JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

LIPSCHITZ

# Recherches sur la transformation, par des substitutions réelles, d'une somme de deux ou de trois carrés en elle-même

*Journal de mathématiques pures et appliquées 4^e série*, tome 2 (1886), p. 373-439.
<http://www.numdam.org/item?id=JMPA_1886_4_2__373_0>

# *Recherches sur la transformation, par des substitutions réelles, d'une somme de deux ou de trois carrés en elle-même;*

PAR M. LIPSCHITZ.

Traduction publiée avec l'autorisation de l'auteur, par J. MOLK, à Besançon.

La théorie, due à Gauss, des nombres complexes entiers repose sur la décomposition de ces nombres en nombres complexes entiers irréductibles, autrement dit *nombres complexes premiers*. On peut, à l'aide du même procédé de décomposition, représenter toutes les substitutions, à coefficients rationnels, qui transforment une somme de deux carrés en elle-même. La transformation d'une somme de trois carrés en elle-même conduit au calcul des quaternions; en considérant les substitutions correspondant à cette transformation et dont les coefficients sont des nombres rationnels, on est amené à étudier les quaternions entiers et, dans cette étude, ce qui importe tout d'abord est la décomposition des quaternions entiers en quaternions entiers irréductibles, autrement dit *quaternions premiers*. J'ai cherché à approfondir cette question et je donne, dans ce Mémoire, les résultats auxquels je suis parvenu. De même que la décomposition, en ses facteurs premiers, d'un nombre complexe entier dépend de sa norme, qui est une somme de deux carrés entiers, de même la décomposition, en ses facteurs premiers, d'un quaternion entier dépend de sa norme, qui est une somme

de quatre carrés entiers. C'est pourquoi mon Mémoire s'appuie sur les recherches déjà faites qui ont pour objet de mettre les nombres entiers sous la forme d'une somme de quatre carrés.

Après Fermat qui, le premier, a énoncé, comme remarque au problème 31 du Livre IV de Diophante, le célèbre théorème sur la possibilité de représenter un entier quelconque par la somme d'un nombre déterminé de nombres polygonaux d'une certaine espèce, Euler s'est occupé du théorème d'après lequel on peut représenter un entier quelconque par la somme de quatre carrés, dans le Mémoire intitulé : *Demonstratio theorematis Fermatiani, omnem numerum primum formæ* $4n+1$ *esse summam duorum quadratorum* (*N. Comm. Petrop.*, t. V, p. 3, 1754; *Comm. ar.*, t. I, p. 210).

Ce Mémoire contient (art. **93**) le théorème d'Algèbre à l'aide duquel on peut représenter, par une somme de quatre carrés, le produit de deux sommes de quatre carrés; on peut déduire immédiatement de ce théorème les règles du calcul des quaternions. Dans les œuvres posthumes de Gauss (*Œuvres complètes*, t. III, p. 384) se trouve une autre manière de présenter le même théorème; on y fait usage de paires de quantités complexes conjuguées.

La première démonstration complète du théorème, que chaque entier est la somme de quatre carrés, se trouve dans le Mémoire de Lagrange, *Démonstration d'un théorème d'Arithmétique* (*N. Mémoires de l'Académie des Sciences de Berlin*, 1770, *Œuvres*, t. III, p. 189); elle a été commentée avec détails par Euler dans le Mémoire : *Novæ demonstrationes circa resolutionem numerorum* (*Acta erudit.*, p. 193, 1773, Lips.; *Acta Petrop.*, t. I, II, p. 48, 1775; *Exhib.*, 1772, septembr. 21; *Comm. ar.*, t. I, p. 538). En déterminant, à l'aide de la théorie des fonctions elliptiques, de combien de manières différentes on peut mettre un entier donné sous la forme d'une somme de quatre carrés, Jacobi jeta un nouveau jour sur ce sujet. On trouve cette détermination à la fin des *Fundamenta nova;* elle est bien mise en évidence dans la Note sur la décomposition d'un nombre donné en quatre carrés; enfin, dans le Mémoire : *De compositione numerorum e quatuor quadratis* (*Journal de Crelle*, t. 12, p. 167), elle est donnée d'une façon purement arithmétique. Le Mémoire de Lejeune-Dirichlet : *Sur l'équation* $t^2+u^2+v^2+w^2=4m$ (*Journal de Liou-*

*ville*, 2ᵉ série, t. I, p. 210), contient une reproduction plus concise de cette démonstration; c'est dans ce Mémoire que Lejeune-Dirichlet nous apprend qu'il possède depuis longtemps une démonstration du même théorème basée sur des principes différents, et que cette démonstration trouvera sa place naturelle dans un travail qui l'occupe depuis quelque temps. On sait que la mort l'a empêché de publier les recherches qu'il avait faites sur ce sujet.

Je dois aussi rappeler la démonstration complète du théorème de Fermat concernant les nombres polygonaux, qui a été donnée par Cauchy, et que l'on trouve dans le premier volume des *Exercices*, p. 263 ; ainsi que les recherches de M. Hermite sur la représentation des nombres entiers par une somme de quatre carrés, qui font l'objet de son second Mémoire sur la théorie des formes quadratiques (*Journal de Crelle*, t. 47, p. 343).

Je voudrais encore faire une remarque générale sur la marche suivie dans mes recherches. La décomposition des nombres complexes entiers en leurs facteurs premiers tient essentiellement, ce me semble, à ce que le résultat de la multiplication de ces nombres est indépendant de l'ordre dans lequel on effectue cette opération. Pour les nombres algébriques quelconques, la multiplication dont on fait usage jouit de la même propriété et, une fois les notions convenables introduites, les lois de la décomposition continuent à avoir lieu, comme l'a montré M. Dedekind (*Vorlesungen Dirichlet's über Zahlentheorie*, 2ᵉ et 3ᵉ édition) et [*Sur la théorie des nombres entiers algébriques* (*Bulletin de Darboux*, 1877)]. La démonstration de l'existence des facteurs premiers idéaux dans la théorie, due à M. Kummer, des nombres complexes entiers provenant de la division du cercle, repose, d'autre part, sur certaines congruences qui apparaissent sous une forme simple dans la décomposition des nombres complexes entiers de la forme $a + b\sqrt{-1}$. M. Dedekind a communiqué les congruences correspondantes, se rapportant à la théorie des nombres algébriques, en annonçant, dans les *Göttingischen gelehrten Anzeigen* du 20 septembre 1871, la seconde édition des *Vorlesungen Dirichlet's* que je citais tout à l'heure. On fera remarquer dans le Mémoire actuel que la possibilité de mettre un quaternion entier sous forme de produit de quaternions entiers irréductibles repose également sur l'existence de

certaines congruences; mais ici l'ordre dans lequel se succèdent les facteurs irréductibles du produit est d'une importance capitale. Ainsi, au domaine des nombres entiers complexes de Gauss viennent s'adjoindre, d'une part, le domaine de tous les nombres algébriques, d'autre part, le domaine des quaternions entiers; mais, si l'on remarque plus d'une analogie, on remarque aussi plus d'un contraste entre ces différents domaines. C'est pour pouvoir bien éclairer ces analogies et ces contrastes que je m'occuperai tout d'abord de la décomposition des nombres complexes de Gauss. Je commencerai par exposer les principes de la transformation réelle d'une somme de deux carrés en elle-même; j'établirai, en prenant cette transformation pour base, les règles du calcul des quantités complexes, après quoi je passerai à l'étude des nombres complexes entiers. Je considérerai ensuite la transformation réelle d'une somme de trois carrés en elle-même; j'établirai, en prenant cette transformation pour base, les règles du calcul des quaternions, après quoi je passerai à l'étude des quaternions entiers.

## 1.

### *Transformation réelle d'une somme de deux carrés en elle-même et définition des quantités complexes.*

Si une substitution linéaire à coefficients réels $\alpha_{11}$, $\alpha_{12}$; $\alpha_{21}$, $\alpha_{22}$, qui représente les variables réelles $x_1$ et $x_2$ en fonction des variables réelles $y_1$ et $y_2$, transforme la somme des carrés des premières variables dans la somme des carrés des dernières, on a, à la fois, les équations

$$(1)\qquad \begin{cases} x_1 = \alpha_{11} y_1 + \alpha_{12} y_2, \\ x_2 = \alpha_{21} y_1 + \alpha_{22} y_2, \end{cases}$$

$$(2)\qquad x_1^2 + x_2^2 = y_1^2 + y_2^2.$$

Le déterminant de substitution ne peut alors être égal qu'à $+1$ ou à $-1$; supposons-le égal à $+1$. L'équation (2) est évidemment encore vérifiée et la valeur du déterminant ne change pas si, au lieu de la

substitution (1), nous en employons une autre déduite de (1) en multipliant les quatre coefficients par l'unité négative. De chacun de ces deux systèmes on peut déduire un nouveau système en ajoutant l'unité à chacun des éléments de celle des diagonales du déterminant de substitution qui joint le premier élément à gauche au dernier élément à droite. Les déterminants de ces deux nouveaux systèmes

$$(3)\qquad \begin{vmatrix} \alpha_{11}+1 & \alpha_{12} \\ \alpha_{21} & \alpha_{22}+1 \end{vmatrix},$$

$$(3_a)\qquad \begin{vmatrix} -\alpha_{11}+1 & -\alpha_{12} \\ -\alpha_{21} & -\alpha_{22}+1 \end{vmatrix}$$

sont respectivement égaux à

$$(4)\qquad 2+\alpha_{11}+\alpha_{22};$$

$$(4_a)\qquad 2-\alpha_{11}-\alpha_{22};$$

la somme de ces valeurs étant égale au nombre 4, l'un au moins des deux déterminants a une valeur différente de zéro. Si donc, pour une substitution donnée, le déterminant (3) était nul, le déterminant $(3_a)$ ne serait sûrement pas nul. Cette remarque permet de supposer que le système donné de coefficients $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ est tel que la valeur du déterminant (3) correspondant est différente de zéro. Nous ferons cette hypothèse dans tout ce qui suivra.

