BULLETIN DE LA S. M. F.

H. POINCARÉ

Sur la représentation des nombres par les formes

Bulletin de la S. M. F., tome 13 (1885), p. 162-194

<http://www.numdam.org/item?id=BSMF_1885__13__162_1>

Sur la représentation des nombres par les formes;

par H. Poincaré.

(Séance du 28 mars 1885.)

Étant donnée une forme, c'est-à-dire un polynôme, homogène par rapport à plusieurs variables, et à coefficients entiers, donner à ces variables des valeurs entières, telles que la forme devienne égale à un nombre entier donné.

Ce problème est complètement résolu en ce qui concerne les formes quadratiques binaires; mais il y a encore beaucoup à dire à ce sujet, en ce qui concerne les formes plus compliquées.

PREMIÈRE PARTIE.

FORMES BINAIRES.

Représenter un nombre entier par une forme binaire, c'est un problème dont la solution est contenue explicitement ou implicitement dans les travaux de :

MM. Eisenstein (*Journal de Crelle,* t. 28).

Hermite (*Journal de Crelle,* t. 42 et 47).

Kummer (*Journal de Liouville,* 2e série, t. XVI).

Dedekind (*Mémoire sur les nombres entiers algébriques.* Paris, Gauthier-Villars, 1877).

Je crois pourtant qu'il est encore possible d'approfondir et d'éclaircir cette solution.

Méthode générale.

Nous adopterons la terminologie et les notations de M. Dedekind, que je vais rappeler.

Soit une équation algébrique

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

à coefficients entiers. Soient

$$\alpha_1, \ \alpha_2, \ \ldots, \ \alpha_m$$

ses racines. Un nombre entier complexe sera une expression de la forme

$$x_0 + x_1\alpha_1 + x_2\alpha_1^2 + \ldots + x_{m-1}\alpha_1^{m-1}.$$

Nous l'appellerons x pour abréger. Sa norme sera le produit

$$(x_0 + x_1\alpha_1 + x_2\alpha_1^2 + \ldots + x_{m-1}\alpha_1^{m-1})(x_0 + x_1\alpha_2 + x_2\alpha_2^2 + \ldots + x_{m-1}\alpha_2^{m-1})\ldots \times (x_0 + x_1\alpha_m + \ldots + x_{m-1}\alpha_m^{m-1}).$$

Un module sera le système des nombres complexes

$$x^{(1)}m_1 + x^{(2)}m_2 + \ldots + x^{(n)}m_n,$$

où $m_1, m_2, \ldots, m_n$ peuvent prendre toutes les valeurs entières,

positives ou négatives. Nous le représenterons par la notation

$$(2)\qquad \begin{vmatrix} x_0^{(1)} & x_0^{(2)} & \dots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(n)} \\ \dots & \dots & \dots & \dots \\ x_{m-1}^{(1)} & x_{m-1}^{(2)} & \dots & x_{m-1}^{(n)} \end{vmatrix}.$$

Si $n = m$, la norme de ce module sera la valeur de l'expression (2) considérée comme un déterminant.

Un idéal sera un module, tel que $n = m$, et que le produit d'un nombre complexe quelconque appartenant au module, par un nombre entier complexe quelconque, appartienne également au module.

Cela posé, envisageons une forme quelconque

$$F = B_m x^m + B_{m-1} x^{m-1} y + \dots + B_1 x y^{m-1} + B_0 y^m,$$

et supposons qu'on cherche à représenter à l'aide de cette forme le nombre entier N.

L'égalité

$$F = N$$

peut s'écrire, en posant

$$B_m x = x_1,$$

$$x_1^m + B_{m-1} x_1^{m-1} y + B_{m-2} B_m x_1^{m-2} y^2 + \dots + B_1 B_m^{m-2} x_1 y^{m-1} + B_0 B_m^{m-1} y^m = B_m^{m-1} N.$$

Supposons que l'on ait choisi l'équation (1), de telle sorte que

$$A_{m-1} = B_{m-1}, \quad A_{m-2} = B_{m-2} B_m, \quad \dots, \quad A_1 = B_1 B_m^{m-2}, \quad A_0 = B_0 B_m^{m-1}.$$

On cherchera à représenter le nombre $B_m^{m-1} N$ par la forme

$$\Phi = x^m + A_{m-1} x^{m-1} y + A_{m-2} x^{m-2} y^2 + \dots + A_1 y + A_0.$$

On trouvera par exemple que l'on a

$$\Phi = B_m^{m-1} N,$$

en faisant

$$x = a, \quad y = b.$$

On examinera si a est divisible par B_m; s'il ne l'est pas, on rejettera le système de solutions; s'il l'est, on saura que l'on obtient l'égalité

$$F = N$$

en faisant

$$x = \frac{a}{B_m}, \quad y = b.$$

Le problème est donc ramené au suivant : *Représenter un nombre entier par la forme*

$$\Phi = (x + \alpha_1 y)(x + \alpha_2 y)\dots(x + \alpha_m y) = \text{norme}(x + \alpha_1 y).$$

On résoudra le problème plus général : *Représenter un nombre entier par la forme*

$$\Psi = \text{norme}(x_0 + \alpha_1 x_1 + \alpha_1^2 x_2 + \dots + \alpha_1^{m-1} x_{m-1}),$$

qui contient m indéterminées $x_0, x_1, x_2, \dots, x_{m-1}$.

Supposons qu'on l'ait résolu et qu'on ait trouvé que la forme Ψ représente le nombre entier proposé, si l'on y fait

$$x_0 = \beta_0, \quad x_1 = \beta_1, \quad x_2 = \beta_2, \quad x_3 = \beta_3, \quad \dots, \quad x_{m-1} = \beta_{m-1}.$$

Si l'on a

$$\beta_2 = \beta_3 = \dots = \beta_{m-1} = 0,$$

on saura que Φ devient égal au nombre entier proposé quand on y fait

$$x = \beta_0, \quad y = \beta_1,$$

sinon on rejettera la solution.

Le problème est donc ramené au suivant : *Substituer à la place de* $x_0, x_1, \dots, x_{m-1}$ *des nombres entiers, tels que* Ψ *devienne égal à un nombre donné.*

Supposons le problème résolu, soit N le nombre donné. Soit

$$\Psi(x_0, x_1, \dots, x_{m-1}) = N.$$

Le système des nombres complexes

$$(3) \quad (x_0 + \alpha_1 x_1 + \dots + \alpha_1^{m-1} x_{m-1})(m_0 + \alpha_1 m_1 + \dots + \alpha_1^{m-1} m_{m-1}),$$

où

$$m_0, m_1, \dots, m_{m-1}$$

sont des entiers indéterminés, est un idéal de norme N. Ce sera un *idéal principal.* On formera donc tous les idéaux de norme N. Soit

$$(4) \qquad y^{(1)} \mu_1 + y^{(2)} \mu_2 + \dots + y^{(m)} \mu_m$$

l'un de ces idéaux. On doit chercher si c'est un idéal principal : et

dans le cas où c'en est un, on doit chercher à le ramener à la forme (3); quand il sera ramené à cette forme, on aura les valeurs cherchées de $x_0, x_1, \ldots, x_{m-1}$.

La norme d'un nombre complexe contenu dans la formule (3) est égale à

$$\mathrm{N}\,\Psi(m_0, m_1, \ldots, m_{m-1}). \tag{5}$$

Quant à

$$\mathrm{norme}(y^{(1)}\mu_1 + y^{(2)}\mu_2 + \ldots + y^{(m)}\mu_m), \tag{6}$$

c'est une forme de degré m, avec les m indéterminées

$$\mu_1, \mu_2, \ldots, \mu_m.$$

Par la méthode de M. Hermite, on reconnaîtra si les formes (5) et (6) sont équivalentes. Si elles ne le sont pas, (4) n'est pas un idéal principal et il n'y a pas à s'en occuper. Si elles le sont, on passera de l'une à l'autre, en posant

$$\mu_i = \lambda_{i,0} m_0 + \lambda_{i,1} m_1 + \lambda_{i,2} m_2 + \ldots + \lambda_{i\,m-1} m_{m-1}.$$

L'expression (4) deviendra alors

$$\sum_{i=0}^{i=m-1} m_i(y^{(1)}\lambda_{1\,i} + y^{(2)}\lambda_{2,i} + \ldots + y^{(m)}\lambda_{m\,i}). \tag{7}$$

