 + \ldots + n_m\alpha^m,$$

où les n sont des nombres entiers simples.

THÉORÈME XVI. — *Si une infinité de nombres complexes appartenant à un réseau entier sont en progression géométrique et ont même module, le rapport x de deux quelconques d'entre eux (et en particulier la raison de la progression géométrique) satisfait à une équation de la forme*

$$x^2 + px + 1 = 0,$$

où p est entier.

En effet, si A est un des nombres complexes en question, le réseau donné est un diviseur du réseau

$$R_m = A(n_0 + n_1 x + n_2 x^2 + \ldots + n_m x^m),$$

quelque grand que soit m. Or, si x ne satisfaisait pas à une équation

$$x^2 + px + q = 0$$

(où p et q sont entiers), le réseau R_m aurait une norme aussi petite que l'on veut, ce qui est absurde; de plus,

$$\mathrm{mod}\, Ax = \mathrm{mod}\, A,$$
$$\mathrm{mod}\, x = 1,$$
$$q = 1. \qquad \text{C. Q. F. D.}$$

TROISIÈME PARTIE.

REPRÉSENTATION DES FORMES PAR DES RÉSEAUX.

Définition. — Nous dirons que le réseau

$$(x = am + bn,\ y = cm + dn)$$

représente la forme

$$(am + bn)^2 - D(cm + dn)^2.$$

Il est évident qu'une forme quelconque

$$am^2 + 2bmn + cn^2$$

est représentée par le réseau

$$\begin{bmatrix} \frac{b}{\sqrt{a}} & \sqrt{a} \\ \sqrt{\frac{b^2-ac}{Da}} & 0 \end{bmatrix}.$$

THÉORÈME XVII. — *Le déterminant de la forme représentée par un réseau est égal à* D *multiplié par le carré de la norme de ce réseau.*

En effet, si l'on a

$$(am + bn)^2 - D(cm + dn)^2 = Am^2 + 2Bmn + Cn^2,$$

on aura

$$A = a^2 - Dc^2,$$
$$B = ab - Dcd,$$
$$C = b^2 - Dd^2,$$

d'où

$$B^2 - AC = D(ad - bc)^2. \qquad \text{C. Q. F. D.}$$

Définitions. — 1° On dira que le réseau

$$Am + Bn$$

est directement semblable au réseau

$$(Am + Bn)C,$$

C étant un nombre complexe quelconque.

2° On dira que le réseau

$$Am + Bn$$

est égal au réseau

$$(Am + Bn)C$$

si la norme de C est égale à 1.

3° On dira que le réseau A est directement similaire au réseau B s'il est semblable directement à un réseau C équivalent à B.

4° On dira que le réseau A est symétrique du réseau

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

s'il est égal au réseau

$$\begin{bmatrix} a & b \\ -c & -d \end{bmatrix}.$$

5° On dira que le réseau A est inversement semblable au réseau

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

s'il est directement semblable au réseau

$$\begin{bmatrix} a & b \\ -c & -d \end{bmatrix}.$$

6° On dira que deux formes sont semblables si elles sont dérivées d'une même primitive.

Remarque. — Ces expressions de *similitude* et d'*égalité,* empruntées à la Géométrie, pourront étonner au premier abord; elles se justifieront toutefois si l'on remarque que, si l'on fait la transformation homographique

$$x = x', \quad y = y'\sqrt{-D},$$

les transformés de deux réseaux semblables ou égaux (selon les définitions qui précèdent) seront des réseaux parallélogrammatiques, géométriquement semblables ou égaux.

De même nous dirons que des triangles fondamentaux de deux réseaux semblables ou égaux sont semblables ou égaux, et cette dénomination n'engendrera pas de confusion, parce qu'il ne sera jamais question entre ces figures d'égalité ou de similitude géométrique.

Résultats divers. — Les définitions qui précèdent permettent d'énoncer immédiatement les résultats suivants :

1° Deux réseaux égaux ou symétriques représentent la même forme ou des formes opposées.

2° Deux réseaux équivalents représentent des formes équivalentes.

3° Deux réseaux semblables représentent des formes semblables.

THÉORÈME XVIII. — *Une même forme ne peut être représentée que par des réseaux égaux ou symétriques.*

En effet, pour que les réseaux

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix}$$

soient égaux ou symétriques, il faut et il suffit que

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \lambda & \pm \mathrm{D}\nu \\ \nu & \pm \lambda \end{bmatrix} \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix},$$

où

$$\lambda^2 - \mathrm{D}\nu^2 = 1,$$

ainsi qu'il est aisé de s'en assurer en se reportant à la définition de l'égalité et de la symétrie des réseaux.

On doit avoir, quels que soient m et n,

$$(\alpha m + \beta n)^2 - \mathrm{D}(\gamma m + \delta n)^2 = (\alpha_1 m + \beta_1 n)^2 - \mathrm{D}(\gamma_1 m + \delta_1 n)^2$$

ou, posant $\alpha_1 m + \beta_1 n = x$, $\gamma_1 m + \delta_1 n = y$,

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \lambda & \mu \\ \nu & \rho \end{bmatrix} \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix},$$

d'où

$$\alpha m + \beta n = \lambda x + \mu y, \quad \gamma m + \delta n = \nu x + \rho y;$$

on aura identiquement

$$x^2 - \mathrm{D}y^2 = (\lambda x + \mu y)^2 - \mathrm{D}(\nu x + \rho y)^2,$$

d'où

$$(19 \qquad \begin{cases} \lambda^2 - \mathrm{D}\nu^2 = 1, \\ \lambda\mu - \mathrm{D}\nu\rho = 0, \\ \mu^2 - \mathrm{D}\rho^2 = \mathrm{D}. \end{cases}$$

Il faut faire voir que

$$\mu = \pm D\nu, \quad \rho = \pm \lambda.$$

En effet, des équations (19) on tire

$$\lambda\mu = D\nu\rho, \tag{20}$$

$$\lambda^2\mu^2 = D^2\nu^2\rho^2, \tag{21}$$

$$D\nu^2\mu^2 - D^2\nu^2\rho^2 = D^2\nu^2. \tag{22}$$

De (21) et de (22) nous tirerons

$$(\lambda^2 - D\nu^2)\mu^2 = D^2\nu^2, \tag{23}$$

ou, puisque $\lambda^2 - D\nu^2 = 1$, $\mu^2 = D^2\nu^2$,

$$\mu = \pm D\nu. \tag{24}$$

Remplaçant μ par sa valeur (24) dans l'équation (20), il vient, en divisant par $D\nu$,

$$\lambda = \pm \rho. \qquad \text{C. Q. F. D.}$$

Corollaire. — La forme principale

$$m^2 - Dn^2$$

ne peut être représentée que par l'un des réseaux

$$\begin{bmatrix} \lambda & \pm D\nu \\ \nu & \pm \lambda \end{bmatrix},$$

où

$$\lambda^2 - D\nu^2 = 1.$$

Définitions. — Pour abréger le langage dans ce qui va suivre, nous appellerons *le p d'une forme* la racine carrée de son déterminant divisé par D.

Le m et le μ de la forme

$$ax^2 + 2bxy + cy^2$$

seront respectivement les p. g. c. d. de

$$a,\ 2b,\ c$$

et de

$$a,\ b,\ c.$$

Son e et son ε seront définis par les équations

$$e = \frac{p}{m}, \quad \varepsilon = \frac{p}{\mu}.$$

Le p, le m, le μ, le e et le ε d'un réseau seront le p, le m, le μ, le e et le ε de la forme qu'il représente.

Il est évident que le p d'un réseau n'est autre chose que sa norme.

Le réseau sera dit *propre* ou *impropre* selon qu'il représentera une forme dérivée d'une forme proprement ou improprement primitive, c'est-à-dire selon que son m sera ou non égal à son μ, ou son e à son ε.

THÉORÈME XIX. — *Pour qu'un réseau donné*

$$Am + Bn$$

divise le réseau

$$h\sqrt{D}(Am + Bn),$$

il faut et il suffit que h soit divisible par l'ε du réseau donné.