Le déterminant (3) paraît dès que l'on cherche à former, à l'aide de la substitution (1), les équations qui donnent $y_1$ et $y_2$ en fonction des sommes $x_1+y_2$ et $x_2+y_2$. Les équations (1) donnent, en effet, immédiatement

$$(5)\qquad \begin{cases} x_1+y_1=(\alpha_{11}+1)y_1+\alpha_{12}y_2, \\ x_2+y_2=\alpha_{21}y_1+(\alpha_{22}+1)y_2, \end{cases}$$

et, comme le déterminant (3) n'est pas nul, on peut tirer de ces équations, sans ambiguïté, $y_1$ et $y_2$ en fonction de $x_1+y_1$ et $x_2+y_2$. On obtient, par suite, les différences $x_1-y_1$ et $x_2-y_2$ exprimées, sans

ambiguïté, en fonction des sommes $x_1 + y_1$ et $x_2 + y_2$. Il vient

$$(6)\qquad \begin{cases} x_1 - y_1 = \dfrac{(\alpha_{11} - \alpha_{22})(x_1 + y_1) + 2\alpha_{12}(x_2 + y_2)}{2 + \alpha_{11} + \alpha_{22}}, \\ x_2 - y_2 = \dfrac{2\alpha_{21}(x_1 + y_1) + (\alpha_{22} - \alpha_{11})(x_2 + y_2)}{2 + \alpha_{11} + \alpha_{22}}. \end{cases}$$

Comme on a supposé que $\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$ était égal à $+1$, on a

$$\alpha_{11} - \alpha_{22} = 0, \qquad \alpha_{12} + \alpha_{21} = 0.$$

Si donc, $\lambda_0$ désignant une quantité quelconque différente de zéro, on détermine deux quantités $\lambda_{12}$ et $\lambda_{21}$ par les relations

$$(7)\qquad \frac{\alpha_{12}}{1 + \alpha_{11}} = \frac{\lambda_{12}}{\lambda_0}, \qquad \lambda_{12} + \lambda_{21} = 0,$$

l'équation (6) peut s'écrire

$$(8)\qquad \begin{cases} x_1 - y_1 = \dfrac{\lambda_{12}}{\lambda_0}(x_2 + y_2), \\ x_2 - y_2 = \dfrac{\lambda_{21}}{\lambda_0}(x_1 + y_1) \end{cases}$$

ou encore

$$(9)\qquad \begin{cases} \lambda_0 x_1 + \lambda_{21} x_2 = \lambda_0 y_1 + \lambda_{12} y_2, \\ \lambda_{12} x_1 + \lambda_0 x_2 = \lambda_{21} y_1 + \lambda_0 y_2. \end{cases}$$

Si l'on ajoute à la première des équations (9), multipliée par l'unité, la seconde des équations (9) multipliée par un facteur symbolique $i_{12}$, on peut mettre les deux termes de l'équation que l'on obtient sous forme d'un produit en posant

$$(10)\qquad \begin{cases} \lambda_0 x_1 + \lambda_{21} x_2 + i_{12}(\lambda_{12} x_1 + \lambda_0 x_2) \\ \quad = (\lambda_0 + i_{12}\lambda_{12})(x_1 + i_{12} x_2), \\ \lambda_0 y_1 + \lambda_{12} y_2 + i_{12}(\lambda_{21} y_1 + \lambda_0 y_2) \\ \quad = (y_1 + i_{12} y_2)(\lambda_0 - i_{12}\lambda_{12}). \end{cases}$$

Pour que ces équations (10) soient vérifiées, il suffit de supposer que le symbole $i_{12}$ vérifie l'équation

$$i_{12}^2 = -1. \tag{11}$$

Les propriétés de ce symbole sont alors identiques à celles du symbole $\sqrt{-1}$, et l'on voit que le résultat de la multiplication de deux *expressions complexes*

$$(\lambda_0 + i_{12}\lambda_{12}), \quad (x_1 + i_{12}x_2)$$

ne change pas si l'on change l'ordre des deux facteurs. En égalant les deux produits (10), on obtient l'équation symbolique

$$(\lambda_0 + i_{12}\lambda_{12})(x_1 + i_{12}x_2) = (y_1 + i_{12}y_2)(\lambda_0 - i_{12}\lambda_{12}), \tag{12}$$

qui comprend les deux équations (1). En multipliant les deux membres de cette équation (12) par l'expression $(\lambda_0 - i_{12}\lambda_{12})$ conjuguée de $(\lambda_0 + i_{12}\lambda_{12})$, on obtient une équation

$$(\lambda_0^2 + \lambda_{12}^2)(x_1 + i_{12}x_2) = (y_1 + i_{12}y_2)(\lambda_0 - i_{12}\lambda_2)^2, \tag{13}$$

dont le premier membre contient en facteur la *norme* de $(\lambda_0 + i_{12}\lambda_{12})$,

$$\mathfrak{N}(\lambda_0 + i_{12}\lambda_{12}) = \lambda_0^2 + \lambda_{12}^2. \tag{13*}$$

En prenant, comme point de départ, une substitution (1) pour laquelle le déterminant (3) n'est pas nul, nous sommes parvenus à l'équation symbolique (12), dans laquelle $\lambda_0$ est différent de zéro. Si nous prenons, inversement, comme point de départ, une quantité complexe quelconque $\lambda_0 + i_{12}\lambda_{12}$ dont la partie réelle $\lambda_0$ soit différente de zéro (ou, si l'on veut, un système de deux quantités réelles $\lambda_0$, $\lambda_{12}$, la première quelconque mais différente de zéro, la seconde entièrement arbitraire), et si nous formons, à l'aide de cette quantité complexe, une équation (12), l'équation (13) qui se déduit de cette équation (12) donne, pour les variables $x_1$ et $x_2$, des fonctions linéaires (1) des variables $y_1$ et $y_2$ vérifiant l'équation (2). Les coefficients de ces fonc-

tions linéaires sont

$$(14)\qquad \alpha_{11}=\alpha_{22}=\frac{\lambda_0^2-\lambda_{12}^2}{\lambda_0^2+\lambda_{12}^2},\qquad \alpha_{12}=-\alpha_{21}=\frac{2\lambda_0\lambda_{12}}{\lambda_0^2+\lambda_{12}^2};$$

le déterminant $\alpha_{11}\alpha_{22}-\alpha_{12}\alpha_{21}$ est égal à $+1$, et le déterminant (4) correspondant a pour valeur

$$(15)\qquad \frac{4\lambda_0^2}{\lambda_0^2+\lambda_{12}^2};$$

comme $\lambda_0$ est choisi différent de zéro, ce déterminant n'est pas nul. Ainsi toutes les quantités complexes $\lambda_0+i_{12}\lambda_{12}$, dont la partie réelle $\lambda_0$ est différente de zéro, nous ramènent à des substitutions linéaires (1), au déterminant $+1$, pour lesquelles le déterminant (4) est différent de zéro. Nous conviendrons d'écrire simplement $i$, au lieu de $i_{13}$, dans ce qui va suivre.

Considérons maintenant une substitution linéaire liant les variables $y_1, y_2$ à de nouvelles variables $z_1, z_2$ de telle sorte qu'on ait

$$(16)\qquad y_1^2+y_2^2=z_1^2+z_2^2.$$

Prenons d'abord la substitution particulière

$$(17)\qquad y_1=-z_1,\qquad y_2=-z_2;$$

elle peut être remplacée par l'unique équation

$$(18)\qquad i(y_1+iy_2)=(z_1+iz_2)(-i).$$

En composant les substitutions (1) et (17), on obtient la substitution

$$(19)\qquad \begin{cases} x_1=-\alpha_{11}z_1-\alpha_{12}z_2, \\ x_2=-\alpha_{21}z_1-\alpha_{22}z_2; \end{cases}$$

en combinant les équations (12) et (18) correspondantes, on obtient l'équation

$$(20)\quad i(\lambda_0+i\lambda_{12})(x_1+ix_2)=(z_1+iz_2)(-i)(\lambda_0-i\lambda_{12}).$$

Ainsi, en remplaçant dans l'équation (12) la quantité complexe $(\lambda_0 + i\lambda_{12})$ par la quantité complexe $i(\lambda_0 + i\lambda_{12})$, on obtient, comme substitution correspondante, au lieu de la substitution (1), la substitution (19) qui diffère de (1) en ce que tous ses coefficients sont multipliés par l'unité négative. Or toutes les substitutions linéaires à considérer se déduisent, comme nous l'avons vu, des substitutions (1) pour lesquelles le déterminant (4) n'est pas nul, en y ajoutant celles qui en dérivent en changeant le signe des coefficients. Toutes les substitutions linéaires en question sont donc représentées par l'ensemble des équations (12) et (20). Mais les quantités complexes

$$\lambda_0 + i\lambda_{12} \quad \text{et} \quad i(\lambda_0 + i\lambda_{12}),$$

où $\lambda_0$ n'est pas nul, représentent sans exception toutes les quantités complexes dont la norme est différente de zéro. Il en résulte que toutes les substitutions linéaires considérées sont représentées par les équations (12) ou, si l'on veut, par les équations (14), pourvu que les deux quantités réelles $\lambda_0$ et $\lambda_{12}$ ne soient pas nulles simultanément, ou, en d'autres termes, pourvu que la norme de $(\lambda_0 + i\lambda_{12})$ ne soit pas nulle.