Les expressions (3) et (7) devront être identiques, ce qui donnera pour les valeurs cherchées de $x_0, x_1, \ldots, x_{m-1}$

$$\begin{aligned}
x_0 &= y_0^{(1)}\lambda_{1,0} + y_0^{(2)}\lambda_{2,0} + y_0^{(3)}\lambda_{3,0} + \ldots + y_0^{(m)}\lambda_{m,0},\\
x_1 &= y_1^{(1)}\lambda_{1,0} + y_1^{(2)}\lambda_{2,0} + \ldots\ldots\ldots\ldots + y_1^{(m)}\lambda_{m,0},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
x_{m-1} &= y_{m-1}^{(1)}\lambda_{1,0} + \lambda_{m-1}^{(2)}\lambda_{2,0} + \ldots\ldots\ldots\ldots + y_{m-1}^{(m)}\lambda_{m,0}.
\end{aligned}$$

En résumé, pour chercher si le nombre N peut être représenté par la forme F, on cherchera si le nombre $\mathrm{B}_m^{m-1}\mathrm{N}$ peut être représenté par la forme Ψ; à cet effet, on formera tous les idéaux de norme $\mathrm{B}_m^{m-1}\mathrm{N}$, et si

$$\mathrm{Y} = y^{(1)}\mu_1 + y^{(2)}\mu_2 + \ldots + y^{(m)}\mu_m$$

est l'un d'entre eux, on formera la forme

$$\mathrm{norme}\,\mathrm{Y}$$

et l'on examinera si elle est équivalente à

$$\Psi B_m^{m-1} N$$

et quelle est la substitution qui permet de passer de l'une à l'autre. La connaissance de cette substitution donne immédiatement la solution du problème.

Le problème est donc ramené aux deux questions suivantes :

1° Former tous les idéaux de norme donnée;

2° Reconnaître si deux formes décomposables en facteurs linéaires sont équivalentes.

La deuxième question a été complètement résolue par M. Hermite. Nous n'avons donc à nous occuper pour le moment que de la première.

Formation des idéaux.

Soit un module quelconque

$$x^{(1)} m_1 + x^{(2)} m_2 + \ldots + x^{(n)} m_n.$$

Les nombres complexes $x^{(1)}$, $x^{(2)}$, ..., $x^{(n)}$ forment ce que M. Dedekind appelle la base de ce module. Ce module s'écrit, d'après la notation convenue,

$$(2) \qquad \begin{vmatrix} x_0^{(1)} & x_0^{(2)} & \ldots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \ldots & x_1^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ x_{m-1}^{(1)} & x_{m-1}^{(2)} & \ldots & x_{m-1}^{(n)} \end{vmatrix}.$$

Il est clair qu'on pourrait donner au module une autre base, et par conséquent l'exprimer d'une infinité de manières sous la forme (2). On pourra, par exemple, dans le Tableau (2), ajouter à une colonne quelconque une autre colonne multipliée par un entier constant, ou bien encore supprimer une colonne entièrement formée de zéros. On arrivera ainsi, si $m < n$, à ramener l'expression du module à la forme simple

$$(8) \qquad \begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & b_2 & b_3 & b_4 \\ 0 & 0 & c_3 & c_4 \\ 0 & 0 & 0 & d_4 \end{vmatrix}.$$

J'ai écrit le Tableau (8) comme si m était égal à 4. Il m'arrivera

fréquemment, quand j'écrirai l'expression d'un module, de donner à m une valeur particulière, afin de mieux me faire entendre. Mais il restera entendu que ce que je dirai sera vrai pour toute valeur de m.

Quelles sont les conditions pour que le module

$$(9) \qquad \begin{vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{vmatrix}$$

soit un idéal? Il faut que le produit d'un nombre quelconque de ce module par un nombre entier complexe quelconque (par exemple α_1) fasse partie du module.

Je dis que a, b, c, d, e sont divisibles par f. En effet, si

$$x_0 + x_1\alpha_1 + x_2\alpha_1^2$$

est un nombre complexe appartenant au module (9), on aura

$$x_2 \equiv 0 \pmod{f}.$$

Or les nombres suivants

$$a\alpha_1^2, \quad b\alpha_1 + d\alpha_1^2$$

devront faire partie du module, ce qui exige

$$a \equiv d \equiv 0 \pmod{f}.$$

Il en sera de même de

$$(10) \qquad b\alpha_1^2 + d\alpha_1^3, \quad c\alpha_1 + e\alpha_1^2 + f\alpha_1^3, \quad c\alpha_1^2 + e\alpha_1^3 + f\alpha_1^4.$$

Mais, dans le cas particulier, l'équation (1) s'écrit

$$\alpha_1^3 = A_2\alpha_1^2 - A_1\alpha_1 + A_0,$$

de sorte que les trois nombres complexes (10) s'écrivent

$$dA_0 - dA_1\alpha_1 + (b + A_2 d)\alpha_1^2,$$
$$fA_0 + (c - fA_1)\alpha_1 + (e + A_2 f)\alpha_1^2,$$
$$(fA_2A_0 + eA_0) + (fA_0 - fA_2A_1 - eA_1)\alpha_1 + (c - fA_1 + fA_2^2 + eA_2)\alpha_1^2.$$

S'ils font partie du module (9) on devra avoir

$$b + A_2 d \equiv e + A^2 f \equiv c - fA_1 + fA_2^2 + eA_2 \equiv 0 \pmod{f}.$$

d'où

$$b \equiv e \equiv c \equiv 0 \pmod{f}.$$

Je dis que a et b doivent être divisibles par d.

Car, si le nombre complexe

$$x_0 + x_1\alpha_1 + x_2\alpha_1^2$$

fait partie du module (9), on doit avoir

$$x_1 \equiv e\frac{x_2}{f} \pmod{d}.$$

Or les nombres

$$a\alpha_1,\ b\alpha_1 + d\alpha_1^2$$

font partie du module (9).

On a donc

$$a \equiv 0,\quad b \equiv e\frac{d}{f} \pmod{d},$$

mais $\frac{e}{f}$ est un nombre entier; on a donc

$$b \equiv 0 \pmod{d}.$$

De même, pour que le module (8) soit un idéal, il faut

$$\begin{aligned}
&a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv b_2 \equiv b_3 \equiv b_4 \equiv c_3 \equiv c_4 \equiv 0 \pmod{d_4},\\
&a_1 \equiv a_2 \equiv a_3 \equiv b_2 \equiv b_3 \equiv 0 \pmod{c_3},\\
&a_1 \equiv a_2 \equiv 0 \pmod{b_2}.
\end{aligned}$$

En général, dans un Tableau tel que (8), le dernier chiffre significatif de chaque colonne est sur la diagonale qui va de l'angle supérieur gauche du Tableau à l'angle inférieur droit. Si le module correspondant est un idéal, tous les chiffres d'une colonne seront divisibles par le dernier chiffre significatif de cette colonne, et le dernier chiffre significatif de chaque colonne est divisible par le dernier chiffre significatif de la colonne suivante.

Je dirai qu'un idéal est *simple* si le dernier chiffre significatif de chaque colonne, sauf la première, est l'unité; par exemple, l'idéal suivant

$$\begin{vmatrix} a & b & 0 & 0 \\ 0 & 1 & b & 0 \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

sera simple.

Je dirai qu'il est *primitif* si le dernier chiffre significatif des K premières colonnes est un même nombre a, et si celui des m — K dernières colonnes est l'unité.

Par exemple, l'idéal suivant

$$(11)\qquad \begin{vmatrix} a & 0 & c & 0 & 0 \\ 0 & a & b & c & 0 \\ 0 & 0 & 1 & b & c \\ 0 & 0 & 0 & 1 & b \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

sera primitif.

Envisageons d'abord les idéaux primitifs; je dis qu'un idéal primitif quelconque

$$(12)\qquad \begin{vmatrix} a & \alpha & c & f & l \\ 0 & a & b & e & k \\ 0 & 0 & 1 & d & h \\ 0 & 0 & 0 & 1 & g \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

peut toujours être ramené à la forme (11). En effet, α devant être divisible par a, on remplacera α par zéro en retranchant de la deuxième colonne la première, multipliée par un nombre entier. On peut donc toujours supposer

$$\alpha = 0.$$

Le nombre

$$c + b\alpha_1 + \alpha_1^2$$

faisant partie de l'idéal (12), les nombres

$$c\alpha_1 + b\alpha_1^2 + \alpha_1^3,$$
$$c\alpha_1^2 + b\alpha_1^3 + \alpha_1^4$$

devront aussi en faire partie. Le module (11) sera donc divisible par le module (12); or ces deux modules ont même norme; donc ils sont identiques.

Cherchons maintenant la condition pour que le module (11) soit un idéal. Pour cela, il faut et il suffit que tous ses nombres complexes multipliés par α_1 fassent aussi partie du module (11). Mais il suffit de vérifier ce résultat pour les nombres de la base, et

parmi eux pour les nombres

$$a\alpha_1,\ c\alpha_1^2 + b\alpha_1^3 + \alpha_1^4,$$

car il est tout vérifié pour les autres.