En effet, supposons que le réseau $Am + Bn$ réduit à sa plus simple expression s'écrive

$$\begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix}.$$

Le réseau

$$h\sqrt{D}(Am + Bn)$$

s'écrira alors

$$h\sqrt{D}\left[\left(\alpha + \gamma\sqrt{D}\right)m + \beta n\right]$$

ou

$$\left(h\gamma D + h\alpha\sqrt{D}\right)m + h\beta\sqrt{D}n.$$

Pour qu'il soit multiple de $Am + Bn$, il faut et il suffit que les équations

$$\begin{aligned} h\gamma D &= \alpha m + \beta n, \\ h\alpha &= \gamma m, \\ 0 &= \alpha m_1 + \beta n_1, \\ h\beta &= \gamma m_1 \end{aligned}$$

donnent pour m, n, m_1, n_1 des valeurs entières, ce qui exige que

$$h\alpha \equiv h\beta \equiv 0 \pmod{\gamma},$$

$$h\frac{\alpha^2 - D\gamma^2}{\gamma} \equiv 0 \pmod{\beta}$$

ou

$$h\alpha\beta \equiv h\beta^2 \equiv h(\alpha^2 - D\gamma^2) \equiv 0 \pmod{\beta\gamma},$$

ou, puisque $p = \beta\gamma$ et que μ est le p. g. c. d. de $\alpha\beta$, β^2 et $\alpha^2 - D\gamma^2$,

$$h\mu \equiv 0 \pmod{p},$$

ou

$$h \equiv 0 \left(\mathrm{mod.}\ \frac{p}{\mu}\right),$$

ou

$$h \equiv 0 \pmod{\varepsilon}. \qquad \text{C. Q. F. D.}$$

Corollaire. — Pour qu'un réseau donné

$$Am + Bn$$

divise le réseau

$$\left(t + u\sqrt{D}\right)(Am + Bn),$$

où t et u sont entiers, il faut et il suffit que

$$u \equiv 0 \pmod{\varepsilon}.$$

THÉORÈME XX. — *Pour qu'un réseau donné*

$$Am + Bn$$

divise (pour une valeur convenablement choisie de t) le réseau

$$\left(\frac{t}{2} + u\sqrt{D}\right)(Am + Bn),$$

où t et u sont entiers, il faut et il suffit que

$$u \equiv 0 \pmod{e}.$$

De plus, pour $u = e$, on devra donner à t une valeur paire ou impaire selon que le réseau donné est propre ou impropre.

En effet, soient encore

$$A = \alpha + \gamma\sqrt{D},$$
$$B = \beta,$$

d'où

$$\left(\frac{t}{2} + u\sqrt{D}\right)(Am + Bn)$$
$$= m\left[\left(u\gamma D + \frac{\alpha t}{2}\right) + \sqrt{D}\left(u\alpha + \frac{t\gamma}{2}\right)\right] + n\beta\left(\frac{t}{2} + u\sqrt{D}\right).$$

Les conditions de divisibilité seront alors que les équations

$$u\gamma D + \frac{\alpha t}{2} = \alpha m + \beta n,$$
$$u\alpha + \frac{t\gamma}{2} = \gamma m,$$
$$\frac{t\beta}{2} = \alpha m_1 + \beta n_1,$$
$$u\beta = \gamma m_1$$

donnent pour m, n, m_1, n_1 des valeurs entières, c'est-à-dire que l'on ait

$$u\beta^2 \equiv 0 \pmod{\beta\gamma},$$
$$2u\alpha\beta \equiv t\beta\gamma \pmod{2\beta\gamma},$$
$$u(\alpha^2 - D\gamma^2) \equiv 0 \pmod{\beta\gamma}.$$

Il est clair que ces conditions seront remplies, soit pour toutes les valeurs paires, soit pour toutes les valeurs impaires de t, toutes les fois que l'on aura

$$u\beta^2 \equiv 2u\alpha\beta \equiv u(\alpha^2 - D\gamma^2) \equiv 0 \pmod{\beta\gamma}$$

ou, puisque m est le p. g. c. d. de β^2, $2\alpha\beta$ et $\alpha^2 - D\gamma^2$, et que $e = \frac{\beta\gamma}{m}$,

toutes les fois que

$$u \equiv 0 \pmod{e}.$$

Supposons que l'on fasse

$$u = e.$$

Si le réseau est propre, $e = \varepsilon$ et

$$e\alpha\beta \equiv 0 \pmod{\beta\gamma},$$

d'où

$$t\beta\gamma \equiv 0 \pmod{2\beta\gamma},$$
$$t \equiv 0 \pmod{2}.$$

Si au contraire le réseau est impropre, on a $e = \frac{\varepsilon}{2}$; donc u n'est pas divisible par ε; donc on n'a pas

$$e\alpha\beta \equiv 0 \pmod{\beta\gamma},$$

et l'on n'a pas non plus, par conséquent,

$$t \equiv 0 \pmod{2}.$$

Le théorème énoncé est donc démontré.

Corollaire. — Pour qu'un réseau

$$Am + Bn$$

soit impropre, il faut et il suffit qu'il existe un réseau

$$\left(\frac{t}{2} + u\sqrt{D}\right)(Am + Bn)$$

qui soit un de ses multiples et où u est un nombre entier, pendant que t est un nombre entier impair.

THÉORÈME XXI. — *Pour qu'un réseau entier* $\left(a + c\sqrt{D}\right)m + bn$ *ait son* ε *égal à* 1, *il faut et il suffit que*

$$a \equiv b \equiv 0 \pmod{c}, \quad \frac{a^2}{c^2} \equiv D \pmod{\frac{b}{c}}.$$

Soit

$$\left(a + c\sqrt{\mathrm{D}}\right)m + bn$$

le réseau donné réduit à sa plus simple expression; pour que son ε soit égal à 1, il faut et il suffit que

$$a^2 - \mathrm{D}c^2 \equiv ab \equiv b^2 \equiv 0 \pmod{bc}.$$

Premier cas. — a, b et c sont premiers entre eux.

Comme on a

$$a \equiv b \equiv 0 \pmod{c},$$

c doit être égal à 1, sans quoi, comme il divise a, b et c, ces trois nombres ne seraient pas premiers entre eux.

Puisque l'on a $c = 1$, les conditions se réduisent à

$$a^2 - \mathrm{D} \equiv 0 \pmod{b}.$$

Second cas. — a, b et c ne sont pas premiers entre eux.

Ce cas se ramène facilement au précédent. En effet, soit d le p. g. c. d. de a, b et c. Soient

$$a = a_1 d, \quad b = b_1 d, \quad c = c_1 d.$$

a_1, b_1, c_1 seront premiers entre eux, et, pour que le réseau

$$\left(a + c\sqrt{\mathrm{D}}\right)m + bn$$

ait un ε égal à 1, il faut et il suffit qu'il en soit de même de

$$\left(a_1 + c_1\sqrt{\mathrm{D}}\right)m + b_1 n,$$

c'est-à-dire que

$$c_1 = 1,$$
$$a_1^2 - \mathrm{D} \equiv 0 \pmod{b_1}.$$

Problème. — *Rechercher quelles sont les transformations qui ramènent une forme à elle-même.*

Autrement dit, rechercher si un réseau est similaire à lui-même.

Cherchons d'abord s'il est directement similaire à lui-même.

Soit $Am + Bn$ le réseau donné, où A et B sont des nombres complexes, m et n les indéterminées; rechercher si ce réseau est équivalent à

$$CAm + CBn,$$

où C représente un nombre complexe indépendant de m et de n.

Je dis que $\mathrm{mod}C = 1$.

En effet, s'il n'en était ainsi, le plus petit module de tous les nombres complexes $CAm + CBn$ serait ou plus grand ou plus petit que le plus petit module de tous les nombres complexes $Am + Bn$, et, par conséquent, les deux réseaux ne sauraient être équivalents. De plus, $C^2Am + C^2Bn$ et en général $C^pAm + C^pBn$ seront équivalents à $Am + Bn$, c'est-à-dire que les nombres $A, AC^2, AC^3, \ldots, AC^p$, qui sont en progression géométrique, appartiennent au réseau $Am + Bn$. Donc C satisfait à une équation de la forme

$$C^2 + pC + 1 = 0,$$

où p est entier.