A l'aide d'une quantité complexe quelconque dont la norme n'est pas nulle $(\mu_0 + i\mu_{12})$, formons la relation analogue à (12)

$$(21) \qquad (\mu_0 + i\mu_{12})(y_1 + iy_2) = (z_1 + iz_2)(\mu_0 - i\mu_{12}),$$

à laquelle correspond une substitution linéaire, semblable à (1), nous permettant de passer des variables réelles $y_1$ et $y_2$ aux variables réelles $z_1$ et $z_2$. En appliquant successivement la substitution (1) et cette dernière substitution, nous obtenons une nouvelle substitution à laquelle correspond l'équation

$$(22) \qquad \begin{cases} (\mu_0 + i\mu_{12})(\lambda_0 + i\lambda_{12})(x_1 + ix_2) \\ \quad = (z_1 + iz_2)(\mu_0 - i\mu_{12})(\lambda_0 - i\lambda_{12}); \end{cases}$$

dans cette équation paraît le produit des deux quantités complexes $(\mu_0 + i\mu_{12})$ et $(\lambda_0 + i\lambda_{12})$; la norme de ce produit est différente de zéro parce que la norme de chacun des deux facteurs est différente de

zéro; on voit aussi qu'il est permis, sans rien changer au résultat, de permuter d'une manière quelconque l'ordre dans lequel on effectue les substitutions que l'on veut composer.

## II.

PROBLÈME. — *Trouver tous les nombres complexes entiers dont la norme est égale à un nombre entier donné.*

*Trouver toutes les substitutions rationnelles qui transforment une somme de deux carrés en elle-même.*

Nous commencerons par chercher les conditions auxquelles doit satisfaire un entier positif $m$ donné, pour pouvoir être égal à la norme d'un nombre complexe entier quelconque. Dans le cas où ces conditions sont vérifiées, nous nous proposerons de trouver *tous* les nombres complexes entiers dont la norme est égale à $m$. Enfin nous chercherons à mettre, de toutes les manières possibles, chacun de ces nombres complexes entiers sous la forme d'un produit de nombres complexes entiers irréductibles. Pour abréger, nous dirons souvent *entier complexe* au lieu de nombre complexe entier et *nombre premier complexe* au lieu de nombre complexe entier irréductible.

On peut diviser les entiers complexes $(\lambda_0 + i\lambda_{12})$ en deux groupes : ceux pour lesquels les deux entiers réels $\lambda_0$ et $\lambda_{12}$ n'ont pas de diviseur commun et ceux pour lesquels ils ont un diviseur commun; les entiers complexes du premier groupe sont les *entiers complexes proprement dits*, ceux du second groupe sont les *entiers complexes impropres*. Nous restreindrons le problème posé aux entiers complexes proprement dits.

Si $(\lambda_0 + i\lambda_{12})$ est un entier complexe proprement dit, les entiers $\lambda_0$ et $\lambda_{12}$ ne peuvent être tous deux pairs; sa norme $(\lambda_0^2 + \lambda_{12}^2)$ ne peut donc être qu'un nombre impair ou le double d'un nombre impair. Posons

$$\lambda_0^2 + \lambda_{12}^2 = m, \tag{1}$$

et désignons par $p$ un quelconque des nombres premiers impairs qui

divisent $m$; soit $\gamma$ le nombre de fois que $m$ contient $p$ en facteur. Je dis qu'on peut alors toujours trouver deux nombres entiers $\xi_1$ et $\xi_2$, qui ne soient pas divisibles par $p$ tous les deux, et qui vérifient les congruences

$$(2) \qquad \left\{ \begin{array}{l} \lambda_0\,\xi_1 + \lambda_{21}\xi_2 \equiv 0 \\ \lambda_{12}\xi_1 + \lambda_0\,\xi_2 \equiv 0 \end{array} \right\} \pmod{p^\gamma}.$$

Aucun des entiers $\lambda_0$ et $\lambda_{12}$ ne peut être divisible par $p$; car, si l'un d'eux était divisible par $p$, l'autre le serait aussi à cause de la relation (1), et $\lambda_0 + i\lambda_{12}$ serait, par suite, un entier complexe impropre. Il en résulte que l'on peut vérifier chacune des deux congruences (2), sans tenir compte de l'autre, par des entiers $\xi_1$ et $\xi_2$. A l'aide de la relation (1), on montre facilement que, si l'une des deux congruences est vérifiée pour des entiers déterminés $\xi_1$ et $\xi_2$, l'autre est également vérifiée pour ces mêmes entiers. D'ailleurs, en ajoutant à la première de ces congruences multipliée par $\xi_1$ la seconde multipliée par $\xi_2$, et en observant que $\lambda_0$ n'est pas divisible par $p$, on obtient une nouvelle congruence

$$(3) \qquad \xi_1^2 + \xi_2^2 \equiv 0 \pmod{p^\gamma}$$

vérifiée par les mêmes entiers $\xi_1$, $\xi_2$.

Si, dans la première congruence (2), on prend $\xi_2$ égal à l'unité, la valeur entière correspondante de $\xi_1$, $\xi_1 \equiv \omega$, est déterminée sans ambiguïté par la congruence

$$(4) \qquad \lambda_0\omega + \lambda_{21} \equiv 0 \pmod{p^\gamma};$$

si nous donnons ensuite à $\xi_2$ une valeur entière quelconque non divisible par $p$, la valeur entière correspondante de $\xi_1$ est déterminée sans ambiguïté par la congruence

$$(5) \qquad \xi_1 \equiv \omega\xi_2 \pmod{p^\gamma};$$

$\omega$ vérifie d'ailleurs la congruence connue

$$(6) \qquad \omega^2 + 1 \equiv 0 \pmod{p^\gamma}.$$

Considérons donc tous les couples de nombres $(\xi_1, \xi_2)$ qui satisfont aux congruences (2), sans être divisibles par $p$. On les obtient en multipliant les deux nombres de l'un quelconque d'entre eux par un même entier quelconque.

Si nous regardons comme équivalents et si nous groupons dans une même classe ces couples de nombres, chaque entier complexe $(\lambda_0 + i\lambda_{12})$ appartiendra, d'après ce qui précède, *à une classe bien déterminée* de solutions des congruences (2), de la congruence (3) ou, ce qui est identique, à une racine bien déterminée de la congruence (6). Il faut donc que cette congruence (6) soit possible pour que l'équation (1) ait lieu.

Or, d'après un théorème connu, cette congruence est possible ou ne l'est pas, selon que le reste de la division par 4 du nombre premier impair $p$ est égal à 1 ou à 3; et, dans le premier cas, la congruence a toujours deux racines. Donc les entiers $m$ qui ont des diviseurs premiers de la forme $4r + 3$ ne peuvent être représentés comme normes d'entiers complexes proprement dits, et il suffit de considérer les nombres $m$ dont tous les diviseurs premiers impairs sont de la forme $4r+1$. C'est pourquoi les nombres premiers de la forme $4r+3$ qui, comme on le sait, jouent aussi le rôle de nombres premiers dans la théorie des nombres complexes entiers, ne paraissent pas dans la suite de nos recherches.

Je vais maintenant montrer que tout nombre premier impair $p$ de la forme $4r+1$ peut être mis sous la forme $\lambda_0^2 + \lambda_{12}^2$, de manière que l'entier complexe correspondant $(\lambda_0 + i\lambda_{12})$ appartienne à une classe choisie à volonté parmi les deux classes de solutions de la congruence

$$(3^*) \qquad \xi_1^2 + \xi_2^2 \equiv 0 \pmod{p},$$

ou, si l'on veut, appartienne à une racine choisie à volonté parmi les deux racines de la congruence

$$(6^*) \qquad \omega^2 + 1 \equiv 0 \pmod{p}.$$

Observons d'abord que l'entier complexe cherché $(\lambda_0 + i\lambda_{12})$ ne

peut pas être le produit de deux entiers complexes dont les normes soient, toutes deux, différentes de l'unité; l'entier complexe cherché est donc nécessairement un nombre premier complexe, de sorte qu'une fois ce nombre entier complexe trouvé, nous n'aurons pas besoin de chercher encore à le mettre sous forme d'un produit de nombres premiers complexes. Ceci posé, fixons arbitrairement l'une des racines $\omega$ de la congruence

$$\omega^2 + 1 \equiv 0 \pmod{p},$$

et formons, à l'aide de cette racine $\omega$ et d'un entier quelconque $\xi_2$ non divisible par $p$, le système d'entiers

$$\xi_1 \equiv \omega\xi_2, \quad \xi_2 \pmod{p}; \tag{7}$$

nous pouvons alors choisir, dans ce système, deux entiers, l'un congru à $\xi_1$, l'autre congru à $\xi_2$, qui soient numériquement plus petits que $\frac{p}{2}$. Ces deux entiers ne peuvent être simultanément divisibles par $p$; si donc $\tau$ est leur plus grand commun diviseur, $\tau$ n'est pas divisible par $p$.