Donc, pour que le module (11) soit un idéal, il faut et il suffit que

$$a\alpha_1^2 \text{ et } c\alpha_1^3 + b\alpha_1^4 + \alpha_1^5$$

fassent partie de ce module.

Comme on a identiquement

$$a\alpha_1^2 = a(c + b\alpha_1 + \alpha_1^2) - b(a\alpha_1) - c(a),$$

le nombre $a\alpha_1^2$ fera toujours partie du module. Occupons-nous donc du nombre

$$c\alpha_1^3 + b\alpha_1^4 + \alpha_1^5.$$

L'équation (1) s'écrivant ici

$$\alpha_1^5 = A_4\alpha_1^4 - A_3\alpha_1^3 + A_2\alpha_1^2 - A_1\alpha_1 + A_0,$$

ce nombre est égal à

$$A_0 + A_1\alpha_1 + A_2\alpha_1^2 + (c - A_3)\alpha_1^3 + (b + A_4)\alpha_1^4.$$

S'il fait partie du module (11), il devra pouvoir se mettre sous la forme

$$a(\lambda_0 + \lambda_1\alpha_1 + \lambda_2\alpha_1^2 + \lambda_3\alpha_1^3 + \lambda_4\alpha_1^4) + (c + b\alpha_1 + \alpha_1^2)(\mu_0 + \mu_1\alpha_1 + \mu_2\alpha_1^2),$$

les λ et les μ étant des nombres entiers.

Si nous convenons d'écrire

$$x_0 + x_1\alpha_1 + \ldots + x_{m-1}\alpha_1^{m-1} \equiv 0 \pmod{a}$$

quand

$$x_0 \equiv x_1 \equiv \ldots \equiv x_{m-1} \equiv 0 \pmod{a},$$

nous aurons

$$\left.\begin{aligned} &A_0 - A_1\alpha_1 + A_2\alpha_1^2(c - A_3)\alpha_1^3 + (b + A_4)\alpha_1^4 \\ &\quad - (c + b\alpha_1 + \alpha_1^2)(\mu_0 + \mu_1\alpha_1 + \mu_2\alpha_1^2) \equiv 0 \end{aligned}\right\} \pmod{a}$$

ou bien

$$\left.\begin{aligned} &A_0 - A_1\alpha_1 + A_2\alpha_1^2 - A_3\alpha_1^3 + A_4\alpha_1^4 - \alpha_1^5 \\ &\quad - (c + b\alpha_1 + \alpha_1^2)(\mu_0 + \mu_1\alpha_1 + \mu_2\alpha_1^2 - \alpha_1^3) \equiv 0 \end{aligned}\right\} \pmod{a},$$

c'est-à-dire que, si l'on envisage la congruence

$$(13) \qquad \xi^5 - A_4\xi^4 + A_3\xi^3 - A_2\xi^2 + A_1\xi - A_0 \equiv 0 \pmod{a}.$$

elle peut se réduire en deux autres, et que l'une d'elles est

$$\xi^2 + b\xi + c \equiv 0 \pmod{a}. \tag{14}$$

Donc, pour que le module (11) soit un idéal, il faut et il suffit que le premier membre de (14) soit un facteur du premier membre de (13), suivant le module a.

Un idéal peut être toujours mis sous la forme

$$x^{(1)}(m_{0,1} + m_{1,1}\alpha_1 + \ldots + m_{m-1,1}\alpha_1^{m-1}) + \ldots + x^{(p)}(m_{0,p} + m_{1,p}\alpha_1 + \ldots + m_{m-1,p}\alpha_1^{m-1}).$$

Les nombres $x^{(1)}$, $x^{(2)}$, ..., $x^{(p)}$ forment alors sa trame.

Par exemple, la trame de l'idéal (11) se composera des deux nombres

$$a \text{ et } c + b\alpha_1 + \alpha_1^2,$$

parce que tout nombre entier complexe faisant partie de l'idéal est la somme d'un multiple du premier et d'un multiple du second.

Un idéal est déterminé quand on connaît sa trame. La trame d'un idéal principal se compose d'un seul nombre.

On déduit de ce qui précède la règle suivante pour former tous les idéaux primitifs.

On remplacera dans le premier membre de (1) α_i par ξ et l'on considérera l'expression ainsi obtenue comme le premier membre d'une congruence suivant un module quelconque a.

Si cette congruence n'est pas irréductible, on envisagera l'un quelconque des facteurs de son premier membre

$$\xi^p + \beta_{p-1}\xi^{p-1} + \beta_{p-2}\xi^{p-2} + \ldots + \beta_1\xi + \beta_0. \tag{15}$$

On y remplacera ξ par α_i et l'on obtiendra ainsi un nombre complexe qui formera avec a la trame de l'idéal cherché.

Il faut ajouter aux idéaux ainsi obtenus les idéaux principaux qui ont pour trame un nombre entier réel a et qui s'écriraient

$$\begin{vmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{vmatrix}.$$

Cherchons à appliquer cette règle au problème suivant :

Former tous les idéaux simples de norme a.

L'idéal cherché devra être de la forme

$$(16)\qquad \begin{vmatrix} a & -\xi & 0 & 0 & 0 \\ 0 & 1 & -\xi & 0 & 0 \\ 0 & 0 & 1 & -\xi & 0 \\ 0 & 0 & 0 & 1 & -\xi \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Quant à ξ, ce sera une racine réelle de la congruence

$$(17)\qquad \xi^5 - A_4\xi^4 + A_3\xi^3 - A_2\xi^2 + A_1\xi - A_0 \equiv 0 \pmod{a}.$$

Tout nombre faisant partie de l'idéal (16) sera de la forme

$$(18)\qquad am_0 + (\alpha_1 - \xi)(m_1 + \alpha_1 m_2 + \alpha_1^2 m_3 + \alpha_1^3 m_4).$$

Si, dans ce nombre, on remplace α_1 par ξ, on obtient un nombre entier divisible par a. Réciproquement, soit

$$x = x_0 + x_1\alpha_1 + x_2\alpha_1^2 + x_3\alpha_1^3 + x_4\alpha_1^4$$

un nombre entier complexe qui devient égal à un nombre entier divisible par a quand on y remplace α_1 par ξ. On aura identiquement

$$\begin{aligned} x = {} & x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3 + x_4\xi^4 \\ & + (\alpha_1 - \xi)[x_1 + x_2(\alpha_1 + \xi) + x_3(\alpha_1^2 + \alpha_1\xi + \xi^2) + x_4(\alpha_1^3 + \alpha_1^2\xi + \alpha_1\xi^2 + \xi^3)], \end{aligned}$$

qui devient égal à l'expression (18) quand on fait

$$\begin{aligned} m_0 &= \frac{1}{a}(x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3 + x_4\xi^4), \\ m_1 &= x_1 + x_2\xi + x_3\xi^2 + x_4\xi^3, \\ m_2 &= x_2 + x_3\xi + x_4\xi^2, \\ m_3 &= x_3 + x_4\xi, \\ m_4 &= x_4. \end{aligned}$$

Le nombre x fait donc partie de l'idéal (16). Nous désignerons donc souvent cet idéal par la notation abrégée

$$(a, \xi).$$

Considérons maintenant l'idéal (11) et supposons d'abord que a soit une puissance d'un nombre premier, et que la congruence

$$(19)\qquad \xi^2 + b\xi + c \equiv 0 \pmod{a}$$

ait deux racines réelles ξ_1 et ξ_2.

Tout nombre faisant partie de l'idéal (11) sera de la forme

$$a(m_0+m_1\alpha_1)+(1+b\alpha_1+c\alpha_1^2)(m_2+m_3\alpha_1+m_4\alpha_1^2)$$

et, si l'on y remplace α_1 par ξ_1 par exemple, on aura

$$a(m_0+m_1\xi_1)+(1+b\xi_1+c\xi_1^2)(m_2+m_3\xi_1+m_4\xi_1^2)\equiv 0 \pmod a.$$

Si donc

$$x=x_0+x_1\alpha_1+x_2\alpha_1^2+x_3\alpha_1^3+x_4\alpha_1^4$$

appartient à l'idéal (11), on aura

$$(20)\qquad \left\{\begin{array}{l} x_0+x_1\xi_1+x_2\xi_1^2+x_3\xi_1^3+x_4\xi_1^4\equiv 0 \\ x_0+x_1\xi_2+x_2\xi_2^2+x_3\xi_2^3+x_4\xi_2^4\equiv 0 \end{array}\right\} \pmod a.$$

Réciproquement, si l'on a les congruences (20), le nombre x appartiendra à l'idéal (11), comme il est aisé de le vérifier.