Premier cas. — p est pair. Soit

$$C = t + u\sqrt{D};$$

on devra avoir

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

Soit $t_1 + u_1\sqrt{D}$ la racine entière de l'équation

$$\mathrm{mod}C = 1$$

dont l'argument est le plus petit; on a

$$C = \left(t_1 + u_1\sqrt{D}\right)^m$$

(où m est entier, positif ou négatif).

Soit $D\varepsilon^2$ le déterminant de la forme donnée, que nous supposerons toujours primitive.

Le réseau donné est un diviseur de

$$\varepsilon\sqrt{D}(Am + Bn)$$

et ne divise aucun des réseaux tels que

$$h\sqrt{D}(Am + Bn),$$

à moins que

$$h \equiv 0 \pmod{\varepsilon}.$$

Pour que $C(Am + Bn)$ soit équivalent à $Am + Bn$, il faut donc et il suffit que

$$u \equiv 0 \pmod{\varepsilon}.$$

Deuxième cas. — p est impair. Soit

$$C = \frac{t + u\sqrt{D}}{2};$$

on devra avoir

$$t^2 - u^2 D = 4.$$

Dans ce cas, t, u et D sont impairs.

En effet, on ne peut avoir t pair, car $t = p$.

Donc $u^2 D$ est impair; donc u et D sont impairs.

De plus,

$$u \equiv 0 \pmod{\varepsilon},$$

car, puisque le réseau $\frac{t + u\sqrt{D}}{2}(Am + Bn)$ est équivalent à $Am + Bn$, $\left(t + u\sqrt{D}\right)(Am + Bn)$ est multiple de $Am + Bn$.

De plus, il faut, d'après ce qu'on a vu plus haut, que le réseau donné représente une forme improprement primitive.

Troisième cas. — Rechercher si le réseau est inversement semblable à lui-même.

Soit $Am + Bn$ le réseau donné; soit $A_1 m + B_1 n$ le réseau que l'on obtient en changeant, dans $Am + Bn$, $\sqrt{D}$ en $-\sqrt{D}$. Soit

$$C(A_1 m + B_1 n)$$

un réseau semblable à $A_1 m + B_1 n$ et équivalent à $Am + Bn$.

Soient ρ et φ le module et l'argument d'un point quelconque du réseau

$Am + Bn$, ρ et $-\varphi$ ceux du point correspondant de $A_1 m + B_1 n$, R et ω ceux de C ($R = 1$). Le réseau

$$C(A_1 m + B_1 n)$$

comprendra le point qui a pour module et pour argument

$$\rho \text{ et } \omega - \varphi.$$

Ce point doit faire partie du réseau $Am + Bn$. Il faut donc et il suffit que ce réseau se reproduise quand on change le module et l'argument ρ et φ de tous ses points en ρ et $\omega - \varphi$.

Le réseau est alors semblable à un réseau

$$am + bn,$$

qui ne change pas quand on change $\sqrt{D}$ en $-\sqrt{D}$, car le réseau

$$(Am + Bn)C,$$

où C a pour module 1 et pour argument $-\frac{\omega}{2}$, contient à la fois les points

$$\rho, \quad \varphi - \frac{\omega}{2},$$

$$\rho, \quad \frac{\omega}{2} - \varphi,$$

c'est-à-dire qu'il ne change pas quand on y change tous les arguments de signe.

DES TRIANGLES AMBIGUS.

On sait que, pour reconnaître l'équivalence de deux formes, on ramène ces deux formes à des formes équivalentes plus simples appelées *formes réduites,* et l'on examine si les formes réduites obtenues sont identiques (si $D < 0$) ou appartiennent à une même période (si $D > 0$).

Dans le cas où $D < 0$, on se sert depuis longtemps d'une représentation géométrique des formes qui ne diffère de celle que je propose dans ce travail que parce que les ordonnées et les abscisses des différents

points des réseaux sont multipliées par certains rapports donnés. Dans ce cas, on sait parfaitement à quoi correspondent géométriquement les formes dites réduites et les formes contiguës; une pareille recherche ne nous conduirait à rien de nouveau; nous nous restreindrons donc au cas où $D < 0$.

Définitions. — Nous appellerons *première asymptote* la droite $\sqrt{D}x = y$, *seconde asymptote* la droite $\sqrt{D}x = -y$, *triangle fondamental* un triangle formé par l'origine et deux points du réseau donné, et ne contenant à son intérieur aucun autre point du réseau (l'aire de ce triangle est égale à la demi-norme), *triangle ambigu* un triangle fondamental tel que la première asymptote soit intérieure à l'angle du triangle qui a son sommet à l'origine et la seconde asymptote extérieure à cet angle.

Par exemple, dans la *fig.* 2, où OX et OY sont les asymptotes, OAB est un triangle ambigu.

Fig. 2.

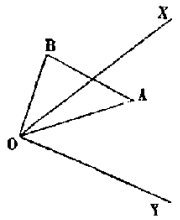
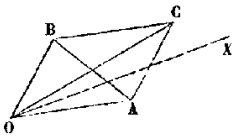


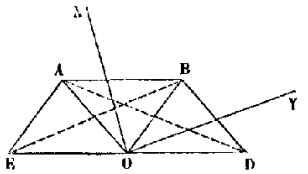
Fig. 3.



Si l'on complète le parallélogramme OABC (*fig.* 3), dont une moitié est un triangle fondamental OAB, les triangles OAC et OBC sont aussi fondamentaux; on les appellera *triangles dérivés* de OAB. De même, OAB sera le primitif de OAC.

Tout triangle OAB a deux primitifs OAD et OBE.

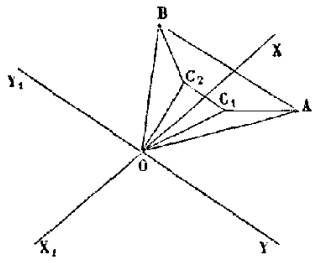
Fig. 4.



THÉORÈME XXII. — *Parmi les triangles fondamentaux d'un réseau, il y en a toujours qui sont ambigus.*

En effet, soient X_1OX, Y_1OY les deux asymptotes; soient A et B deux points du réseau, situés, le premier dans l'angle XOY, le second dans l'angle XOY_1.

Fig. 5.



Supposons que le triangle OAB contienne un certain nombre de points du réseau $C_1, C_2, \ldots, C_n$; supposons que, en faisant tourner une droite OX autour de O depuis OA jusqu'à OB, cette droite rencontre successivement les points $C_1, C_2, \ldots, C_n$; les triangles

$$OAC_1,\ OC_1C_2,\ OC_2C_3,\ \ldots,\ OC_{n-1}C_n,\ OC_nB$$

sont fondamentaux, et l'un au moins d'entre eux contient à l'intérieur de son angle

$$C_kOC_{k+1}$$

la première asymptote et est par conséquent ambigu.

THÉORÈME XXIII. — *Si un triangle est ambigu, un de ses deux dérivés, et un seul, est ambigu.*

Car la première asymptote (OX, *fig.* 2) est comprise soit dans l'angle AOC, soit dans l'angle COB, puisqu'elle l'est dans l'angle AOB.

THÉORÈME XXIV. — *Si un triangle est ambigu, un de ses deux primitifs, et un seul, est ambigu.*

Car la seconde asymptote (OY, *fig.* 3), n'étant pas comprise dans l'angle AOB, est soit dans l'angle BOD, soit dans l'angle AOE, et par conséquent soit dans l'angle AOD, soit dans l'angle BOE; quant à la première asymptote, qui est dans l'angle AOB, elle est à la fois dans les angles AOD et BOE.

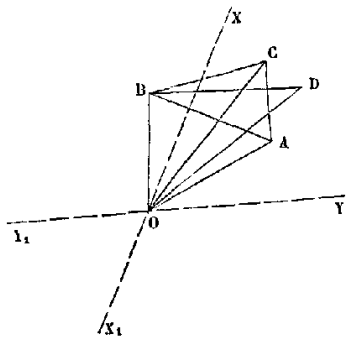
Conséquence. — Il existe une infinité de triangles ambigus disposés en une série continue (période) de telle manière que chacun d'eux soit le dérivé du précédent et le primitif du suivant.