Je désignerai par $\rho_0$ et $\rho_{21}$ les deux entiers choisis divisés par $\tau$, de sorte que

$$\tau\rho_0 \equiv \xi_1, \qquad \tau\rho_{21} \equiv \xi_2 \pmod{p}, \tag{8}$$

et je définirai $\rho_{12}$ par l'équation

$$\rho_{12} + \rho_{21} = 0. \tag{9}$$

La norme $\tau^2(\rho_0^2 + \rho_{12}^2)$ est divisible par $p$, et est plus petite que $\frac{1}{2}p^2$; son second facteur $\rho_0^2 + \rho_{12}^2$, qui est la norme de l'entier complexe

$$(\rho_0 + i\rho_{12}),$$

jouit donc des mêmes propriétés, et nous pouvons écrire, en désignant par $t$ un entier plus petit que $\frac{p}{2}$,

$$\rho_0^2 + \rho_{12}^2 = pt; \tag{10}$$

d'ailleurs, comme $\tau$ n'est pas divisible par $p$, nous avons les congruences

$$(11) \qquad \left\{ \begin{array}{l} \rho_0\ \xi_1 + \rho_{21}\xi_2 \equiv 0 \\ \rho_{12}\xi_1 + \rho_0\ \xi_2 \equiv 0 \end{array} \right\} \pmod{p}.$$

De l'entier complexe proprement dit $(\rho_0 + i\rho_{12})$ que nous venons de former, et auquel correspondent les relations (10) et (11), nous allons déduire un autre entier complexe proprement dit $[\rho_0^{(1)} + i\rho_{12}^{(1)}]$, auquel correspondent des relations semblables à (10) et (11), mais pour lequel le multiple de $p$, dans la relation (10), est plus petit que $t$. Déterminons, à cet effet, les deux entiers $\varphi_0$ et $\varphi_{12}$, numériquement plus petits que $\frac{t}{2}$ ou au plus égaux à $\frac{t}{2}$, qui vérifient les congruences

$$(12) \qquad \varphi_0 \equiv \rho_0, \qquad \varphi_{12} \equiv \rho_{12} \pmod{t}.$$

Le nombre entier $\varphi_0^2 + \varphi_{12}^2$ contient alors $t$ en facteur, et si nous posons

$$(13) \qquad \varphi_0^2 + \varphi_{12}^2 = tt^{(1)},$$

le nombre entier $t^{(1)}$ est plus petit ou au plus égal à $\frac{t}{2}$, et ne peut, par suite, être divisible par $p$, puisque $t$ est plus petit que $\frac{p}{2}$. Formons ensuite le produit $(\varphi_0 - i\varphi_{12})(\rho_0 + i\rho_{12})$; ses deux éléments réels $\varphi_0\rho_0 + \varphi_{12}\rho_{12}$ et $\varphi_0\rho_{12} - \rho_0\varphi_{12}$ sont divisibles par $t$; sa norme est égale à $pt^2t^{(1)}$; elle est donc divisible par $p$, mais n'est pas divisible par $p^2$; donc, le plus grand commun diviseur de $\varphi_0\rho_0 + \varphi_{12}\rho_{12}$ et de $\varphi_0\rho_{12} - \rho_0\varphi_{12}$ est égal à $\tau^{(1)}t$, où $\tau^{(1)}$ n'est pas divisible par $p$. Nous pouvons ainsi définir un entier complexe proprement dit $[\rho_0^{(1)} + i\rho_{12}^{(1)}]$ par l'équation

$$(14) \qquad (\varphi_0 - i\varphi_{12})(\rho_0 + i\rho_{12}) = \tau^{(1)}t[\rho_0^{(1)} + i\rho_{12}^{(1)}].$$

On déduit maintenant facilement des congruences (11), par multiplication et addition, les congruences

$$(15) \qquad \left\{ \begin{array}{l} \tau^{(1)}t[\rho_0^{(1)}\xi_1 + \rho_{21}^{(1)}\xi_2] \equiv 0 \\ \tau^{(1)}t[\rho_{12}^{(1)}\xi_1 + \rho_0^{(1)}\xi_2] \equiv 0 \end{array} \right\} \pmod{p},$$

qui entraînent, comme ni $\tau^{(1)}$, ni $t$ ne sont divisibles par $p$, les congruences

$$\left.\begin{aligned} \rho_0^{(1)}\xi_1 + \rho_{21}^{(1)}\xi_2 &\equiv 0 \\ \rho_{12}^{(1)}\xi_1 + \rho_0^{(1)}\xi_2 &\equiv 0 \end{aligned}\right\} \pmod p. \tag{16}$$

D'autre part, les équations (10), (13) et (14) donnent immédiatement la relation

$$[\rho_0^{(1)}]^2 + [\rho_{12}^{(1)}]^2 = p\frac{t^{(1)}}{[\tau^{(1)}]^2}, \tag{17}$$

et, comme $t^{(1)}$ n'est pas plus grand que $\frac{t}{2}$, le nombre entier $\frac{t^{(1)}}{[\tau^{(1)}]^2}$ vérifie nécessairement l'inégalité $\frac{t^{(1)}}{[\tau^{(1)}]^2} \leq \frac{t}{2}$, et est, par suite, plus petit que $t$. Les relations (16) et (17), formées à l'aide de $\rho_0^{(1)}$ et $\rho_{12}^{(1)}$ sont bien semblables aux relations (11) et (10) formées à l'aide de $\rho_0$ et $\rho_{12}$, et le multiple entier de $p$ dans la relation (17) est plus petit que $t$.

Rien n'empêche de répéter le même raisonnement et de former ainsi successivement des entiers complexes $[\rho_0^{(2)} + i\rho_{12}^{(2)}]$, $[\rho_0^{(3)} + i\rho_{12}^{(3)}]$, etc., vérifiant comme $(\rho_0 + i\rho_{12})$ et $[\rho_0^{(1)} + i\rho_{12}^{(1)}]$ les relations (10) et (11), et ayant dans l'équation (10) comme multiple de $p$ un nombre entier de plus en plus petit, jusqu'à ce qu'enfin cet entier soit égal à l'unité. On arrive ainsi à former un entier complexe $[\rho_0^{(s)} + i\rho_{12}^{(s)}]$, dont les éléments $\rho_0^{(s)}$, $\rho_{12}^{(s)}$ vérifient les relations

$$(\rho_0^{(s)})^2 + (\rho_{12}^{(s)})^2 = p, \tag{18}$$

$$\left.\begin{aligned} \rho_0^{(s)}\xi_1 + \rho_{21}^{(s)}\xi_2 &\equiv 0 \\ \rho_{12}^{(s)}\xi_1 + \rho_0^{(s)}\xi_2 &\equiv 0 \end{aligned}\right\} \pmod p, \tag{19}$$

et qui jouit, par suite, des deux propriétés d'avoir une norme égale au nombre premier impair donné et d'appartenir à une classe donnée de solutions de la congruence $\xi_1^2 + \xi_2^2 \equiv 0 \pmod p$.

Les entiers complexes que l'on obtient en multipliant $(\rho_0^{(s)} + i\rho_{12}^{(s)})$ par une des quatre unités $1, -1, i, -i$, appartiennent manifestement à la même classe de solutions de la congruence (3*). Nous choisirons arbitrairement l'un de ces quatre entiers complexes pour nous en servir dans les calculs suivants.

On peut aussi représenter le nombre premier impair $p$ comme norme du nombre premier complexe $(\rho_0^{(s)} - i\rho_{12}^{(s)})$ conjugué de $(\rho_0^{(s)} + i\rho_{12}^{(s)})$; mais ce nombre premier complexe $(\rho_0^{(s)} - i\rho_{12}^{(s)})$ n'appartient pas à la même classe de solutions de la congruence (3*) que $(\rho_0^{(s)} + i\rho_{12}^{(s)})$. Il appartient, en effet, à la classe de solutions de la congruence (3*) dont le système $(\xi_1, -\xi_2)$ fait partie, et les deux systèmes $(\xi_1, \xi_2)$ et $(\xi_1, -\xi_2)$ ne peuvent être équivalents, puisque, s'ils l'étaient, $2\xi_2$ serait divisible par $p$, ce qui n'est pas. Les quatre nombres premiers complexes, que l'on obtient en multipliant $(\rho_0^{(s)} - i\rho_{12}^{(s)})$ par les quatre unités $1, -1, i, -i$, appartiennent manifestement à la même classe et nous choisirons aussi l'un de ces quatre entiers pour nous en servir dans les calculs suivants.

Avant d'aller plus loin, il nous faut chercher la condition nécessaire et suffisante pour que la partie réelle et la partie imaginaire du produit de deux entiers complexes proprement dits $(\lambda_0 + i\lambda_{12})$ et $(\mu_0 + i\mu_{12})$ soient divisibles par une puissance $p^\nu$ d'un nombre premier impair $p$. Des deux congruences

$$(20) \qquad \left\{\begin{array}{l} \mu_0\lambda_0 - \mu_{12}\lambda_{12} \equiv 0 \\ \mu_0\lambda_{12} + \mu_{12}\lambda_0 \equiv 0 \end{array}\right\} \pmod{p^\nu},$$

on déduit les congruences

$$(21) \quad \mu_0(\lambda_0^2 + \lambda_{12}^2) \equiv 0, \qquad \mu_{12}(\lambda_0^2 + \lambda_{12}^2) \equiv 0 \qquad (\mathrm{mod}\, p^\nu).$$

$$(22) \quad (\mu_0^2 + \mu_{12}^2)\lambda_0 \equiv 0, \qquad (\mu_0^2 + \mu_{12}^2)\lambda_{12} \equiv 0 \qquad (\mathrm{mod}\, p^\nu).$$

Comme $\mu_0$ et $\mu_{12}$ sont premiers entre eux, la norme $\lambda_0^2 + \lambda_{12}^2$ est nécessairement divisible par $p^\nu$, et comme $\lambda_0$ et $\lambda_{12}$ sont premiers entre eux, la norme $\mu_0^2 + \mu_{12}^2$ est aussi divisible par $p^\nu$. Donc, d'après ce qui précède, les entiers complexes proprement dits $(\lambda_0 + i\lambda_{12})$ et $(\mu_0 + i\mu_{12})$ appartiennent, le premier à une classe déterminée de solutions $(\xi_1, \xi_2)$, le second à une classe déterminée de solutions $(\eta_1, \eta_2)$ de la congruence (3). Si l'on convient de dire qu'un entier complexe est congru à zéro suivant un module entier réel lorsque sa partie réelle et sa partie imaginaire sont toutes deux divisibles par cet entier réel, on peut réunir en une seule les deux congruences (2) qui définissent

le système $(\xi_1, \xi_2)$ et écrire

$$(23) \qquad (\lambda_0 + i\lambda_{12})(\xi_1 + i\xi_2) \equiv 0 \pmod{p^\gamma}.$$

De même, au lieu des congruences (20), on peut écrire

$$(24) \qquad (\mu_0 + i\mu_{12})(\lambda_0 + i\lambda_{12}) \equiv 0 \pmod{p^\gamma}.$$

La congruence (23) montre que la solution $(\xi_1, \xi_2)$ est équivalente à $(\lambda_0, -\lambda_{12})$; de même, la solution $(\eta_1, \eta_2)$ est équivalente à $(\mu_0, -\mu_{12})$. Mais la congruence (24) montre que $(\mu_0, \mu_{12})$ est équivalent à $(\lambda_0, -\lambda_{12})$. La condition nécessaire demandée est donc que chacune des normes $\lambda_0^2 + \lambda_{12}^2$ et $\mu_0^2 + \mu_{12}^2$ soit divisible par $p^\gamma$ et que les solutions $(\mu_0, \mu_{12})$ et $(\lambda_0, -\lambda_{12})$ de la congruence (3) soient équivalentes. En répétant le même raisonnement dans l'ordre inverse, on voit facilement que ces conditions nécessaires sont aussi suffisantes. Nous ferons plusieurs fois usage de ce lemme.