Supposons que la congruence (19) ait ses racines imaginaires; je dirai encore que, pour que x appartienne à l'idéal (11), il faut et il suffit que les congruences (20) aient lieu. Mais quel sera alors le sens de ces congruences où entrent des imaginaires? On remplacera les congruences (20) par les congruences (21)

$$(21)\qquad \left\{\begin{array}{l} 2x_0+x_1(\xi_1+\xi_2)+x_2(\xi_1^2+\xi_2^2)+x_3(\xi_1^3+\xi_2^3)+x_4(\xi_1^4+\xi_2^4)\equiv 0 \\ x_0(\xi_1+\xi_2)+x_1(\xi_1^2+\xi_2^2)+x_2(\xi_1^3+\xi_2^3)+x_3(\xi_1^4+\xi_2^4)+x_4(\xi_1^5+\xi_2^5)\equiv 0 \end{array}\right\} \pmod a.$$

Si ξ_1 et ξ_2 sont imaginaires, toute fonction symétrique de ξ_1 et ξ_2 sera un nombre entier réel. Les congruences (21) ont donc toujours un sens. Quand ξ_1 et ξ_2 sont réels, les systèmes (20) et (21) sont équivalents. Nous dirons qu'ils le sont encore quand ξ_1 et ξ_2 sont imaginaires. Dans ce sens, on pourra dire que, pour que x appartienne à (11), il faut et il suffit que les congruences (20) soient satisfaites.

Supposons maintenant que a soit un nombre quelconque; la congruence (19) peut avoir plus de deux racines réelles. Si l'on en choisit deux telles que

$$\xi^2+b\xi+c\equiv(\xi-\xi_1)(\xi-\xi_2) \pmod a,$$

ce qui est toujours possible; on trouvera encore que la condition nécessaire et suffisante pour que x fasse partie de (11), c'est que les congruences (20) soient satisfaites.

PROBLÈME. — *Former tous les idéaux primitifs.*

On prendra un nombre quelconque a. On envisagera la congruence

$$(22)\quad F(\xi) = \xi^m - A_{m-1}\xi^{m-1} + A_{m-2}\xi^{m-2} - \ldots \pm A_1\xi \mp A_0 \equiv 0 \pmod a.$$

On choisira m racines réelles ou imaginaires

$$\xi_1, \xi_2, \ldots, \xi_m$$

de cette congruence, de telle sorte que l'on ait identiquement

$$F(\xi) \equiv (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_m) \pmod a.$$

Parmi ces racines $\xi_1, \xi_2, \ldots, \xi_m$, il y en aura d'imaginaires; mais ces imaginaires se répartiront en cycles, de telle façon que tout polynôme entier symétrique de toutes les racines d'un même cycle soit un nombre entier réel. Si donc l'un des cycles est formé, par exemple, des racines

$$\xi_1, \xi_2, \ldots, \xi_q,$$

le produit

$$(\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_q)$$

sera réel.

Cela posé, on choisira au hasard p racines de la congruence (22), par exemple

$$(23)\qquad \xi_1, \xi_2, \ldots, \xi_p,$$

mais de telle sorte que, si une racine imaginaire fait partie du système (23), il en soit de même de toutes les racines du cycle. On formera les congruences

$$(24)\qquad \left.\begin{array}{l} x_0 + x_1\xi_1 + x_2\xi_1^2 + \ldots + x_{m-1}\xi_1^{m-1} \equiv 0 \\ x_0 + x_1\xi_2 + x_2\xi_2^2 + \ldots + x_{m-1}\xi_2^{m-1} \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_0 + x_1\xi_p + x_2\xi_p^2 + \ldots + x_{m-1}\xi_p^{m-1} \equiv 0 \end{array}\right\} \pmod a.$$

Si ces congruences sont satisfaites, le nombre

$$x = x_0 + x_1\alpha_1 + x_2\alpha_1^2 + \ldots + x_{m-1}\alpha_1^{m-1}$$

appartiendra à un certain idéal primitif que je désignerai par la notation abrégée

$$(a, \xi_1, \xi_2, \ldots, \xi_p).$$

On obtiendra de la sorte tous les idéaux primitifs.

Idéaux premiers.

L'idéal

$$(25)\qquad \begin{vmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{vmatrix}$$

est-il un idéal premier? Pour cela il faut d'abord que a soit premier; car, s'il était divisible par un nombre entier b, l'idéal (25) serait divisible par l'idéal

$$\begin{vmatrix} b & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{vmatrix}.$$

Il faut en outre que la congruence

$$(26)\qquad \xi^4 - A_3\xi^3 + A_2\xi^2 - A_1\xi + A_0 \equiv 0 \pmod{a}$$

soit irréductible; car, si l'on avait identiquement, par exemple,

$$\xi^4 - A_3\xi^3 + A_2\xi^2 - A_1\xi + A_0 \equiv (\xi^2 + b\xi + c)(\xi^2 + b'\xi + c') \pmod{a},$$

l'idéal (25) serait divisible par l'idéal

$$\begin{vmatrix} a & 0 & c & 0 \\ 0 & a & b & c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Ces conditions sont suffisantes. Pour que (25) soit premier, il faut et il suffit que a soit premier et que la congruence (26) soit irréductible.

A part les idéaux premiers ainsi trouvés, je dis que tout idéal premier est primitif. Je dis que l'idéal

$$(27)\qquad \begin{vmatrix} abc & dba & eba & ha & ma \\ 0 & ab & fba & ka & na \\ 0 & 0 & ab & la & pa \\ 0 & 0 & 0 & a & qa \\ c & 0 & 0 & 0 & a \end{vmatrix}$$

ne peut être premier.

1° Il est divisible par

$$\begin{vmatrix} a & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 0 & a \end{vmatrix}.$$

Pour qu'il soit premier, il faut donc d'abord

$$a = 1.$$

Supposons cette condition remplie.

2° Il est divisible par l'idéal

$$\begin{vmatrix} b & 0 & 0 & h & 0 \\ 0 & b & 0 & k & h \\ 0 & 0 & b & l & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}. \tag{29}$$

En effet, les nombres

$$b(\alpha_1 + d)\alpha_1,\ (\alpha_1^3 + l\alpha_1^2 + k\alpha_1 + h)\alpha_1$$

devant faire partie de l'idéal (27), cet idéal divise

$$\begin{vmatrix} bc & bd & 0 & h & 0 \\ 0 & b & bd & k & h \\ 0 & 0 & b & l & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}. \tag{28}$$

(Je tiens compte de la condition $a = 1$.)

Mais (27) et (28) ont même norme; donc ils sont identiques. Or il est clair que (29) divise (28).

Donc (27) n'est pas premier. C. Q. F. D.

Considérons donc un idéal primitif quelconque

$$\begin{vmatrix} a & 0 & c & 0 \\ 0 & a & b & c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}. \tag{30}$$

Que faut-il pour qu'il soit premier?

Il faut d'abord que a soit premier; car, si a était divisible par p,

(3o) serait divisible par

$$\begin{vmatrix} p & 0 & c & 0 \\ 0 & p & b & c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Il faut ensuite que la congruence

$$\xi^2 + b\xi + c \equiv 0 \pmod{a},$$

soit irréductible; car, si l'on avait, par exemple,

$$\xi^2 + b\xi + c \equiv (\xi + \xi_1)(\xi + \xi_2) \pmod{a}$$

(3o) serait divisible par

$$\begin{vmatrix} a & \xi_1 & 0 & 0 \\ 0 & 1 & \xi_1 & 0 \\ 0 & 0 & 1 & \xi_1 \\ 0 & 0 & 0 & 1 \end{vmatrix};$$

ces conditions sont suffisantes.

Problème. — *Former tous les idéaux premiers.*

On égalera a à un nombre premier P quelconque; on décomposera le premier membre de la congruence (22) en facteurs irréductibles. Soit

$$\xi^p + a_{p-1}\xi^{p-1} + a_{p-2}\xi^{p-2} + \ldots + a_1\xi + a_0 \tag{31}$$

l'un de ces facteurs. Supposons que, décomposé en facteurs imaginaires, il s'écrive

$$(\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_p),$$

l'idéal

$$(\mathrm{P}, \xi_1, \xi_2, \ldots, \xi_p)$$

sera premier, et l'on obtiendra de la sorte tous les idéauxpremiers.