Chaque triangle de la période a un côté commun avec le triangle suivant. Il se trouve ainsi qu'en général plusieurs triangles consécutifs de la période ont un côté commun; nous dirons que ces triangles appartiennent à une série, et la période se trouvera ainsi divisée en séries.

Le dernier triangle d'une série est le premier de la série suivante; un pareil triangle appartenant à deux séries s'appelle *triangle limitrophe;* les triangles limitrophes correspondent aux formes réduites.

THÉORÈME XXV. — *Si un réseau admet deux triangles ambigus, ces triangles appartiennent à une même période.*

Fig. 6.



En effet, soit OD (*fig.* 6) un côté d'un triangle ambigu appartenant à un réseau, et soit une période appartenant au même réseau et dont deux triangles consécutifs soient OAB, OBC. Supposons que le triangle dont fait partie OD n'appartienne pas à cette période. La droite OD devra être comprise entre deux droites, OA et OC par exemple, faisant partie de deux triangles consécutifs de la période.

Or, d'après un théorème dû à Bravais, si OAB et OA_1B_1 sont deux triangles fondamentaux, OA_1 et OB_1 sont toutes deux extérieures ou toutes deux intérieures à l'angle BOA.

Donc, si OB_1D est le triangle dont fait partie OD, OB_1 est extérieur à BOC et intérieur à BOA, et, comme il ne peut être compris dans l'angle

AOC, puisque, le triangle étant ambigu, il doit être dans l'angle XOY, (YY,, XX, étant les asymptotes), il coïncide avec OB.

Le triangle étant fondamental, il faut que le point D soit sur la droite AC. Or il n'y a pas sur cette droite de point du réseau entre A et C; donc le point D doit coïncider soit avec A, soit avec C, c'est-à-dire que le triangle donné coïncide avec l'un des triangles de la période. C. Q. F. D.

THÉORÈME XXVI. — *Les triangles ambigus sont semblables (c'est-à-dire donnent naissance à des réseaux semblables) à un nombre fini de types.*

Soient en effet OAB un triangle ambigu, A et B les deux nombres complexes représentés par les points A et B, a et b leurs modules, $\omega + \frac{i\pi}{2\sqrt{D}}$ la différence de leurs arguments.

La forme représentée par un triangle ambigu s'écrit

$$ax^2 + 2bxy + cy^2,$$

où a et c sont de signes contraires. Or on doit avoir, si Dv^2 est le déterminant de la forme,

$$Dv^2 = b^2 - ac$$

ou, posant $c = -c'$,

$$Dv^2 = b^2 + ac'.$$

Or, il est clair que l'on ne pourra satisfaire à cette condition que par un nombre fini de valeurs entières de b, entières et positives de a et de c'.

Conséquence. — Dans une période de triangles ambigus, les formes représentées par les triangles se reproduisent périodiquement.

La relation avec les fractions continues est facile à établir.

Soit, en effet,

$$(x = am + bn,\ y = cm + dn)$$

le réseau donné; on tire de ces deux équations

$$m = \alpha x + \beta y,$$
$$n = \gamma x + \delta y.$$

Si l'on donne à m et à n les valeurs qui correspondent à un sommet du $k^{\text{ième}}$ triangle ambigu de la période, on a, quand k tend vers l'infini,

$$\lim \frac{m}{n} = \frac{\alpha + \beta\sqrt{D}}{\gamma + \delta\sqrt{D}} = H.$$

Si l'on développe H en fraction continue

$$\alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cdots}},$$

les réduites successives ne sont autre chose que les valeurs de $\frac{m}{n}$ qui correspondent aux triangles limitrophes; quant aux nombres $\alpha_0, \alpha_1, \ldots, \alpha_n$, ce sont les nombres des triangles d'une série moins un.

QUATRIÈME PARTIE.

DE LA MULTIPLICATION COMMUTATIVE DES RÉSEAUX.

Nous avons vu un premier genre de multiplication des réseaux, dont nous avons fait plusieurs fois usage et dont voici la définition :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix}.$$

Cette multiplication n'est pas commutative. De plus, elle ne dépend que des réseaux eux-mêmes et nullement de la valeur du nombre D qui sert de base aux nombres complexes qu'ils représentent. Voici maintenant la définition d'un second genre de multiplication qui est commutative et dépend du nombre D. Nous la désignerons par le nom de *produit second* et par le symbole X_2.

Soient

$$Am + Bn,$$
$$A_1 m_1 + B_1 n_1$$

les deux réseaux à multiplier (A, B, A_1, B_1 sont des nombres complexes) ; nous écrirons

$$(Am + Bn)X_2(A_1m_1 + B_1n_1) = AA_1\mu_1 + AB_1\mu_2 + BA_1\mu_3 + BB_1\mu_4,$$

où μ_1, μ_2, μ_3, μ_4 sont les nouvelles indéterminées.

Le réseau représente évidemment tous les produits des nombres complexes représentés par les deux réseaux facteurs. Il suffit, en effet, de faire

$$\mu_1 = mm_1, \quad \mu_2 = mn_1, \quad \mu_3 = nm_1, \quad \mu_4 = nn_1$$

pour que

$$AA_1\mu_1 + AB_1\mu_2 + BA_1\mu_3 + BB_1\mu_4 = (Am + Bn)(A_1m_1 + B_1n_1).$$

THÉORÈME XXVII. — *Tout réseau* H *qui représente tous les produits des nombres complexes représentés par un réseau* R *par les nombres complexes représentés par un réseau* R_1 *est un diviseur du produit second de* R *et de* R_1.

Soient en effet

$$Am + Bn,$$
$$A_1m_1 + B_1n_1,$$

les deux réseaux R et R_1.

AA_1, AB_1, BA_1, BB_1 feront partie du réseau H, qui devra, par conséquent, diviser

$$AA_1\mu_1 + AB_1\mu_2 + BA_1\mu_3 + BB_1\mu_4. \qquad \text{C. Q. F. D.}$$

THÉORÈME XXVIII. — *Si les différents points des deux réseaux facteurs représentent les différents multiples de deux nombres complexes, les différents points de leur produit second représenteront les différents multiples du produit de ces deux nombres.*

Soient, en effet,

$$A_1m_1 + A_1\sqrt{D}m_2,$$
$$A_2\mu_1 + A_2\sqrt{D}\mu_2$$

les deux réseaux facteurs dont les points représentent les différents multiples de A_1 et de A_2.

Le produit second s'écrira

$$A_1 A_2 M_1 + A_1 A_2 \sqrt{D} N_1,$$

c'est-à-dire que ses différents points représenteront les différents multiples de $A_1 A_2$. C. Q. F. D.

Composition des formes.

L'étude de la multiplication seconde des réseaux va nous permettre de retrouver les théorèmes de Gauss au sujet de la composition des formes quadratiques.

Pour cela, remarquons qu'une forme représentée par le réseau

$$\alpha m + \beta n$$

peut s'écrire

$$(\alpha m + \beta n)(\bar{\alpha} m + \bar{\beta} n),$$

où $\bar{\alpha}$ et $\bar{\beta}$ représentent les nombres complexes conjugués de α et de β. La forme donnée peut être alors indifféremment représentée par le réseau

$$\alpha m + \beta n$$

ou par son symétrique

$$\bar{\alpha} m + \bar{\beta} n.$$

Théorème XXIX. — *Si l'on a, quels que soient m, n, μ et ν,*

$$(\alpha m + \beta n)(\bar{\alpha} m + \bar{\beta} n)(\alpha_1 \mu + \beta_1 \nu)(\bar{\alpha}_1 \mu + \bar{\beta}_1 \nu)$$
$$= (\gamma m\mu + \delta m\nu + \varepsilon n\mu + \zeta n\nu)(\bar{\gamma} m\mu + \bar{\delta} m\nu + \bar{\varepsilon} n\mu + \bar{\zeta} n\nu),$$

l'un quelconque des facteurs du second membre est égal au produit d'une constante par deux des facteurs du premier membre.