On peut maintenant former un entier complexe proprement dit dont la norme soit égale à une puissance donnée $p^\gamma$ d'un nombre premier impair et qui appartienne à une classe donnée $(\zeta_1, \zeta_2)$ de solutions de la congruence (3). A cet effet, on commencera, en suivant la méthode indiquée plus haut, par former un nombre premier complexe $(\rho_0 + i\rho_{12})$ dont la norme soit égale à $p$ et qui appartienne à une classe donnée $(\xi_1, \xi_2)$ de solutions de la congruence $\xi_1^2 + \xi_2^2 \equiv 0 \pmod{p}$. Nous pouvons considérer la solution $(\zeta_1, \zeta_2)$ de la congruence (3) comme solution de la congruence $\xi_1^2 + \xi_2^2 \equiv 0 \pmod{p}$; $(\zeta_1, \zeta_2)$ est alors équivalent à $(\xi_1, \xi_2)$ ou à $(\xi_1, -\xi_2)$ : en admettant que ce soit à $(\xi_1, \xi_2)$ nous ne faisons aucune restriction; car, si c'était à $(\xi_1, -\xi_2)$, l'entier complexe $(\rho_0 - i\rho_{12})$ conjugué de $(\rho_0 + i\rho_{12})$ appartiendrait à la classe représentée par $(\xi_1, \xi_2)$ et pourrait être substitué dans ce qui suit à $(\rho_0 + i\rho_{12})$. Ainsi, en considérant les congruences suivant le module $p$, nous pouvons admettre que le système $(\zeta_1, \zeta_2)$ est équivalent au système $(\xi_1, \xi_2)$ et que le système $(\zeta_1, -\zeta_2)$ est équivalent au système $(\xi_1, -\xi_2)$. On formera ensuite les puissances successives de $(\rho_0 + i\rho_{12})$; d'après le lemme démontré, les parties réelles et imaginaires de ces puissances ne peuvent être toutes deux divisibles par $p$; or tout autre

diviseur premier que $p$, commun à ces deux parties, est impossible puisque $\rho_0^2 + \rho_{12}^2 = p$; donc elles sont premières entre elles. De plus, si l'on prend les congruences suivant le module $p^\gamma$, l'entier complexe $(\rho_0 + i\rho_{12})^\gamma$ ne peut appartenir qu'à la classe représentée par le système $(\zeta_1, \zeta_2)$ ou à la classe représentée par le système $(\zeta_1, -\zeta_2)$; la seconde alternative est impossible, car il en résulterait, si nous prenons les congruences suivant le module $p$, que l'entier complexe $(\rho_0 + i\rho_{12})^\gamma$ appartient à la classe représentée par le système $(\xi_1, -\xi_2)$ équivalent au système $(\zeta_1, -\zeta_2)$; tandis que la congruence

$$(\xi_1 + i\xi_2)^2 \equiv 2\xi_1(\xi_1 + i\xi_2) \pmod{p}$$

montre, au contraire, que, les congruences étant prises suivant le module $p$, une puissance quelconque de $(\rho_0 + i\rho_{12})$ appartient à la classe représentée par le système $(\xi_1, \xi_2)$; donc, les congruences étant prises suivant le module $p^\gamma$, l'entier complexe $(\rho_0 + i\rho_{12})^\gamma$, dont la norme est $p^\gamma$, appartient nécessairement à la classe représentée par le système $(\zeta_1, \zeta_2)$.

Soit enfin un entier impair quelconque $m$, ne contenant que des facteurs premiers de la forme $(4r + 1)$,

$$m = p^\gamma q^\delta \ldots.$$

Pour trouver un entier complexe dont la norme soit égale à $m$ et qui appartienne à des classes données de solutions de la congruence $\xi_1^2 + \xi_2^2 \equiv 0$, prise suivant les modules $p^\gamma$, $q^\delta$, ...., nous chercherons les nombres premiers complexes $(\rho_0 + i\rho_{12})$, $(\sigma_0 + i\sigma_{12})$, ... appartenant aux classes correspondantes de solutions de la congruence $\xi_1^2 + \xi_2^2 \equiv 0$ prise suivant les modules $p$, $q$, ... et nous formerons le produit

$$(\rho_0 + i\rho_{12})^\gamma (\sigma_0 + i\sigma_{12})^\delta \ldots = a + ib;$$

nous aurons alors $a^2 + b^2 = m$ et l'entier complexe proprement dit $(a + ib)$, dont les deux éléments $a$ et $b$ sont incongrus suivant le module 2, sera le nombre complexe entier cherché.

Si l'entier donné $m$ est le double d'un entier impair ne contenant que des facteurs premiers de la forme $4r + 1$, nous pouvons appliquer

ce qui précède à l'entier $\frac{m}{2}$ et former un entier complexe $a' + ib'$ dont la norme soit égale à $\frac{m}{2}$; mais alors, comme $(1 + i)$ est un nombre premier complexe, dont la norme est égale à 2, le produit

$$(1 + i)(a' + ib') = a + ib$$

est l'entier complexe cherché dont la norme est égale à $m$.

Pour tous les entiers $m$ qui peuvent être normes d'entiers complexes proprement dits, nous avons donc trouvé, et représenté comme produits de nombres premiers complexes, des entiers complexes proprement dits, dont la norme est $m$, appartenant à toutes les classes possibles. Nous montrerons, pour terminer, qu'en multipliant successivement les entiers complexes proprement dits trouvés par chacune des quatre unités, nous obtenons *tous* les entiers complexes proprement dits qui vérifient l'équation (1) et chacun *une fois* seulement.

Quand un nombre complexe entier proprement dit $(\lambda_0 + i\lambda_{12})$ est donné et que sa norme $m$ ou la moitié de sa norme est égale au produit $p^\gamma . q^\delta \ldots$, où les facteurs premiers impairs $p, q, \ldots$ sont nécessairement de la forme $4r + 1$, on peut mettre ce nombre complexe entier sous la forme d'un produit de nombres premiers complexes de la manière suivante : on cherche d'abord les classes de solutions, prises suivant les module $p^\gamma$, $q^\delta$, ..., auxquelles appartient le nombre complexe donné $(\lambda_0 + i\lambda_{12})$; on détermine ensuite les nombres premiers complexes $(\rho_0 + i\lambda_{12})$, $(\sigma_0 + i\sigma_{12})$, ..., dont les normes sont $p, q, \ldots$, et qui appartiennent aux classes de solutions correspondant aux précédentes, mais prises suivant les modules $p, q, \ldots$ (d'après une remarque faite plus haut, ces nombres premiers complexes sont déterminés sans ambiguïté); enfin on forme le produit

$$(\rho_0 + i\rho_{12})^\gamma (\sigma_0 + i\sigma_{12})^\delta \ldots,$$

que l'on multiplie encore par le facteur $(1 + i)$ quand le nombre entier $m$ est le double d'un nombre impair; on obtient ainsi un entier complexe que nous désignerons par $(a + ib)$.

Le lemme démontré et ce qui précède montrent que la partie réelle

et la partie imaginaire du produit

$$(\lambda_0 + i\lambda_{12})(a - ib)$$

sont toutes deux divisibles par $m$. Donc, comme la norme de ce produit est égale à $m^2$, ce produit lui-même est égal à l'entier $m$ multiplié par l'une des quatre unités $1, -1, i, -i$. Si $m$ est un nombre premier impair, il en résulte que l'entier complexe $(\lambda_0 + i\lambda_{12})$ est égal à l'une des quatre unités multipliée par le nombre premier complexe $(\rho_0 + i\rho_{12})$ appartenant à la même classe de solutions et défini sans ambiguïté. Dans le cas le plus général, l'entier complexe proprement dit donné $(\lambda_0 + i\lambda_{12})$ est, de même, égal à l'une des quatre unités multipliée par le produit de nombres premiers complexes définis sans ambiguïté et entièrement déterminés, sauf toutefois l'ordre dans lequel ils sont rangés dans le produit. Ceci montre que nous obtenons bien, par le procédé indiqué plus haut, *tous* les entiers complexes proprement dits vérifiant l'équation (1); chacun de ces entiers complexes est mis de toutes les manières possibles sous forme de produit de nombres premiers complexes si l'on range ces nombres premiers complexes de toutes les manières possibles. Le nombre d'entiers complexes proprement dits que l'on obtient ainsi est égal, comme on le voit immédiatement, à $4.2^n$, où $n$ désigne le nombre de facteurs premiers impairs différents contenus dans $m$.