Tous les nombres appartenant à cet idéal seront compris dans la formule

$$\mathrm{P}(\mathrm{N}_0 + \alpha_1\mathrm{N}_1 + \ldots + \alpha_1^{p-1}\mathrm{N}_{p-1}) + (\alpha_1^p + a_{p-1}\alpha_1^{p-1} + \ldots + a_1\alpha_1 + a_0)(\mathrm{N}_p + \mathrm{N}_{p+1}\alpha_1 + \ldots + \mathrm{N}_{m-1}\alpha_1^{m-p-1}),$$

où les N sont des entiers indéterminés.

La trame de l'idéal se composera des deux nombres

$$P \text{ et } \alpha_1^p + a_{p-1}\alpha_1^{p-1} + \ldots + a_1\alpha_1 + a_0.$$

Puissances d'un idéal premier.

Envisageons l'idéal premier que je viens de définir.

Envisageons la congruence

$$\xi^m - A_{m-1}\xi^{m-1} + \ldots \pm A_0 \equiv 0 \pmod{P^\lambda}. \tag{32}$$

L'un des facteurs irréductibles de cette congruence sera congru (module P) à

$$\xi^p + a_{p-1}\xi^{p-1} + a_{p-2}\xi^{p-2} + \ldots + a_0.$$

Or, on a pu choisir (31) d'une façon arbitraire, pourvu que a_{p-1}, a_{p-2}, ..., a_0 donnent certains restes à P. On aura donc pu le choisir de telle façon que ce soit un facteur irréductible de la congruence (32).

Cela posé, la puissance $\lambda^{\text{ième}}$ de l'idéal premier considéré qui a pour trame

$$P \text{ et } \alpha_1^p + a_{p-1}\alpha_1^{p-1} + \ldots + a_1\alpha_1 + a_0$$

aura pour trame

$$P^\lambda,\ (\alpha_1^p + a_{p-1}\alpha_1^{p-1} + \ldots + a_1\alpha_1 + a_0)^\lambda$$

et l'ensemble des nombres

$$P^\mu(\alpha_1^p + a_{p-1}\alpha_1^{p-1} + \ldots + a_1\alpha_1 + a_0)^{\lambda-\mu}. \tag{33}$$

L'un des communs diviseurs des nombres compris dans l'expression (33), où

$$\mu = 1,\ 2,\ \ldots,\ \lambda - 1,$$

sera

$$\alpha_1^p + a_{p-1}\alpha_1^{p-1} + \ldots + a_0 = \Pi.$$

Donc la puissance $\lambda^{\text{ième}}$ cherchée sera divisible par l'idéal (34), dont tous les nombres sont donnés par la formule

$$P^\lambda(N_0 + \alpha_1 N_1 + \ldots + \alpha_1^{p-1} N_{p-1}) + P(N_p + N_{p+1}\alpha_1 + \ldots + N_{m-1}\alpha_1^{m-p-1}).$$

Or elle a même norme que cet idéal. Elle est donc identique à cet idéal.

Multiplication des idéaux premiers entre eux.

Tout idéal primitif ou non primitif peut être considéré à la fois comme le produit et comme le plus petit commun multiple d'un certain nombre d'idéaux primitifs premiers entre eux et puissances d'un idéal premier.

Nous savons maintenant former toutes les puissances d'un idéal premier. Comment maintenant multiplier entre elles deux pareilles puissances premières entre elles? Soient

$$(35)\qquad \begin{vmatrix} p^\lambda & 0 & b & 0 & 0 & 0 \\ 0 & p^\lambda & a & b & 0 & 0 \\ 0 & 0 & 1 & a & b & 0 \\ 0 & 0 & 0 & 1 & a & b \\ 0 & 0 & 0 & 0 & 1 & a \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

$$(36)\qquad \begin{vmatrix} p^\mu & 0 & 0 & e & 0 & 0 \\ 0 & p^\mu & 0 & d & e & 0 \\ 0 & 0 & p^\mu & c & d & e \\ 0 & 0 & 0 & 1 & c & d \\ 0 & 0 & 0 & 0 & 1 & c \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

les deux puissances à multiplier entre elles. Soit $\mu < \lambda$ et supposons les deux puissances premières entre elles; on devra avoir identiquement

$$\begin{aligned} &A_6 - A_5\xi^5 + A_4\xi^4 - A_3\xi^3 + A_2\xi^2 - A_1\xi + A_0 \\ &\equiv (\xi^2 + a\xi + b)(\xi^3 + c\xi^2 + d\xi + e)(\xi - \lambda) \pmod{p^\lambda}. \end{aligned}$$

Le produit aura pour trame

$$p^{\lambda+\mu},\ p^\mu(\alpha_1^2 + \alpha_1 a + b),\ p^\lambda(a_1^3 + c\alpha_1^2 + d\alpha_1 + e)$$

et

$$(\alpha_1^2 + \alpha_1 a + b)(\alpha_1^3 + c\alpha_1^2 + d\alpha_1 + e) = \alpha_1^5 + k\alpha_1^4 + l\alpha_1^3 + m\alpha_1^2 + n\alpha_1 + q.$$

Il aura pour norme

$$p^{2\lambda+3\mu}.$$

Envisageons le module

$$(37)\qquad \begin{vmatrix} p^\lambda & 0 & bp^\mu & 0 & 0 & q \\ 0 & p^\lambda & ap^\mu & bp^\mu & 0 & n \\ 0 & 0 & p^\mu & ap^\mu & bp^\mu & m \\ 0 & 0 & 0 & p^\mu & ap^\mu & l \\ 0 & 0 & 0 & 0 & p^\mu & k \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Il sera divisible par (35) et par (36), et par conséquent par leur plus petit commun multiple qui est leur produit. De plus il aura même norme que leur produit. Donc ce sera leur produit.

Dans le cas particulier $\lambda = \mu$, (37) se réduit à l'idéal primitif

$$\begin{vmatrix} p^\lambda & 0 & 0 & 0 & 0 & q \\ 0 & p^\lambda & 0 & 0 & 0 & n \\ 0 & 0 & p^\lambda & 0 & 0 & m \\ 0 & 0 & 0 & p^\lambda & 0 & l \\ 0 & 0 & 0 & 0 & p^\lambda & k \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

On ferait de même pour multiplier entre eux plus de deux idéaux puissances d'un idéal premier.

Pour nous résumer et pour donner des résultats un énoncé simple, nous allons donner quelques définitions.

$F(\alpha_1)$ sera l'expression

$$\alpha_1^m - A_{m-1}\alpha_1^{m-1} + A_{m-2}\alpha_1^{m-2} - \ldots \pm A_0,$$

qui est nulle, comme on le sait, si l'on remplace α_1 par sa valeur tirée de l'équation (1).

Nous dirons qu'un nombre complexe

$$H_1 = \alpha_1^\mu + a_{\mu-1}\alpha_1^{\mu-1} + \ldots + a_0$$

est un facteur du nombre complexe

$$H_2 = \alpha_1^\nu + b_{\nu-1}\alpha_1^{\nu-1} + \ldots + b_0,$$

suivant le module B, si l'on veut trouver un nombre complexe

$$K = \alpha_1^{\nu-\mu} + c_{\nu-\mu-1}\alpha_1^{\nu-\mu-1} + \ldots + c_0$$

tel que

$$H_2 - H_1 K$$

soit divisible par B.

De même nous dirons que H_1 est un facteur de $F(\alpha_1)$ suivant le module B, si l'on peut trouver un nombre complexe

$$K' = \alpha_1^{m-\mu} + c'_{m-\mu-1}\alpha_1^{m-\mu-1} + \ldots + c'_0$$

tel que

$$F(\alpha_1) - H_1 K'$$

soit divisible par B.

Règle pour former tous les idéaux dont la norme est une puissance h d'un nombre premier p.

Soient

H_1 un facteur de $F(\alpha_1)$, suivant le module p^h,
H_2 un facteur de H_1, ...
H_n un facteur de H_{n-1}.

Soient $\mu_1, \mu_2, \ldots, \mu_n$ les ordres de $H_1, H_2, \ldots, H_n$.
Soit

$$\lambda_1, \lambda_2, \ldots, \lambda_n, \lambda$$

une série de nombres entiers croissants, tels que

$$\lambda_1(m-\mu_1) + \lambda_2(\mu_1-\mu_2) + \ldots + \lambda_n(\mu_{n-1}-\mu_n) + \lambda\mu_n = h.$$

Le module dont tous les nombres complexes sont compris dans la formule

$$(38)\quad \left\{\begin{array}{l} P\,p^{\lambda_1}H_1(N_m + N_{m-1}\alpha_1 + \ldots + N_{\mu_1+1}\alpha_1^{m-\mu_1-1}) \\ \quad + p^{\lambda_2}H_2(N_{\mu_1} + N_{\mu_1-1}\alpha_1 + \ldots + N_{\mu_2+1}\alpha_1^{\mu_1-\mu_2-1}) \\ \quad + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \quad + p^{\lambda_n}H_n(N_{\mu_{n-1}} + N_{\mu_{n-1}-1}\alpha_1 + \ldots + N_{\mu_n+1}\alpha_1^{\mu_{n-1}-\mu_n-1}) \\ \quad + p^{\lambda}(N_{\mu_n} + N_{\mu_n-1}\alpha_1 + \ldots + N_1\alpha_1^{\mu_n-1}), \end{array}\right.$$

où les N sont des entiers indéterminés, sera un idéal de norme p^h et de plus on obtient par ce procédé tous les idéaux de norme p^h.