Appelons en effet, pour abréger, Γ, $\bar{\Gamma}$ les deux facteurs du second membre, A, $\bar{A}$, B, $\bar{B}$ ceux du premier membre, de telle sorte que

$$A.\bar{A}.B.\bar{B} = \Gamma.\bar{\Gamma}.$$

Si nous considérons un instant μ et ν comme des constantes, les deux

membres deviennent deux formes égales en m et en n. La première est représentée par le réseau

$$\lambda A,$$

où λ est un nombre complexe indépendant de m et de n. La seconde forme est représentée par le réseau Γ. Les deux formes étant égales, les réseaux Γ et λA sont égaux ou symétriques (théorème XVIII). Supposons qu'ils soient égaux, car, s'ils ne l'étaient pas, au lieu de représenter la première forme par le réseau λA, on la représenterait par

$$\overline{\lambda A}.$$

Les deux réseaux étant égaux, l'expression

$$\frac{\Gamma}{\lambda A}$$

est indépendante de m et de n, et il en est évidemment de même de l'expression

$$\frac{\Gamma}{AB}.$$

De même, en considérant m et n comme des constantes, on verrait que $\frac{\Gamma}{AB}$ est indépendant de μ et de ν.

Donc

$$\frac{\Gamma}{AB} = \text{const.} \qquad \text{C. Q. F. D.}$$

THÉORÈME XXX. — *Si une forme est transformable dans le produit de deux autres, son réseau est égal à un multiple du produit second des réseaux des deux autres.*

En effet, dire que la forme

$$(AM + BN)(\overline{A}M + \overline{B}N)$$

est transformable en le produit des deux formes

$$(\alpha m + \beta n)(\overline{\alpha} m + \overline{\beta} n),$$
$$(\alpha_1 \mu + \beta_1 \nu)(\overline{\alpha}_1 \mu + \overline{\beta}_1 \nu),$$

c'est dire que, quand on y fait

$$(21)\qquad \begin{cases} \mathrm{M} = pm\mu + p'm\nu + p''n\mu + p'''n\nu, \\ \mathrm{N} = qm\mu + q'm\nu + q''n\mu + q'''n\nu, \end{cases}$$

elle devient identique à ce produit, quels que soient m, n, μ et ν.

D'après le théorème précédent, on a donc, en donnant à M et à N les valeurs (21),

$$(\alpha m + \beta n)(\alpha_1 \mu + \beta_1 \nu) = \lambda(\mathrm{AM} + \mathrm{BN}),$$

où λ est un nombre complexe indépendant de m, de n, de μ et de ν.

Cette relation, ayant lieu pour toutes les valeurs entières de m, n, μ et ν, est identique, et l'on a

$$(22)\qquad \begin{cases} \alpha\alpha_1 = \lambda(\mathrm{A}p + \mathrm{B}q), \\ \alpha\beta_1 = \lambda(\mathrm{A}p' + \mathrm{B}q'), \\ \beta\alpha_1 = \lambda(\mathrm{A}p'' + \mathrm{B}q''), \\ \beta\beta_1 = \lambda(\mathrm{A}p''' + \mathrm{B}q'''), \end{cases}$$

c'est-à-dire que le réseau

$$\alpha\alpha_1 \mathrm{M}_1 + \alpha\beta_1 \mathrm{M}_2 + \beta\alpha_1 \mathrm{M}_3 + \beta\beta_1 \mathrm{M}_4$$

divise

$$\lambda(\mathrm{AM} + \mathrm{BN}). \qquad \text{C. Q. F. D.}$$

Théorème XXXI. — *Si une forme*

$$(\mathrm{AM} + \mathrm{BN})(\bar{\mathrm{A}}\mathrm{M} + \bar{\mathrm{B}}\mathrm{N})$$

est le résultat de la composition de deux autres

$$(\alpha m + \beta n)(\bar{\alpha} m + \bar{\beta} n),$$
$$(\alpha_1 m_1 + \beta_1 n_1)(\bar{\alpha}_1 m_1 + \bar{\beta}_1 n_1),$$

son réseau est égal au produit second des réseaux des deux formes composantes.

En effet, je dis que λA et λB peuvent être représentés par le réseau

$$\alpha\alpha_1 M_1 + \alpha\beta_1 M_2 + \beta\alpha_1 M_3 + \beta\beta_1 M_4.$$

En effet, on peut choisir les nombres entiers M_1, M_2, M_3, M_4 de telle façon que

$$pM_1 + p'M_2 + p''M_3 + p'''M_4 = 1,$$
$$qM_1 + q'M_2 + q''M_3 + q'''M_4 = 0,$$

puisque, par hypothèse, les déterminants formés avec les nombres p, p', p'', p''' d'une part, q, q', q'', q''' de l'autre, sont premiers entre eux.

Si l'on multiplie ensuite les équations (22) respectivement par

$$M_1,\ M_2,\ M_3,\ M_4,$$

et qu'on les ajoute, il viendra

$$\alpha\alpha_1 M_1 + \alpha\beta_1 M_2 + \beta\alpha_1 M_3 + \beta\beta_1 M_4 = \lambda A.$$

De même, on trouverait

$$\alpha\alpha_1 N_1 + \alpha\beta_1 N_2 + \beta\alpha_1 N_3 + \beta\beta_1 N_4 = \lambda B.$$

Donc les deux réseaux

$$\alpha\alpha_1 m_1 + \alpha\beta_1 m_2 + \beta\alpha_1 m_3 + \beta\beta_1 m_4$$

et

$$\lambda(AM + BN)$$

sont identiques. C. Q. F. D.

Maintenant que la composition des formes est ramenée à la multiplication des réseaux, les théorèmes de Gauss se démontrent aisément.

Dans ce qui va suivre, nous appellerons p_1, m_1, μ_1, e_1, ε_1 les p, m, μ, e et ε de la forme résultante, p', m', μ', e', ε', p'', m'', μ'', e'', ε'' les p, m, μ, e et ε des formes composantes.

THÉORÈME XXXII. — *Le déterminant de la forme qui résulte de la composition de deux autres formes ayant respectivement pour déterminants* Dp'^2 *et* Dp''^2, *et, pour* m, m' *et* m'', *est égal à*

$$Dp_1^2,$$

où p_1 est le p. g. c. d. de

$$m'p'' \text{ et } m''p'.$$

En effet, soient

$$a'x'^2 + 2b'x'y' + c'y'^2,$$
$$a''x''^2 + 2b''x''y'' + c''y''^2$$

les deux formes composantes.

Soient

$$A'x' + B'y', \quad A''x'' + B''y''$$

leurs réseaux, où

$$\begin{aligned} \operatorname{mod} A' &= \rho', & \operatorname{mod} A'' &= \rho'', \\ \operatorname{mod} B' &= \rho'_1, & \operatorname{mod} B'' &= \rho''_1, \\ \arg A' &= \frac{1}{\sqrt{-D}}\varphi', & \arg A'' &= \frac{1}{\sqrt{-D}}\varphi'', \\ \arg B' &= \frac{1}{\sqrt{-D}}\varphi'_1, & \arg B'' &= \frac{1}{\sqrt{-D}}\varphi''_1. \end{aligned}$$

D'après le problème I, p' et p'', c'est-à-dire les normes de $A'x' + B'y'$ et $A''x'' + B''y''$, sont égaux à

$$\frac{1}{\sqrt{-D}}\rho'\rho'_1 \sin(\varphi' - \varphi'_1), \quad \frac{1}{\sqrt{-D}}\rho''\rho''_1 \sin(\varphi'' - \varphi''_1).$$

D'après le théorème X, p_1, c'est-à-dire la norme de

$$A'A''\mu_1 + B'A''\mu_2 + A'B''\mu_3 + B'B''\mu_4,$$

est le p. g. c. d. de

$$\begin{aligned} \alpha_1 &= \text{norme}(A'A''\mu_1 + B'A''\mu_2), \\ \alpha_2 &= \text{norme}(A'A''\mu_1 + A'B''\mu_3), \\ \alpha_3 &= \text{norme}(A'A''\mu_1 + B'B''\mu_4), \\ \alpha_4 &= \text{norme}(B'A''\mu_2 + A'B''\mu_3), \\ \alpha_5 &= \text{norme}(B'A''\mu_2 + B'B''\mu_4), \\ \alpha_6 &= \text{norme}(A'B''\mu_3 + B'B''\mu_4). \end{aligned}$$