On conclut des relations (7) du § I que toutes les substitutions rationnelles dont le déterminant est égal à $+1$, qui transforment une somme de deux carrés en elle-même, conduisent à un entier complexe proprement dit $\pm(\lambda_0 + i\lambda_{12})$; on obtient donc toutes ces substitutions en donnant dans les équations (14) du § I

$$\alpha_{11} = \alpha_{22} = \frac{\lambda_0^2 - \lambda_{12}^2}{\lambda_0^2 + \lambda_{12}^2}, \qquad \alpha_{12} = -\alpha_{21} = \frac{2\lambda_0\lambda_{12}}{\lambda_0^2 + \lambda_{12}^2},$$

à $\lambda_0$ et à $\lambda_{12}$ toutes les valeurs entières possibles pour lesquelles $(\lambda_0 + i\lambda_{12})$ est un entier complexe proprement dit. On peut facilement reconnaître dans quel cas les deux numérateurs et le dénominateur $\lambda_0^2 + \lambda_{12}^2$ de ces expressions ont un diviseur commun. Ce diviseur doit également diviser $2\lambda_0^2$ et $2\lambda_{12}^2$; donc, comme $\lambda_0$ et $\lambda_{12}$ et, par suite aussi,

$\lambda_0^2$ et $\lambda_{12}^2$ sont premiers entre eux, ce diviseur commun ne peut être que l'un des deux nombres 1 ou 2. Lorsque $\lambda_0^2 + \lambda_{12}$ est un entier impair, le numérateur $\lambda_0^2 - \lambda_{12}^2$ de $\alpha_{11}$ est impair; lorsque $\lambda_0^2 + \lambda_{12}^2$ est le double d'un entier impair, $\lambda_0^2 - \lambda_{12}^2$ est pair; le numérateur $2\lambda_0\lambda_{12}$ de $\alpha_{12}$ est évidemment toujours pair. Pour les valeurs de $\lambda_0$ et $\lambda_{12}$, pour lesquelles le dénominateur est un nombre impair, il n'y a donc pas d'autre diviseur commun aux deux numérateurs et au dénominateur que l'unité. Pour les valeurs de $\lambda_0$ et $\lambda_{12}$ pour lesquelles le dénominateur est pair, le diviseur commun est le nombre 2; on peut simplifier et le dénominateur réduit est alors un nombre impair comme dans le cas précédent. Ainsi les coefficients de toute substitution rationnelle qui transforme une somme de deux carrés en elle-même ont, comme dénominateur commun réduit, un nombre entier impair dont tous les facteurs premiers sont de la forme $4r + 1$.

## III.

### *Transformation réelle d'une somme de trois carrés en elle-même et définition des quaternions.*

Si une substitution linéaire à coefficients réels $\alpha_{11}$, $\alpha_{12}$, $\alpha_{13}$; $\alpha_{21}$, $\alpha_{22}$, $\alpha_{23}$; $\alpha_{31}$, $\alpha_{32}$, $\alpha_{33}$, qui représente les variables réelles $x_1$, $x_2$, $x_3$ en fonction des variables réelles $y_1$, $y_2$, $y_3$, transforme la somme des carrés des premières variables dans la somme des carrés des dernières, on a, à la fois, les équations

$$(1)\qquad \begin{cases} x_1 = \alpha_{11}y_1 + \alpha_{12}y_2 + \alpha_{13}y_3, \\ x_2 = \alpha_{21}y_1 + \alpha_{22}y_2 + \alpha_{23}y_3, \\ x_3 = \alpha_{31}y_1 + \alpha_{32}y_2 + \alpha_{33}y_3, \end{cases}$$

$$(2)\qquad x_1^2 + x_2^2 + x_3^2 = y_1^2 + y_2^2 + y_3^2.$$

Le déterminant de substitution ne peut alors être égal qu'à $+1$ ou à $-1$; supposons-le égal à $+1$. L'équation (2) est évidemment encore vérifiée, et la valeur du déterminant ne change pas si, au lieu de la substitution (1), nous en employons une autre déduite de (1) en mul-

tipliant par l'unité négative deux quelconques des trois colonnes de coefficients.

De chacun des quatre systèmes ainsi obtenus, on peut déduire un nouveau système en ajoutant l'unité à tous les éléments de celle des diagonales du déterminant de substitution correspondant qui joint le premier élément à gauche au dernier élément à droite. Les déterminants de ces quatre nouveaux systèmes,

$$(3)\qquad \begin{vmatrix} \alpha_{11}+1 & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22}+1 & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33}+1 \end{vmatrix},$$

$$(3_a)\qquad \begin{vmatrix} \alpha_{11}+1 & -\alpha_{12} & -\alpha_{13} \\ \alpha_{21} & -\alpha_{22}+1 & -\alpha_{23} \\ \alpha_{31} & -\alpha_{32} & -\alpha_{33}+1 \end{vmatrix},$$

$$(3_b)\qquad \begin{vmatrix} -\alpha_{11}+1 & \alpha_{12} & -\alpha_{13} \\ -\alpha_{21} & \alpha_{22}+1 & -\alpha_{23} \\ -\alpha_{31} & \alpha_{32} & -\alpha_{33}+1 \end{vmatrix},$$

$$(3_c)\qquad \begin{vmatrix} -\alpha_{11}+1 & -\alpha_{12} & \alpha_{13} \\ -\alpha_{21} & -\alpha_{22}+1 & \alpha_{23} \\ -\alpha_{31} & -\alpha_{32} & \alpha_{33}+1 \end{vmatrix}$$

sont respectivement égaux à

$$(4)\qquad 2+2\alpha_{11}+2\alpha_{22}+2\alpha_{33},$$

$$(4_a)\qquad 2+2\alpha_{11}-2\alpha_{22}-2\alpha_{33},$$

$$(4_b)\qquad 2-2\alpha_{11}+2\alpha_{22}-2\alpha_{33},$$

$$(4_c)\qquad 2-2\alpha_{11}-2\alpha_{22}+2\alpha_{33};$$

on le voit facilement, en tenant compte de ce que chaque élément du déterminant est égal au mineur correspondant. La somme de ces quatre valeurs étant égale au nombre 8, l'un au moins des quatre déterminants a une valeur différente de zéro. Cette remarque permet de supposer que le système donné de coefficients $\alpha_{11}, \alpha_{12}, \ldots \alpha_{33}$ est

tel que la valeur du déterminant (3) correspondant est différente de zéro. Nous ferons cette hypothèse dans tout ce qui suivra.

Les équations (1) donnent immédiatement

$$(5)\quad \begin{cases} x_1+y_1=(\alpha_{11}+1)y_1+\alpha_{12}y_2+\alpha_{13}y_3, \\ x_2+y_2=\alpha_{21}y_1+(\alpha_{22}+1)y_2+\alpha_{23}y_3, \\ x_3+y_3=\alpha_{31}y_1+\alpha_{32}y_2+(\alpha_{33}+1)y_3, \end{cases}$$

et, comme le déterminant (3) n'est pas nul, on peut tirer de ces équations, sans ambiguïté, $y_1, y_2$ et $y_3$ en fonction de $x_1+y_1$, $x_2+y_2$ et $x_3+y_3$. On obtient, par suite, les différences $x_1-y_1$, $x_2-y_2$, $x_3-y_3$ exprimées, sans ambiguïté, en fonction des sommes $x_1+y_1$, $x_2+y_2$, $x_3+y_3$. Il vient

$$(6)\quad \begin{cases} x_1-y_1=\dfrac{(\alpha_{12}-\alpha_{21})(x_2+y_2)+(\alpha_{13}-\alpha_{31})(x_3+y_3)}{1+\alpha_{11}+\alpha_{22}+\alpha_{33}}, \\ x_2-y_2=\dfrac{(\alpha_{21}-\alpha_{12})(x_1+y_1)+(\alpha_{23}-\alpha_{32})(x_3+y_3)}{1+\alpha_{11}+\alpha_{22}+\alpha_{33}}, \\ x_3-y_3=\dfrac{(\alpha_{31}-\alpha_{13})(x_1+y_1)+(\alpha_{32}-\alpha_{23})(x_2+y_2)}{1+\alpha_{11}+\alpha_{22}+\alpha_{33}}. \end{cases}$$

On peut représenter les coefficients qui paraissent dans ces relations (ils forment un système gauche) par des fractions ayant un dénominateur quelconque différent de zéro. Nous poserons

$$(7)\quad \begin{cases} \dfrac{\alpha_{12}-\alpha_{21}}{1+\alpha_{11}+\alpha_{22}+\alpha_{33}}=\dfrac{\lambda_{12}}{\lambda_0}, & \lambda_{12}+\lambda_{21}=0, \\ \dfrac{\alpha_{13}-\alpha_{31}}{1+\alpha_{11}+\alpha_{22}+\alpha_{33}}=\dfrac{\lambda_{13}}{\lambda_0}, & \lambda_{13}+\lambda_{31}=0, \\ \dfrac{\alpha_{23}-\alpha_{32}}{1+\alpha_{11}+\alpha_{22}+\alpha_{33}}=\dfrac{\lambda_{23}}{\lambda_0}, & \lambda_{23}+\lambda_{32}=0. \end{cases}$$

Au lieu des équations (6), nous pouvons alors écrire simplement

$$(8)\quad \begin{cases} x_1-y_1=\dfrac{\lambda_{12}(x_2+y_2)+\lambda_{13}(x_3+y_3)}{\lambda_0}, \\ x_2-y_2=\dfrac{\lambda_{21}(x_1+y_1)+\lambda_{23}(x_3+y_3)}{\lambda_0}, \\ x_3-y_3=\dfrac{\lambda_{31}(x_1+y_1)+\lambda_{32}(x_2+y_2)}{\lambda_0} \end{cases}$$

ou encore, en multipliant par $\lambda_0$,

$$(9)\qquad \begin{cases} \lambda_0 x_1 + \lambda_{21} x_2 + \lambda_{31} x_3 = \lambda_0 y_1 + \lambda_{12} y_2 + \lambda_{13} y_3, \\ \lambda_{12} x_1 + \lambda_0 x_2 + \lambda_{32} x_3 = \lambda_{21} y_1 + \lambda_0 y_2 + \lambda_{23} y_3, \\ \lambda_{13} x_1 + \lambda_{23} x_2 + \lambda_0 x_3 = \lambda_{31} y_1 + \lambda_{32} y_2 + \lambda_0 y_3. \end{cases}$$