Il en résulte que le nombre des idéaux de norme p^h est fini; car $F(\alpha_1)$ n'admet qu'un nombre fini de facteurs H_1 suivant le module p^h, H_1 n'admet qu'un nombre fini de facteurs H_2 suivant le module p^h, ...

Il est vrai qu'on peut remplacer respectivement

$$H_1, H_2, \ldots, H_n$$

par

$$H_1 + p^h K_1,\ H_2 + p^h K_2,\ \ldots,\ H_n + p^h K_n,$$

$K_1, K_2, \ldots, K_n$ étant des nombres complexes quelconques d'ordre $\mu_1 - 1, \mu_2 - 1, \ldots, \mu_n - 1$, sans que ces nombres cessent d'être facteurs les uns des autres et de $F(\alpha_1)$ suivant le module p^h. Mais, en faisant cette substitution, on ne change pas l'idéal correspondant.

Remarquons que l'on peut disposer de $K_1, K_2, \ldots, K_n$, de telle sorte :

1° Que H_1 soit divisible par H_2, H_2 par H_3, ..., H_{n-1} par H_n;

2° Que H_1 soit un facteur de $F(\alpha_1)$ non seulement par rapport au module p^h, mais par rapport au module p^k, k étant aussi grand qu'on voudra.

Supposons, pour plus de simplicité, que l'on ait disposé ainsi de $K_1, K_2, \ldots, K_n$. Soit à décomposer en facteurs premiers un idéal dont la norme est p^h.

Supposons (ce que nous pouvons toujours faire, ainsi qu'on vient de le voir) que H_2 divise H_1, H_3 divise H_2, ..., H_n divise H_{n-1}.

Soit

$$H_{n-1} = H_n K_{n-1}, \quad H_{n-2} = H_{n-1} K_{n-2}, \quad \ldots, \quad H_1 = H_2 K_1.$$

L'idéal (38), qu'il s'agit de décomposer en facteurs premiers, a pour trame

$$p^{\lambda}, p^{\lambda_n} H_n, p^{\lambda_{n-1}} H_{n-1}, \ldots, p^{\lambda_2} H_2, p^{\lambda_1} H_1.$$

Il sera le produit des idéaux primitifs qui ont respectivement pour trames

$$p^{\lambda_1}, (p^{\lambda_2 - \lambda_1}, K_1), (p^{\lambda_3 - \lambda_1}, K_2), \ldots, (p^{\lambda_n - \lambda_1}, K_{n-1}), (p^{\lambda - \lambda_1}, H_n).$$

Il reste à décomposer chacun de ces idéaux primitifs en facteurs premiers.

Envisageons le premier de ces idéaux, à savoir celui qui a pour trame p^{λ_1} : c'est la puissance λ_1 de celui qui a pour trame p; pour obtenir les facteurs premiers de cet idéal, envisageons la congruence

$$\xi^m - A_{m-1}\xi^{m-1} + \ldots \pm A_0 \equiv 0 \pmod{p}. \tag{39}$$

Décomposons-la en facteurs irréductibles et supposons que, si l'on remplace dans ces facteurs ξ par α_1, ils deviennent des nombres complexes $h_1, h_2, \ldots, h_q$. L'idéal dont la trame est p aura pour facteurs premiers les idéaux dont la trame est respectivement

$$(p, h_1), (p, h_2), \ldots, (p, h_q).$$

Envisageons maintenant l'idéal dont la trame est

$$p^{\lambda_2-\lambda_1}, k_1 :$$

ce sera la puissance $\lambda_2 - \lambda_1$ de l'idéal dont la trame est

$$p, k_1.$$

Soit

$$k_1 = \alpha_1^\nu + a_{\nu-1}\alpha_1^{\nu-1} + \ldots + a_0.$$

Considérons les facteurs irréductibles de la congruence

$$\xi^\nu + a_{\nu-1}\xi^{\nu-1} + \ldots + a_0 \equiv 0 \pmod{p}$$

et supposons que, quand on y remplace, ξ par α_1, ils deviennent des nombres complexes

$$h'_1, h'_2, \ldots, h'_q.$$

Les facteurs premiers de l'idéal dont la trame est

$$p, k_1$$

seront es idéaux dont les trames sont respectivement

$$(p, h'_1), (p, h'_2), \ldots, (p, h'_q).$$

On opérerait de même pour les autres idéaux primitifs, de telle sorte que l'idéal (38) se trouvera décomposé en facteurs premiers.

Cas exceptionnels.

1° La congruence (39) est irréductible.

Dans ce cas il n'y a pas d'idéal dont la norme est p^h si h n'est pas divisible par m; il n'y en a qu'un si h est divisible par m : c'est celui dont la trame est $p^{\frac{h}{m}}$ et c'est la puissance $\frac{h}{m}$ de l'idéal dont la trame est p qui est premier.

2° La congruence (39) a des racines multiples.

Dans tout ce qui précède, on a supposé implicitement que la

congruence (39) n'avait pas de racine multiple. Remontons en effet jusqu'au point où il s'est agi de trouver la puissance $\lambda^{\text{ième}}$ d'un idéal premier donné.

L'un des facteurs irréductibles de la congruence (32), ai-je dit, est congrue à (31) (mod P). Cela ne serait plus vrai si la congruence (32) ou, ce qui revient au même, la congruence (39) avait des racines multiples.

Ainsi la congruence

$$\xi^2 - D \equiv 0 \pmod{p^2}$$

admet ou n'admet pas de racines réelles, c'est-à-dire est décomposable ou non en deux facteurs irréductibles, selon que la congruence

$$\xi^2 - d \equiv 0 \pmod{p}$$

est elle-même réductible ou irréductible. Cela est vrai toutes les fois que D n'est pas divisible par p.

Supposons maintenant que D soit divisible par p sans l'être par p^2.

La première congruence sera irréductible, le premier membre de la seconde sera le carré du facteur irréductible ξ.

Pour voir comment on devra opérer pour lever cette difficulté, commençons par un exemple simple; soit

$$(40) \qquad \begin{vmatrix} p & -\xi & 0 & 0 \\ 0 & 1 & -\xi & 0 \\ 0 & 0 & 1 & -\xi \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

un idéal premier simple et supposons que ξ soit racine double de (39).

Cherchons le carré, le cube, etc., la puissance $\lambda^{\text{ième}}$ de (40).

Supposons d'abord, toujours pour plus de simplicité, $\xi = 0$, ce qui exige

$$A_1 \equiv A_0 \equiv 0 \pmod{p}.$$

Cherchons d'abord le carré de l'idéal donné

$$(40) \qquad \begin{vmatrix} p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Je dis que ce sera

$$(41) \qquad \begin{vmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

En effet, il est aisé de constater que (41) est un idéal. Or le carré de (40) a pour trame

$$p^2,\ p\alpha_1,\ \alpha_1^2,$$

et, comme ces trois nombres font partie de (41), (41) divise le carré de (40). Or ces deux idéaux ont même norme. Donc ils sont identiques. C. Q. F. D.

Cherchons maintenant les puissances paires de (40), la puissance 2α par exemple. C'est chercher la puissance α de (41).

$F(\alpha_1)$ va admettre comme facteur suivant le module $p^{2\alpha}$ un certain facteur quadratique $\alpha_1^2 + \alpha_1\lambda + \mu$, tel que

$$\lambda \equiv \mu \equiv 0 \pmod{p}.$$

L'idéal (41) peut s'écrire

$$\begin{vmatrix} p & 0 & \mu & 0 \\ 0 & p & \lambda & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Il a alors pour trame

$$p \text{ et } \alpha_1^2 + \lambda\alpha_1 + \mu.$$

Sa puissance $\alpha^{\text{ième}}$ a pour trame

$$p^\alpha \text{ et } p^{\alpha-\beta}(\alpha_1^2 + \lambda\alpha_1 + \mu)^\beta.$$

Elle est donc divisible par l'idéal dont la trame est

$$p^\alpha \text{ et } \alpha_1^2 + \lambda\alpha_1 + \mu.$$

Or cet idéal s'écrit

$$(42) \qquad \begin{vmatrix} p^\alpha & 0 & \mu & 0 \\ 0 & p^\alpha & \lambda & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

et a par conséquent même norme que la puissance $\alpha^{\text{ième}}$ de (41). Donc (42) est la puissance $\alpha^{\text{ième}}$ de (41) et la puissance $2\alpha^{\text{ième}}$ de (40).