Or, d'après les résultats du problème I, on aura

$$\alpha_1\sqrt{-D} = \rho'\rho''\rho'_1\rho''\sin(\varphi' - \varphi'_1) = \rho''^2 p'\sqrt{-D},$$

$$\alpha_2\sqrt{-D} = \rho'\rho''\rho'\rho''_1\sin(\varphi'' - \varphi''_1) = \rho'^2 p''\sqrt{-D},$$

$$\begin{aligned}\alpha_3\sqrt{-D} &= \rho'\rho''\rho'_1\rho''_1\sin(\varphi' + \varphi'' - \varphi'_1 - \varphi''_1)\\ &= \rho'\rho''\rho'_1\rho''_1\left[\sin(\varphi' - \varphi'_1)\cos(\varphi'' - \varphi''_1) + \sin(\varphi'' - \varphi''_1)\cos(\varphi' - \varphi'_1)\right],\end{aligned}$$

$$\begin{aligned}\alpha_4\sqrt{-D} &= \rho'\rho''\rho'_1\rho''_1\sin(\varphi'_1 + \varphi'' - \varphi' - \varphi''_1)\\ &= \rho'\rho''\rho'_1\rho''_1\left[\sin(\varphi' - \varphi'_1)\cos(\varphi'' - \varphi''_1) - \sin(\varphi'' - \varphi''_1)\cos(\varphi' - \varphi'_1)\right],\end{aligned}$$

$$\alpha_5\sqrt{-D} = \rho'_1\rho''\rho'_1\rho''_1\sin(\varphi'' - \varphi''_1) = \rho'^2_1 p''\sqrt{-D},$$

$$\alpha_6\sqrt{-D} = \rho'_1\rho''\rho''^2_1\sin(\varphi' - \varphi'_1) = \rho''^2_1 p'\sqrt{-D},$$

ou, tenant compte des résultats du problème II,

$$\alpha_1\sqrt{-D} = a''p'\sqrt{-D}, \qquad \alpha_4\sqrt{-D} = b''p'\sqrt{-D} - b'p''\sqrt{-D},$$

$$\alpha_2\sqrt{-D} = a'p''\sqrt{-D}, \qquad \alpha_5\sqrt{-D} = c''p'\sqrt{-D},$$

$$\alpha_3\sqrt{-D} = b''p'\sqrt{-D} + b'p''\sqrt{-D}, \qquad \alpha_6\sqrt{-D} = c'p''\sqrt{-D},$$

c'est-à-dire que la norme cherchée divise le p. g. c. d. de

$$a''p',\ 2b''p',\ c''p',$$
$$a'p'',\ 2b'p'',\ c'p'',$$

c'est-à-dire celui de

$$m''p' \text{ et } m'p'', \qquad \text{C. Q. F. D.}$$

et qu'elle est divisée par le p. g. c. d. de

$$a''p',\ b''p',\ c''p',$$
$$a'p'',\ b'p'',\ c'p'',$$

c'est-à-dire de

$$\mu''p',\ \mu'p''.$$

Elle est égale, toutes les fois que $b'p''$ et $b''p'$ contiennent le même nombre de facteurs 2, au p. g. c. d. de

$$m''p',\ m'p'',$$

dans les autres cas au p. g. c. d. de

$$\mu'' p', \ \mu' p'',$$

car le p. g. c. d. de

$$b' p'' + b'' p' \text{ et } b' p'' - b'' p'$$

est égal dans le premier cas à celui de

$$2 b' p'', \ 2 b'' p',$$

dans le second cas à celui de

$$b' p'', \ b'' p'.$$

Cela posé, considérons trois cas.

Premier cas. — Les deux réseaux sont propres. Dans ce cas,

$$m' = \mu', \ m'' = \mu'',$$

et la norme est évidemment égale au p. g. c. d. de

$$m'' p' \text{ et } m' p'',$$

qui se confond avec celui de

$$\mu'' p' \text{ et } \mu' p''.$$

Deuxième cas. — L'un des réseaux est propre, et l'autre impropre. Supposons que la forme

$$a' x'^2 + 2 b' x' y' + c' y'^2$$

soit propre, pendant que la forme

$$a'' x''^2 + 2 b'' x'' y'' + c'' y''^2$$

est impropre.

Dans ce cas, la norme cherchée divise le p. g. c. d. de

$$m' p'', \ m'' p'$$

et est divisée par celui de

$$m' p'' = \mu' p'' \text{ et } \mu'' p'.$$

Je dis que ces deux p. g. c. d. sont les mêmes, c'est-à-dire que $\mu'' p$ contient au moins autant de facteurs 2 que $\mu' p''$.

Car, le second réseau étant impropre, μ'' contient juste autant de facteurs 2 que b'' et que p''.

D'autre part, p' contient au moins autant de facteurs 2 que μ'.

Donc $p'\mu''$ contient au moins autant de facteurs 2 que $\mu' p''$.

Donc le p. g. c. d. de $m' p''$ et $m'' p'$ est égal au p. g. c. d. de $\mu' p''$ et $\mu'' p'$, et par conséquent à la norme cherchée. C. Q. F. D.

Troisième cas. — Les deux réseaux sont impropres.

Dans ce cas, b' et b'' contiennent respectivement autant de facteurs 2 que p' et p''. Donc $b' p''$ et $b'' p'$ contiennent le même nombre de facteurs 2. Donc le p. g. c. d. de

$$b' p'' + b'' p',$$
$$b' p'' - b'' p'$$

est égal à celui de

$$2 b' p'', \quad 2 b'' p'.$$

Donc la norme cherchée est égale au p. g. c. d. de

$$m' p'' \text{ et } m'' p'.$$ C. Q. F. D.

Corollaire. — Si δ, δ' sont les déterminants des deux formes composantes, Δ celui de la forme résultante, les quantités

$$\sqrt{\frac{\Delta}{\delta}} \text{ et } \sqrt{\frac{\Delta}{\delta'}}$$

sont commensurables.

THÉORÈME XXXIII. — *m_1 est égal au produit $m' m''$.*

En effet, m' est le p. g. c. d. de tous les nombres

$$a' x'^2 + 2 b' x' y' + c' y'^2,$$

où x' et y' sont entiers; m'' est celui de tous les nombres

$$a'' x''^2 + 2 b'' x'' y'' + c'' y''^2,$$

où x'' et y'' sont entiers.

Donc $m'm''$ est le p. g. c. d. de tous les nombres

$$(a'x'^2 + 2b'x'y' + c'y'^2)(a''x''^2 + 2b''x''y'' + c''y''^2).$$

Or, tous ces nombres sont susceptibles d'être représentés par la forme résultante; donc ils sont tous divisibles par m_1. Donc

$$m'm'' \equiv 0 \pmod{m_1}.$$

Soient

$$\alpha'x' + \beta'y',$$
$$\alpha''x'' + \beta''y''$$

les réseaux correspondant aux deux formes composantes et

$$P = \alpha'\alpha''\mu_1 + \alpha'\beta''\mu_2 + \alpha''\beta'\mu_3 + \beta'\beta''\mu_4$$

leur produit second, qui représente la forme résultante.

Or

$$\alpha'x' + \beta'y'$$

divise

$$\left(\frac{t'}{2} + e'\sqrt{D}\right)(\alpha'x' + \beta'y'),$$

où t' est entier; donc P, qui est égal à

$$(\alpha'\mu_1 + \beta'\mu_3)\alpha'' + (\alpha'\mu_2 + \beta'\mu_4)\beta'',$$

divisera

$$P\left(\frac{t'}{2} + e'\sqrt{D}\right).$$

De même on verrait que P divise

$$P\left(\frac{t''}{2} + e''\sqrt{D}\right).$$

Il divise donc

$$P\left[\frac{\alpha't' + \alpha''t''}{2} + \sqrt{D}(\alpha'e' + \alpha''e'')\right],$$

où α' et α'' sont des entiers quelconques. Or on peut choisir α' et α'' de telle sorte que

$$\alpha'e' + \alpha''e'' = \delta,$$

δ étant le p. g. c. d. de e' et de e''. Donc P divise

$$P\left(\frac{\tau}{2}+\sqrt{D}\delta\right),$$

où τ est entier.