Dans ce système d'equations linéaires, le déterminant des coefficients des premiers membres est égal au déterminant des coefficients des seconds membres; la valeur commune de ces deux déterminants est

$$(9^*)\qquad \lambda_0(\lambda_0^2 + \lambda_{12}^2 + \lambda_{13}^2 + \lambda_{23}^2).$$

Si l'on ajoute les trois équations (9) multipliées respectivement par $\lambda_{23}, \lambda_{31}, \lambda_{12}$, on obtient, en divisant les deux membres par $\lambda_0$ qui est différent de zéro, l'équation

$$(10)\qquad \lambda_{23} x_1 + \lambda_{31} x_2 + \lambda_{12} x_3 = \lambda_{23} y_1 + \lambda_{31} y_2 + \lambda_{12} y_3.$$

En joignant cette équation aux équations (9), on a un système de quatre équations dans lequel chacune des six colonnes contient les mêmes quatre éléments $\lambda_0, \lambda_{12}, \lambda_{13}, \lambda_{23}$, seulement dans un ordre différent et avec des signes parfois différents. Ajoutons, d'une part, les quatre premiers membres de ces équations, multipliés le premier par l'unité, les trois suivants par des symboles $i_{12}, i_{13}, i_{23}$; d'autre part, les quatre seconds membres de ces équations multipliés dans le même ordre par l'unité et les mêmes symboles; et demandons-nous s'il ne serait pas possible de soumettre les symboles $i_{12}, i_{13}, i_{23}$ à des règles de calcul telles que les deux sommes obtenues pussent être mises sous forme de produits de deux facteurs. Pour que la première somme soit égale au produit

$$(11)\qquad (\lambda_0 + i_{12}\lambda_{12} + i_{13}\lambda_{13} + i_{23}\lambda_{23})(x_1 + i_{12} x_2 + i_{13} x_3)$$

et que la seconde somme soit égale au produit

$$(12)\qquad (y_1 + i_{12} y_2 + i_{13} y_3)(\lambda_0 - i_{12}\lambda_{12} - i_{13}\lambda_{13} + i_{23}\lambda_{23}),$$

il faut et il suffit que les symboles $i_{12}$, $i_{13}$, $i_{23}$ vérifient les relations

$$(13)\quad \begin{cases} i_{12}^2 = -1, & i_{13}^2 = -1; & \\ i_{12}i_{13} = i_{23}, & i_{12}i_{23} = -i_{13}, & i_{13}i_{23} = i_{12}; \\ i_{13}i_{12} = -i_{23}, & i_{23}i_{12} = i_{13}, & i_{23}i_{13} = -i_{12}. \end{cases}$$

Pour que les symboles vérifient en outre la *loi d'associativité*, c'est-à-dire pour que l'on puisse grouper d'une manière arbitraire les divers facteurs d'un produit, sans toutefois changer l'ordre de ces facteurs, il faut et il suffit que l'on ait

$$(13^*)\qquad i_{23}^2 = -1.$$

Si nous supposons enfin que les symboles soient liés par les relations

$$(14)\qquad i_{21} = -i_{12}, \qquad i_{31} = -i_{13}, \qquad i_{32} = -i_{23},$$

nous pouvons, sans rien changer aux relations précédentes, permuter les indices 1, 2, 3 des symboles. En posant

$$(15)\qquad i = i_{12}, \qquad j = i_{23}, \qquad k = -i_{13},$$

nous observons que les relations établies sont identiques aux règles de calcul que Hamilton a introduites pour les unités des quaternions; l'expression

$$(16)\qquad \lambda_0 + i_{12}\lambda_{12} + i_{13}\lambda_{13} + i_{23}\lambda_{23}$$

devient alors le quaternion

$$(17)\qquad \lambda_0 + i\lambda_{12} + j\lambda_{23} + k\lambda_{31}.$$

On peut condenser les règles de calcul données par les relations (13), (13*) et (14), en supposant que les unités $i_{12}$, $i_{13}$, $i_{23}$ soient formées à l'aide de trois *symboles primitifs* $k_1$, $k_2$, $k_3$ de la manière suivante,

$$(18)\qquad i_{12} = k_1k_2, \qquad i_{13} = k_1k_3, \qquad i_{23} = k_2k_3,$$

*que la loi d'associativité ait lieu pour ces trois symboles primitifs,* et enfin *que l'on ait*

$$(19) \qquad \text{Pour } a = b, \quad k_a k_b = -1 \qquad (a, b = 1, 2, 3),$$

$$(20) \qquad \text{Pour } a \gtrless b, \quad k_a k_b = -k_b k_a \qquad (a, b = 1, 2, 3).$$

Ceci posé, égalons les deux expressions (11) et (12) déduites des premiers et des seconds membres des équations (9) et (10). En introduisant les symboles $\Lambda$, $\Lambda_1$, X, Y, définis par les équations

$$(21) \quad \begin{cases} \lambda_0 + i_{12}\lambda_{12} + i_{13}\lambda_{13} + i_{23}\lambda_{23} = \Lambda, & x_1 + i_{12}x_2 + i_{13}x_3 = X, \\ \lambda_0 - i_{12}\lambda_{12} - i_{13}\lambda_{13} + i_{23}\lambda_{23} = \Lambda_1, & y_1 + i_{12}y_2 + i_{13}y_3 = Y, \end{cases}$$

il vient

$$(22) \qquad \Lambda X = Y \Lambda_1.$$

Les équations (9) et (10) sont condensées dans l'unique équation symbolique (22).

Il résulte immédiatement des règles de calcul posées pour les trois symboles $i_{12}$, $i_{13}$, $i_{23}$ que le produit de deux quaternions est un quaternion; qu'en intervertissant l'ordre des facteurs, le produit n'est plus le même; qu'en faisant le produit de plusieurs quaternions, la loi d'associativité a lieu; enfin que, si l'on nomme *quaternion conjugué au quaternion* $\Lambda$ le quaternion

$$(23) \qquad \Lambda' = \lambda_0 + i_{21}\lambda_{12} + i_{31}\lambda_{13} + i_{32}\lambda_{23}$$

et *norme du quaternion* $\Lambda$ le produit $\Lambda\Lambda'$ du quaternion $\Lambda$ par son conjugué $\Lambda'$, on a

$$(24) \qquad \mathfrak{N}\Lambda = \lambda_0^2 + \lambda_{12}^2 + \lambda_{13}^2 + \lambda_{23}^2;$$

le quaternion conjugué de $\Lambda'$ est manifestement $\Lambda$, et l'on a

$$\mathfrak{N}\Lambda' = \mathfrak{N}\Lambda.$$

L'expression que nous venons de trouver pour cette norme est le

second facteur du déterminant (9*). (*Comparez* HAMILTON, *Lectures on Quaternions*, p. 87.)

En prenant comme point de départ une substitution (1), pour laquelle le déterminant (3) n'est pas nul, nous sommes parvenus à l'équation symbolique (22), dans laquelle $\lambda_0$ est différent de zéro. Si nous prenons inversement comme point de départ un quaternion quelconque $\Lambda$ dont la partie réelle $\lambda_0$ soit différente de zéro et si nous formons, à l'aide de ce quaternion, une équation (22), nous en déduisons les équations (9) et (10) correspondantes, et l'équation (10) est une conséquence des équations (9). Mais ces équations (9) nous montrent immédiatement que l'équation (2) est vérifiée, et, comme le déterminant (9*) est différent de zéro, nous obtenons, en résolvant les équations (9) par rapport à $x_1$, $x_2$, $x_3$, une substitution (1) entièrement déterminée; son déterminant est d'ailleurs égal à $+1$. Cette substitution, qui a été donnée pour la première fois par Euler, est la suivante :

$$
(25)\quad \left\{\begin{aligned}
x_1 &= \frac{\lambda_0^2-\lambda_{12}^2-\lambda_{13}^2+\lambda_{23}^2}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_1 \\
&\quad + \frac{2(\lambda_0\lambda_{12}-\lambda_{13}\lambda_{23})}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_2 + \frac{2(\lambda_0\lambda_{13}+\lambda_{12}\lambda_{23})}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_3, \\
x_2 &= \frac{2(-\lambda_0\lambda_{12}-\lambda_{13}\lambda_{23})}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_1 \\
&\quad + \frac{\lambda_0^2-\lambda_{12}^2+\lambda_{13}^2-\lambda_{23}^2}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_2 + \frac{2(-\lambda_0\lambda_{23}-\lambda_{12}\lambda_{13})}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_3, \\
x_3 &= \frac{2(-\lambda_0\lambda_{13}+\lambda_{12}\lambda_{23})}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_1 \\
&\quad + \frac{2(\lambda_0\lambda_{23}-\lambda_{12}\lambda_{13})}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_2 + \frac{\lambda_0^2+\lambda_{12}^2-\lambda_{13}^2-\lambda_{23}^2}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}y_3.
\end{aligned}\right.
$$

On la trouve dans le Mémoire d'Euler, intitulé : *Problema algebraicum ob affectiones prorsus singulares memorabile* (*N. Comm.*, XV, p. 75, 1770; *Exhib.*, 1770, Mart. 5, *Comm. ar.*, I, p. 427). Dans une Note publiée parmi ses Œuvres posthumes dans le Tome III de ses Œuvres complètes, et intitulée : *Bemerkungen zu einer Abhandlung Euler's über die orthogonale Substitution*, Jacobi a montré un intérêt particulier pour ce Mémoire d'Euler.

Le déterminant (3), correspondant à la substitution (25), est égal à

$$\frac{8\lambda_0^2}{\lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2}; \tag{26}$$

sa valeur est donc différente de zéro.

Ainsi tous les quaternions $\Lambda$, dont la partie réelle $\lambda_0$ est différente de zéro, nous ramènent à des substitutions linéaires (1), à déterminant $+1$, pour lesquelles le déterminant (3) est différent de zéro.