Cherchons maintenant la puissance $2\alpha+1^{\text{ième}}$ de (40) : c'est le produit de (40) et de (42); elle aura donc pour trame

$$p^{\alpha+1},\quad \alpha_1 p^{\alpha},\quad p(\alpha_1^2+\lambda\alpha_1+\mu),\quad \alpha_1(\alpha_1^2+\lambda\alpha_1+\mu).$$

Supposons, ce qu'on peut toujours faire, que $\alpha_1^2+\lambda\alpha_1+\mu$ soit un facteur $F(\alpha_1)$ suivant le module $p^{2\alpha+1}$.

$$(43)\qquad \begin{vmatrix} p^{\alpha+1} & 0 & \mu & 0 \\ 0 & p^{\alpha} & \lambda & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

sera un idéal dont feront partie tous les nombres de la trame de la puissance cherchée et qui aura même norme que cette puissance; ce sera donc cette puissance elle-même.

Supposons maintenant que

$$F(\alpha_1)=\alpha_1^5-A_4\alpha_1^4+A_3\alpha_1^3-A_2\alpha_1^2+A_1\alpha_1-A_0$$

admette comme facteur suivant le module p

$$(\alpha_1^2+\lambda\alpha_1+\mu)^2.$$

Il admettra comme facteur *irréductible* suivant le module p^h, h étant très grand,

$$\alpha_1^4+H_3\alpha_1^3+H_2\alpha_1^2+H_1\alpha_1+H_0,$$

où

$$H_0\equiv\mu^2,\quad H_1\equiv 2\lambda\mu,\quad H_2\equiv\lambda^2+2\mu,\quad H_3\equiv 2\lambda\pmod{p}.$$

Il y aura alors un idéal premier

$$\begin{vmatrix} p & 0 & \mu & 0 & 0 \\ 0 & p & \lambda & \mu & 0 \\ 0 & 0 & 1 & \lambda & \mu \\ 0 & 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

dont la puissance $2\alpha^{\text{ième}}$ sera

$$\begin{vmatrix} p^\alpha & 0 & 0 & 0 & H_0 \\ 0 & p^\alpha & 0 & 0 & H_1 \\ 0 & 0 & p^\alpha & 0 & H_2 \\ 0 & 0 & 0 & p^\alpha & H_3 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

et la puissance $2\alpha+1^{\text{ième}}$

$$\begin{vmatrix} p^{\alpha+1} & 0 & \mu p^\alpha & 0 & H_0 \\ 0 & p^{\alpha+1} & \lambda p^\alpha & \mu p^\alpha & H_1 \\ 0 & 0 & p^\alpha & \lambda p^\alpha & H_2 \\ 0 & 0 & 0 & p^\alpha & H_3 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Encore un exemple : supposons que $F(\alpha_1)$ admette le facteur

$$(\alpha_1+\xi)^3$$

suivant le module p.

Il admettra comme facteur irréductible, suivant le module p^h, h étant très grand,

$$\alpha_1^3+H_2\alpha_1^2+H_1\alpha_1+H_0,$$

où

$$H_2\equiv 3\xi,\quad H_1\equiv 3\xi^2,\quad H_0\equiv\xi^3\pmod p.$$

Il y aura alors un idéal premier

$$\begin{vmatrix} p & \xi & 0 & 0 & 0 \\ 0 & 1 & \xi & 0 & 0 \\ 0 & 0 & 1 & \xi & 0 \\ 0 & 0 & 0 & 1 & \xi \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

dont les puissances $3\alpha^{\text{ième}}$, $(3\alpha+1)^{\text{ième}}$, $(3\alpha+2)^{\text{ième}}$ sont respectivement

$$\begin{vmatrix} p^\alpha & 0 & 0 & H_0 & 0 \\ 0 & p^\alpha & 0 & H_1 & H_0 \\ 0 & 0 & p^\alpha & H_2 & H_1 \\ 0 & 0 & 0 & 1 & H_2 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

$$\begin{vmatrix} p^{\alpha+1} & \xi p^{\alpha} & 0 & H_0 & 0 \\ 0 & p^{\alpha} & \xi p^{\alpha} & H_1 & H_0 \\ 0 & 0 & p^{\alpha} & H_2 & H_1 \\ 0 & 0 & 0 & 1 & H_2 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

$$\begin{vmatrix} p^{\alpha+1} & 0 & \xi^2 p^{\alpha} & H_0 & 0 \\ 0 & p^{\alpha+1} & 2\xi p^{\alpha} & H_1 & H_0 \\ 0 & 0 & p^{\alpha} & H_2 & H_1 \\ 0 & 0 & 0 & 1 & H_2 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Ces exemples suffiront, je pense, pour faire comprendre comment on devra se tirer d'affaire dans le cas exceptionnel qui nous occupe.

Multiplication de deux idéaux dont les normes sont premières entre elles.

Soient

$$\begin{vmatrix} abcd & abc\zeta & ab\varepsilon & a\gamma \\ 0 & abc & ab\delta & a\beta \\ 0 & 0 & ab & a\alpha \\ 0 & 0 & 0 & a \end{vmatrix}, \quad \begin{vmatrix} a_1b_1c_1d_1 & a_1b_1c_1\zeta_1 & a_1b_1\varepsilon_1 & a_1\gamma_1 \\ 0 & a_1b_1c_1 & a_1b_1\delta_1 & a_1\beta_1 \\ 0 & 0 & a_1b_1 & a_1\alpha_1 \\ 0 & 0 & 0 & a_1 \end{vmatrix}$$

les deux idéaux à multiplier. Leurs normes seront respectivement

$$N = a^4b^3c^2d, \quad N_1 = a_1^4b_1^3c_1^2d_1.$$

La norme de leur produit, qui est en même temps leur plus petit commun multiple, sera

$$NN_1 = (aa_1)^4(bb_1)^3(cc_1)^2(dd_1),$$

N étant premier avec N_1 et par conséquent a, b, c, d premiers avec a_1, b_1, c_1, d_1; on pourra trouver des nombres

$$A, B, T, \Delta, E, Z,$$

tels que

$$\begin{aligned} Z &\equiv \zeta \pmod{d}, & Z &\equiv \zeta_1 \pmod{d_1}, \\ E &\equiv \varepsilon \pmod{cd}, & E &\equiv \varepsilon_1 \pmod{c_1d_1}, \\ \Delta &\equiv \delta \pmod{c}, & \Delta &\equiv \delta_1 \pmod{c_1}, \\ \Gamma &\equiv \gamma \pmod{bcd}, & \Gamma &\equiv \gamma_1 \pmod{b_1c_1d_1}, \\ B &\equiv \beta \pmod{bc}, & B &\equiv \beta_1 \pmod{b_1c_1}. \\ A &\equiv \alpha \pmod{b}, & A &\equiv \alpha_1 \pmod{b_1}. \end{aligned}$$

Les idéaux sont alors équivalents à

$$\begin{vmatrix} abcd & abcZ & abE & a\Gamma \\ o & abc & ab\Delta & aB \\ o & o & ab & aA \\ o & o & o & a \end{vmatrix}, \quad \begin{vmatrix} a_1b_1c_1d_1 & a_1b_1c_1Z & a_1b_1E & a_1\Gamma \\ o & a_1b_1c_1 & a_1b_1\Delta & a_1B \\ o & o & a_1b_1 & a_1A \\ o & o & o & a_1 \end{vmatrix}.$$

Leur produit divisera l'idéal

$$(44) \qquad \begin{vmatrix} abcda_1b_1c_1d_1 & abca_1b_1c_1Z & aba_1b_1E & aa_1T \\ o & abca_1b_1c_1 & aba_1b_1\Delta & aa_1B \\ o & o & aba_1b_1 & aa_1\Delta \\ o & o & o & aa_1 \end{vmatrix}$$

et, à cause de l'identité des normes, sera identique à (44).

Problème. — *Former tous les idéaux de norme* N.

On décomposera N en facteurs premiers; supposons qu'on obtienne de la sorte

$$N = p^h p_1^{h_1} p_2^{h_2}.$$

On formera tous les idéaux de nombre p^h, de norme $p_1^{h_1}$, de norme $p_2^{h_2}$ et on les multipliera entre eux d'après la règle précédente; on obtiendra ainsi tous les idéaux de norme N.