C'est dire que

$$\delta\equiv 0 \pmod{e_1}.$$

Or, d'après le théorème précédent, p_1 est le p. g. c. d. de $m'p''$ et $m''p'$ ou de $m'm''e''$ et $m'm''e'$, c'est-à-dire que l'on a

$$p_1 = m'm''\delta.$$

On a donc

$$p_1 = m'm''\delta\equiv 0 \pmod{m'm''e_1},$$

ou

$$m_1e_1\equiv 0 \pmod{m'm''e_1},$$

ou

$$m_1\equiv 0 \pmod{m'm''}.$$

Mais, puisque l'on a déjà

$$m'm''\equiv 0 \pmod{m_1},$$

c'est que

$$m_1 = m'm''.$$ C. Q. F. D.

THÉORÈME XXXIV. — *Pour que le produit second de deux réseaux soit impropre, il faut et il suffit que l'un des facteurs soit impropre.*

En effet, pour qu'un réseau A soit impropre, il faut et il suffit qu'il divise un réseau tel que

$$\left(\frac{t}{2}+u\sqrt{D}\right)A,$$

où u est entier et t entier impair.

Or, si A divise

$$\left(\frac{t}{2}+u\sqrt{D}\right)A,$$

AX_2B divisera

$$\left(\frac{t}{2}+u\sqrt{D}\right)AX_2B.$$

La réciproque se démontre aisément. Supposons, en effet, que les deux réseaux composants A′ et A″ soient propres, pendant que le produit $A'X_2A''$ serait impropre : je dis que cette supposition est absurde.

On a, en effet,

$$m_1 = m'm''.$$

Si donc on avait

$$m_1 = 2\mu_1, \quad m' = \mu', \quad m'' = \mu'',$$

on n'aurait pas

$$\mu_1 \equiv 0 \pmod{\mu'\mu''},$$

c'est-à-dire que ε_1 ne diviserait pas le p. g. c. d. de ε' et de ε'', ni par conséquent ε' et ε''.

Or il est clair que

$$\text{réseau A divise réseau } \varepsilon A\sqrt{D},$$

et, par conséquent,

$$\text{réseau } AX_2A' \text{ divise réseau } \varepsilon\sqrt{D}\,AX_2A'.$$

Donc

$$\varepsilon \equiv 0 \pmod{\varepsilon_1};$$

on aura de même

$$\varepsilon' \equiv 0 \pmod{\varepsilon_1}.$$

L'hypothèse que nous avons faite est donc absurde, et le produit second de deux réseaux propres est propre lui-même. C. Q. F. D.

Il est aisé de reconnaître dans les trois théorèmes qui précèdent les résultats énoncés par Gauss dans le Chapitre *De compositione formarum* du premier Volume des *Disquisitiones arithmeticæ*.

CINQUIÈME PARTIE.

THÉORIE DES NOMBRES COMPLEXES IDÉAUX.

Les considérations qui précèdent permettent d'exposer d'une manière simple et concrète la théorie des nombres complexes idéaux, qui corres-

pondent aux formes quadratiques de déterminant D (nous supposons toujours que D n'est divisible par aucun carré).

Pour cela, il faut avoir recours à un mode nouveau de représentation des nombres complexes existants. Le nombre $\lambda + \mu\sqrt{D}$ sera représenté par le réseau

$$\begin{bmatrix} \lambda & \mu D \\ \mu & \lambda \end{bmatrix}.$$

Il est clair que tous les points de ce réseau représentent (conformément à la convention faite dans la deuxième Partie de ce travail) tous les multiples existants de $\lambda + \mu\sqrt{D}$ et que le produit de deux nombres complexes existants est représenté (théorème XXVIII) par le produit second des réseaux qui représentent les deux facteurs. Remarquons enfin que deux nombres complexes existants dont le rapport est une unité complexe sont représentés par le même réseau.

Cela posé, nous appellerons *nombre complexe idéal* tout réseau entier dont l'ε est égal à 1. Le réseau

$$\begin{bmatrix} a & b \\ c & o \end{bmatrix}$$

sera un nombre complexe idéal si

$$a \equiv b \equiv o \pmod{c}, \quad \frac{a^2}{c^2} \equiv D \left(\mathrm{mod.}\ \frac{b}{c}\right).$$

Il est clair que le réseau

$$\begin{bmatrix} \lambda & \mu D \\ \mu & \lambda \end{bmatrix}$$

satisfait à cette définition. Les réseaux qui représentent des nombres complexes existants ne sont donc que des cas particuliers des réseaux que nous venons d'appeler *nombres complexes idéaux*.

Le produit de deux nombres idéaux sera le produit second des réseaux correspondants.

THÉORÈME XXXV. — *Si un nombre idéal est le produit de deux autres, il est divisible par chacun des facteurs.*

En effet, soient

$$R = Am + Bn + Am_1\sqrt{D} + Bn_1\sqrt{D},$$
$$R' = A'm' + B'n' + A'm'_1\sqrt{D} + B'n'_1\sqrt{D}$$

les deux facteurs; le produit second aura pour coefficients

$$AA',\ BB',\ AB',\ A'B,\ AA'\sqrt{D},\ BB'\sqrt{D},\ AB'\sqrt{D},\ A'B\sqrt{D}.$$

Il faut démontrer que chacun de ces huit nombres complexes font partie du réseau R.

Or, soient

$$A' = \alpha' + \alpha''\sqrt{D}, \quad B' = \beta' + \beta''\sqrt{D},$$

où α', α'', β', β'' sont des nombres entiers; on aura

$$AA' = A\alpha' + A\alpha''\sqrt{D}.$$

On obtiendra donc AA' en faisant dans R

$$m = \alpha', \quad n = 0, \quad m_1 = \alpha'', \quad n_1 = 0;$$

on obtiendra de même A'B en faisant

$$m = 0, \quad n = \alpha', \quad m_1 = 0, \quad n_1 = \alpha'',$$

$AA'\sqrt{D}$ en faisant

$$m = \alpha''D, \quad n = 0, \quad m_1 = \alpha', \quad n_1 = 0.$$

Le produit de R et de R' est donc divisible par R. C. Q. F. D.

THÉORÈME XXXVI. — *La norme du produit de deux nombres idéaux est égale au produit de leurs normes.*

Application du théorème XXXII.

THÉORÈME XXXVII. — *Le p. g. c. d. et le p. p. c. m. de deux nombres idéaux sont des nombres idéaux.*

En effet, l'ε des deux réseaux donnés étant égal à 1, ils pourront s'écrire

(théorème XIX)

$$R = Am + Bn + Am_1\sqrt{D} + Bn_1\sqrt{D},$$
$$R' = A'm' + B'n' + A'm'_1\sqrt{D} + B'n'_1\sqrt{D}.$$

Le p. g. c. d. s'écrira alors

$$R_1 = Am + Bn + A'm' + B'n' + Am_1\sqrt{D} + Bn_1\sqrt{D} + A'm'_1\sqrt{D} + B'n'_1\sqrt{D},$$

réseau dont l'ε est évidemment égal à 1.

Soit maintenant

$$R'_1 = A_1M + B_1N$$

le p. p. c. m. cherché; les points A_1 et B_1 faisant partie à la fois de R et de R', $A_1\sqrt{D}$ et $B_1\sqrt{D}$ en feront partie également et par conséquent appartiendront à R'_1.

Donc R'_1 divise $R'_1\sqrt{D}$.

Donc l'ε de R'_1 est égal à 1. C. Q. F. D.

THÉORÈME XXXVIII. — *Si deux nombres idéaux sont premiers entre eux, leur p. p. c. m. est en même temps leur produit second.*

En effet, leur produit second P est divisible par chacun d'eux (théorème XXXV); il est donc divisible par leur p. p. c. m. Q (théorème VIII).

Mais P et Q ont même norme (théorèmes VI et XXXVI). Donc ils sont identiques. C. Q. F. D.

Décomposition d'un nombre idéal en facteurs premiers.

Nous appellerons *nombre idéal premier* tout nombre idéal qui n'est divisible par aucun autre, *nombre idéal unimultiple* tout nombre idéal qui n'est divisible que par un nombre idéal premier, et enfin *nombre idéal second* tout nombre idéal dont la norme est une puissance d'un nombre simple premier.

1° *Décomposition d'un nombre idéal quelconque en facteurs seconds.* —

Nous avons vu (théorème IX) qu'un réseau

$$\mathrm{R} = \begin{bmatrix} ac & b \\ c & o \end{bmatrix},$$

où

$$b = p^{\alpha} q^{\beta} r^{\gamma}, \quad c = p^{\alpha'} q^{\beta'} r^{\gamma'}$$

sont b et c décomposés en facteurs premiers, peut être considéré comme le p. p. c. m. des trois réseaux seconds

$$\mathrm{R}_1 = \begin{bmatrix} ap^{\alpha'} & p^{\alpha} \\ p^{\alpha'} & \mathrm{o} \end{bmatrix}, \quad \mathrm{R}_2 = \begin{bmatrix} aq^{\beta'} & q^{\beta} \\ q^{\beta'} & \mathrm{o} \end{bmatrix}, \quad \mathrm{R}_3 = \begin{bmatrix} ar^{\gamma'} & r^{\gamma} \\ r^{\gamma'} & \mathrm{o} \end{bmatrix}.$$

Les réseaux R_1, R_2 et R_3 sont premiers entre eux; de plus, si R est un nombre idéal, ce sont aussi des nombres idéaux.

En effet, puisque

$$b \equiv \mathrm{o} \pmod{c},$$

on aura

$$\alpha \geq \alpha' \quad \text{et} \quad p^{\alpha} \equiv \mathrm{o} \pmod{p^{\alpha'}}.$$

Du reste, si l'on a

$$a^2 \equiv \mathrm{D} \pmod{b},$$

on aura *a fortiori*

$$a^2 \equiv \mathrm{D} \pmod{p^{\alpha-\alpha'}}.$$

Donc R_1 est un nombre idéal, et il en est de même de R_2 et R_3. Donc, en vertu du théorème XXXVIII,

$$\mathrm{R} = \mathrm{R}_1 \mathrm{X}_2 \mathrm{R}_2 \mathrm{X}_2 \mathrm{R}_3.$$

Le réseau R est donc décomposé en facteurs seconds.

2° *Décomposition d'un nombre idéal second en facteurs équimultiples et réduction de ces facteurs à une puissance d'un nombre idéal premier.*

Soit le nombre idéal second

$$\begin{bmatrix} ap^{\alpha''} & p^{\alpha} \\ p^{\alpha'} & \mathrm{o} \end{bmatrix}.$$

On a

$$\alpha \geq \alpha', \quad \alpha'' \geq \alpha',$$
$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^{\alpha-\alpha'}}.$$

Premier cas. — D n'est pas divisible par p et n'est pas reste quadratique à p.

Dans ce cas, on a $\alpha = \alpha'$, car, si l'on avait $\alpha > \alpha'$, la congruence

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^{\alpha-\alpha'}}$$

exigerait : 1° que $\alpha'' = \alpha'$; 2° que D fût reste quadratique à p. On a donc $\alpha = \alpha'$, d'où

$$ap^{\alpha''} \equiv 0 \pmod{p^{\alpha}}.$$

Le réseau donné peut donc s'écrire

$$\begin{bmatrix} 0 & p^{\alpha} \\ p^{\alpha} & 0 \end{bmatrix},$$

c'est-à-dire qu'il est la puissance $\alpha^{\text{ième}}$ du nombre idéal

$$\begin{bmatrix} 0 & p \\ p & 0 \end{bmatrix},$$

lequel est premier, n'étant divisible par aucun autre nombre idéal.

Deuxième cas. — D est divisible par p.

Comme il n'est divisible par aucun carré, il ne contient le facteur p qu'une fois.

Si donc on a

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^{\alpha-\alpha'}},$$

on ne pourra avoir $\alpha - \alpha' > 1$.

En effet, on ne peut avoir

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^2},$$

soit que $\alpha'' - \alpha' = 0$, car alors le premier membre de la congruence n'est pas divisible par p pendant que le second l'est, soit que $\alpha'' - \alpha' > 0$, car

alors le premier membre est divisible par p^2 pendant que le second ne l'est pas.

On a donc

$$\text{ou bien } \alpha = \alpha', \quad \text{ou bien } \alpha = \alpha' + 1.$$

Si $\alpha = \alpha'$, on a

$$ap^{\alpha''} \equiv 0 \pmod{p^\alpha};$$

si $\alpha = \alpha' + 1$, on a

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \equiv 0 \pmod{p}.$$

Donc $\alpha'' > \alpha'$, ou $\alpha'' = \alpha$ ou $> \alpha$.

Donc

$$ap^{\alpha''} \equiv 0 \pmod{p^\alpha}.$$

Le réseau donné peut donc s'écrire

$$\text{soit } \begin{bmatrix} 0 & p^{\alpha'} \\ p^{\alpha'} & 0 \end{bmatrix}, \quad \text{soit } \begin{bmatrix} 0 & p^{\alpha'+1} \\ p^{\alpha'} & 0 \end{bmatrix}.$$

Or il est aisé de voir que, dans le premier cas, il est la puissance $2\alpha'$, dans l'autre cas la puissance $2\alpha' + 1$, du réseau premier

$$\begin{bmatrix} 0 & p \\ 1 & 0 \end{bmatrix}.$$

Troisième cas. — D n'est pas divisible par p, et est reste quadratique à p. Dans ce cas il y a deux nombres idéaux de norme p, qui sont

$$\rho = \begin{bmatrix} a_1 & p \\ 1 & 0 \end{bmatrix} \quad \text{et} \quad \rho' = \begin{bmatrix} a'_1 & p \\ 1 & 0 \end{bmatrix},$$

où

$$a_1 \equiv -a'_1, \quad a_1^2 \equiv a_1'^2 \equiv D \pmod{p}.$$

Reprenons le réseau

$$R = \begin{bmatrix} ap^{\alpha''} & p^\alpha \\ p^{\alpha'} & 0 \end{bmatrix},$$

où l'on a

$$\alpha > \alpha', \quad ap^{2\alpha''-2\alpha'} \equiv \mathrm{D} \pmod{p^{\alpha-\alpha'}}.$$

On aura $\alpha'' = \alpha'$.

R est le plus petit commun multiple des deux réseaux

$$\rho_\alpha = \begin{bmatrix} a_\alpha & p^\alpha \\ 1 & 0 \end{bmatrix}, \quad \rho'_{\alpha'} = \begin{bmatrix} a'_{\alpha'} & p^{\alpha'} \\ 1 & 0 \end{bmatrix},$$

où

$$a_\alpha \equiv a \equiv a_1, \quad a'_{\alpha'} \equiv a'_1, \quad a_\alpha^2 \equiv a_{\alpha'}'^2 \equiv \mathrm{D} \pmod{p}.$$

D'ailleurs, il est évident :

1° Que ρ_α et $\rho'_{\alpha'}$ sont premiers entre eux et sont des nombres idéaux;

2° Que, par conséquent,

$$\mathrm{R} = \rho_\alpha \rho'_{\alpha'};$$

3° Que ρ_α et $\rho'_{\alpha'}$ sont les puissances α et α' de ρ et de ρ', de telle façon que

$$\mathrm{R} = \rho^\alpha \rho'^{\alpha'}.$$

La décomposition en facteurs premiers est donc toujours possible; du reste, on voit aisément, en se reportant à ce qui précède :

1° Qu'un nombre idéal quelconque n'est décomposable que d'une seule manière en facteurs seconds;

2° Qu'un nombre idéal second n'est décomposable que d'une seule manière en unimultiples;

3° Qu'un unimultiple quelconque n'est décomposable que d'une manière en facteurs premiers.

D'où l'on peut tirer le résultat suivant :

Tout nombre complexe idéal ou existant se décompose d'une manière, et d'une seule, en facteurs premiers idéaux.

FIN DU XLVII^e CAHIER.