Problème. — *Reconnaître si un nombre* N *peut être représenté par la forme* $\Psi(x_1, x_2, \ldots, x_m)$.

On formera tous les idéaux de norme N d'après la règle précédente. Supposons que tous les nombres complexes de l'un de ces idéaux soient compris dans la formule

$$\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_m x_m,$$

où les β sont des nombres complexes donnés et les x des entiers indéterminés. On cherchera, d'après la méthode de M. Hermite, si les formes

$$N\Psi(x_1, x_2, \ldots, x_m) \quad \text{et} \quad \text{norme}(\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_m x_m)$$

sont équivalentes. Si elles le sont, le nombre N peut être représenté par Ψ.

Si aucun des idéaux de norme N ne donne une forme équivalente à $N\Psi$, le nombre N ne peut être représenté par Ψ.

Sachant reconnaître si un nombre entier donné peut être représenté par Ψ, on saura reconnaître s'il peut l'être par F.

Imperfection de la méthode.

Si l'on veut trouver toutes les représentations de N par F, on cherche toutes les représentations de $B_m^{m-1}N$ par Ψ; supposons que l'on trouve que Ψ devient égal à $B_m^{m-1}N$ quand on fait

$$x_1 = \beta_1, \quad x_2 = \beta_2, \quad \ldots, \quad x_m = \beta_m.$$

On rejettera toutes les solutions pour lesquelles on n'aura pas à la fois

$$\beta_3 = \beta_4 = \ldots = \beta_m = 0, \quad \beta_1 \equiv 0 \pmod{B_m}.$$

S'il en reste une, on saura que F devient égal à N quand on fait

$$x = \frac{\beta_1}{B_m}, \quad y = \beta_2.$$

On est donc obligé, pour trouver toutes les représentations de N par F, de chercher toutes les représentations de $B_m^{m-1}N$ par Ψ, dont la plus grande partie sera en général inutile. On est forcé, par conséquent, de former un plus grand nombre d'idéaux qu'il ne serait strictement nécessaire. C'est ce qui nous conduit à chercher quelques simplifications.

Pemière simplification. — Le problème de la représentation des nombres par F se ramène à celui de la représentation des nombres par Φ. Occupons-nous donc de ce second problème et cherchons à trouver des nombres entiers ξ, η, tels que

$$\Phi(\xi, \eta) = N,$$

N étant un entier donné.

(On peut toujours supposer que ξ et η sont premiers entre eux; car, s'ils ne l'étaient pas, N devrait être divisible par la puissance $m^{\text{ième}}$ de leur plus grand commun diviseur d et l'on devrait avoir

$$\Phi\left(\frac{\xi}{d}, \frac{\eta}{d}\right) = N d^{-m},$$

et le problème serait ramené à égaler Φ à Nd^{-m} en substituant à la place de x et de y deux nombres entiers $\frac{\xi}{d}$, $\frac{\eta}{d}$, premiers entre eux.)

Si l'on suppose le problème résolu, les nombres complexes compris dans la formule

$$(45) \qquad (\xi + \eta\alpha_1)(m_0 + m_1\alpha_1 + m_2\alpha_1^2 + \ldots + m_{m-1}\alpha_1^{m-1})$$

forment un idéal de norme N et la méthode générale consiste à former tous les idéaux de norme N et à chercher s'ils peuvent se mettre sous la forme (45).

Est-il nécessaire pour cela de former *tous* les idéaux de norme N? Non, car je dis que (45) est un idéal simple. En effet, si $m = 5$ par exemple, cet idéal s'écrit

$$\begin{vmatrix} \xi & 0 & 0 & 0 & A_0\eta \\ \eta & \xi & 0 & 0 & -A_1\eta \\ 0 & \eta & \xi & 0 & A_2\eta \\ 0 & 0 & \eta & \xi & -A_3\eta \\ 0 & 0 & 0 & \eta & \xi + A_4\eta \end{vmatrix},$$

ξ et η étant premiers entre eux; il en sera de même de η et $\xi + A_4\eta$; il existera deux nombres λ_1 et μ_1, tels que

$$\lambda_1\eta + \mu_1(\xi + A_4\eta) = 1.$$

On ne changera pas l'idéal en multipliant la cinquième colonne par μ_1 et y ajoutant la quatrième multipliée par λ_1 et (en même temps) en multipliant la quatrième colonne par $\xi + A_4\eta$ et en retranchant la cinquième multipliée par η; car le déterminant

$$\begin{vmatrix} \lambda_1 & \mu_1 \\ \xi + A_4\eta & -\eta \end{vmatrix} = 1.$$

L'idéal devient ainsi

$$\begin{vmatrix} \xi & 0 & 0 & -A_0\eta^2 & \mu_1 A_0\eta \\ \eta & \xi & 0 & A_1\eta^2 & -\mu_1 A_1\eta \\ 0 & \eta & \xi & -A_2\eta^2 & \mu_1 A_2\eta \\ 0 & 0 & \eta & \xi^2 + A_4\eta\xi + A_3\eta^2 & \lambda_1\xi - \mu_1 A_3\eta \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Les nombres η et $\xi^2 + A_4\eta\xi + A_3\eta^2$ sont premiers entre eux. Il existe donc deux nombres λ_2, μ_2, tels que

$$\lambda_2\eta + \mu_2(\xi_2 + A_4\eta\xi + A_3\eta^2) = 1.$$

On ne changera pas l'idéal en multipliant la quatrième colonne

par μ_2 et y ajoutant la troisième multipliée par λ_2, et en multipliant la troisième par $\xi^2 + A_4\eta_1\xi + A_3\eta_1^2$ et en retranchant la quatrième multipliée par η_1. L'idéal devient alors

$$\begin{vmatrix} \xi & 0 & A_0\eta_1^3 & -\mu_2 A_0\eta_1^2 & \mu_1 A_0\eta_1 \\ \eta_1 & \xi & -A_1\eta_1^3 & \mu_2 A_1\eta_1^2 & -\mu_1 A_1\eta_1 \\ 0 & \eta_1 & \xi^3 + A_4\eta_1\xi^2 + A_3\eta_1^2\xi + A_2\eta_1^3 & \lambda_2\xi - \mu_2 A_2\eta_1^2 & \mu_1 A_2\eta_1 \\ 0 & 0 & 0 & 1 & \lambda_1\xi - \mu_1 A_3\eta_1 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Les nombres η_1 et $\xi^3 + A_4\eta_1\xi^2 + A_3\eta_1^2\xi + A_2\eta_1^3$ sont premiers entre eux, etc.; il est aisé de voir qu'en continuant de la sorte, on amènera l'idéal à la forme

$$\begin{vmatrix} N & a & b & c & d \\ 0 & 1 & e & f & g \\ 0 & 0 & 1 & h & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

ce qui montre que c'est un idéal simple.

Donc, au lieu de former *tous* les idéaux de norme N, il suffira de former tous les idéaux simples de norme N.

Problème. — *Trouver toutes les représentations de* N *par* Φ.

Ce qui précède nous conduit à la règle suivante :

On envisagera la congruence

$$\xi^m - A_{m-1}\xi^{m+1} + A_{m-2}\xi^{m-2} - \ldots \pm A_0 \equiv 0 \pmod N. \tag{46}$$

Soit ξ l'une des racines de cette congruence.

Si les deux formes

$$N\Psi(y_1, y_2, \ldots, y_m)$$

et

$$\text{norme}[Nx_1 + (\alpha_1 - \xi)(x_2 + x_3\alpha_1 + x_4\alpha_1^2 + \ldots + x_m\alpha_1^{m-2})]$$

sont équivalentes et que l'on passe de la seconde à la première en posant

$$\begin{aligned} x_1 &= \lambda_{1,1}y_1 + \lambda_{1,2}y_2 + \ldots + \lambda_{1,m}y_m, \\ x_2 &= \lambda_{2,1}y_1 + \lambda_{2,2}y_2 + \ldots + \lambda_{2,m}y_m, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_m &= \lambda_{m,1}y_1 + \lambda_{m,2}y_2 + \ldots + \lambda_{m,m}y_m, \end{aligned}$$

si l'on a

$$\lambda_{3,1} = \lambda_{4,1} = \ldots = \lambda_{m,1} = 0,$$

on égalera Φ à N en posant

$$x = N\lambda_{1,1} - \xi\lambda_{2,1}, \quad y = \lambda_{2,1},$$

et l'on obtiendra de la sorte toutes les représentations de N par Φ.