Comme on peut déduire une substitution (1), de déterminant $+1$, à déterminant (3) différent de zéro et telle que l'équation (2) soit encore vérifiée, en changeant les signes des coefficients de deux des colonnes d'une substitution (1) donnée, on obtient toutes les substitutions (1) considérées en composant les substitutions (1) obtenues jusqu'ici avec celles qui ont simplement pour effet de changer les signes des coefficients de deux colonnes. Les signes de la deuxième et de la troisième colonne sont changés par la substitution

$$y_1 = z_1, \qquad y_2 = -z_2, \qquad y_3 = -z_3,$$

que l'on peut remplacer par l'équation

$$i_{23}(y_1 + i_{12}y_2 + i_{13}y_3) = (z_1 + i_{12}z_2 + i_{13}z_3)i_{23}. \tag{27}$$

Les signes de la première et de la troisième colonne sont changés par une substitution que l'on peut remplacer par l'équation

$$i_{31}(y_1 + i_{12}y_2 + i_{13}y_3) = (z_1 + i_{12}z_2 + i_{13}z_3)(-i_{31}), \tag{27a}$$

et les signes de la première et de la deuxième colonne sont changés par une substitution que l'on peut remplacer par l'équation

$$i_{12}(y_1 + i_{12}y_2 + i_{13}y_3) = (z_1 + i_{12}z_2 + i_{13}z_3)(-i_{12}). \tag{27b}$$

En posant

$$z_1 + i_{12}z_2 + i_{13}z_3 = Z, \tag{28}$$

et successivement

$$(29)\qquad \begin{cases} \mathrm{I} = i_{23}, & i_{31}, & i_{12}, \\ \mathrm{I}_1 = i_{23}, & -i_{31}, & -i_{12}, \end{cases}$$

on peut écrire ces équations (27), ($27_a$), ($27_b$),

$$(30)\qquad \mathrm{IY} = \mathrm{ZI}_1,$$

et comme, d'après la relation (22), $\Lambda \mathrm{X} = \mathrm{Y}\Lambda_1$, on a, en combinant les relations (22) et (30) et en faisant usage de la loi d'associativité,

$$(31)\qquad \mathrm{I}\Lambda\mathrm{X} = \mathrm{ZI}_1\Lambda_1.$$

Cette relation, qui se déduit de la relation (22) en y remplaçant $\Lambda$ par $\mathrm{I}\Lambda$, jointe à la relation (22), représente, d'après ce que nous avons observé tout à l'heure, toutes les substitutions (1) considérées qui vérifient les équations (2), et dont le déterminant est égal à $+1$. Or un quaternion $\Lambda$ dont la partie réelle est différente de zéro devient, lorsqu'on le multiplie par $\mathrm{I} = i_{23}, i_{31}, i_{12}$, un nouveau quaternion dont la norme n'a pas changé et dont le coefficient de $i_{23}, i_{31}, i_{12}$ est successivement différent de zéro; les quaternions $\Lambda$ et $\mathrm{I}\Lambda$, qui paraissent dans les équations (22) et (31), représentent donc tous les quaternions dont l'un au moins des coefficients est différent de zéro, c'est-à-dire tous les quaternions dont la norme n'est pas nulle. On pourra donc remplacer l'ensemble des relations (22) et (31), où la partie réelle $\lambda_0$ du quaternion $\Lambda$ est supposée différente de zéro, par l'unique relation (22), en convenant de ne plus soumettre le quaternion $\Lambda$ qu'à la restriction d'avoir une norme différente de zéro.

Ainsi la relation (22), dans laquelle $\Lambda$ désigne un quaternion quelconque dont la norme n'est pas nulle, représente toutes les substitutions linéaires considérées. Les équations (25) ont maintenant lieu pour des valeurs réelles quelconques données à $\lambda_0, \lambda_{12}, \lambda_{13}, \lambda_{23}$, le système

$$\lambda_0 = \lambda_{12} = \lambda_{13} = \lambda_{23} = 0$$

étant seul exclu.

A l'aide d'un quaternion quelconque dont la norme n'est pas nulle,

$$\mu_0 + i_{12}\mu_{12} + i_{13}\mu_{13} + i_{23}\mu_{23} = \mathrm{M}, \tag{32}$$

formons la relation analogue à (22),

$$\mathrm{MY} = \mathrm{ZM}_1, \tag{33}$$

à laquelle correspond une substitution linéaire, semblable à (1), nous permettant de passer des variables réelles $y_1, y_2, y_3$ aux variables réelles $z_1, z_2, z_3$. Si nous tenons compte de la loi d'associativité, les relations (22) et (33), multipliées membre à membre, nous donnent une nouvelle relation

$$\mathrm{M\Lambda X} = \mathrm{ZM}_1\Lambda_1. \tag{34}$$

Les deux substitutions linéaires, appliquées successivement, ont donc pour effet d'introduire le produit $\mathrm{M\Lambda}$ des quaternions correspondant à ces deux substitutions linéaires. On voit sans difficulté que le conjugué de $\mathrm{M\Lambda}$ est $\Lambda'\mathrm{M}'$; la norme du produit $\mathrm{M\Lambda}$ est donc égale à $\mathrm{M\Lambda\Lambda'M}'$, c'est-à-dire à $\mathrm{M}\,\mathfrak{N}(\Lambda)\mathrm{M}'$ ou à $\mathfrak{N}(\mathrm{M})\,\mathfrak{N}(\Lambda)$.

De l'équation

$$\mathfrak{N}(\mathrm{M\Lambda}) = \mathfrak{N}(\mathrm{M})\,\mathfrak{N}(\Lambda), \tag{35}$$

on déduit immédiatement que *la norme d'un produit de quaternions est égale au produit des normes de ces quaternions.* Comme $\mathfrak{N}(\mathrm{M})$ et $\mathfrak{N}(\mathrm{M})$ sont supposés différents de zéro, $\mathfrak{N}(\mathrm{M\Lambda})$ est nécessairement différent de zéro. Je ne voudrais pas manquer de faire observer ici que l'équation (35) est, au fond, identique au théorème de l'art. 93 du Mémoire d'Euler : *Demonstratio theorematis Fermatiani*, etc., que j'ai cité en commençant, et que si l'on se propose de parvenir, par multiplications, du théorème d'Euler à l'équation (35), on obtient les règles du calcul des quaternions. (*Comparez* Hamilton, Ouvrage cité, Préface, p. 47.)

D'après ce que nous avons vu jusqu'ici, chaque quaternion $\Lambda$ ap-

partient à un *ensemble* de quaternions, ayant tous, aux signes près, mêmes coefficients de 1, $i_{12}$, $i_{13}$, $i_{23}$, et, par suite, ayant tous même norme. Les quaternions qui appartiennent au même ensemble peuvent être répartis en groupes semblables à ceux que Gauss a introduits pour les quantités complexes $(a + bi)$ dans son célèbre Mémoire sur les restes biquadratiques. Celles des huit quantités $\pm (a \pm bi)$ ayant mêmes éléments réels $a$ et $b$, que l'on obtient en multipliant successivement l'une d'entre elles par les quatre unités $1, -1, i, -i$, sont dites *associées*, tandis que celles qui ont même partie réelle et des coefficients de $i$ égaux, mais de signes contraires, sont dites *conjuguées*. Si l'on remarque qu'à chaque quaternion $\Lambda$ correspond une substitution (1) bien déterminée par la relation (22) et qu'au quaternion $-\Lambda$ correspond la même substitution (1), on est amené à répartir en groupes les quaternions d'un même ensemble d'après les changements que ces divers quaternions, substitués successivement dans l'équation (22), apportent à la substitution (1). Nous avons déjà observé qu'en changeant $\Lambda$ en $I\Lambda$ on changeait les signes des coefficients des deux colonnes désignées par les indices du symbole $i$ auquel est égal I; il y a 8 quaternions qui sont ainsi liés entre eux. Les quaternions d'un même ensemble, ayant même partie réelle $\lambda_0$, sont également au nombre de 8; on peut les mettre sous la forme

$$
\begin{aligned}
\Lambda &= \lambda_0 + i_{12}\lambda_{12} + i_{13}\lambda_{13} + i_{23}\lambda_{23},\\
\Lambda' &= \lambda_0 - i_{12}\lambda_{12} - i_{13}\lambda_{13} - i_{23}\lambda_{23},\\
\Lambda_1 &= \lambda_0 - i_{12}\lambda_{12} - i_{13}\lambda_{13} + i_{23}\lambda_{23} = i_{23}\Lambda\, i_{32},\\
\Lambda'_1 &= \lambda_0 + i_{12}\lambda_{12} + i_{13}\lambda_{13} - i_{23}\lambda_{23} = i_{23}\Lambda' i_{32},\\
\Lambda_2 &= \lambda_0 - i_{12}\lambda_{12} + i_{13}\lambda_{13} - i_{23}\lambda_{23} = i_{13}\Lambda\, i_{31},\\
\Lambda'_2 &= \lambda_0 + i_{12}\lambda_{12} - i_{13}\lambda_{13} + i_{23}\lambda_{23} = i_{13}\Lambda' i_{31},\\
\Lambda_3 &= \lambda_0 + i_{12}\lambda_{12} - i_{13}\lambda_{13} - i_{23}\lambda_{23} = i_{12}\Lambda\, i_{21},\\
\Lambda'_3 &= \lambda_0 - i_{12}\lambda_{12} + i_{13}\lambda_{13} + i_{23}\lambda_{23} = i_{12}\Lambda' i_{21}.
\end{aligned}
$$

En passant de $\Lambda$ à $\Lambda_k$ $(k = 1, 2, 3)$, la $k^{\text{ième}}$ ligne et la $k^{\text{ième}}$ colonne des coefficients de la substitution (1) changent de signe. En passant de $\Lambda$ à $\Lambda'$ ou de $\Lambda_k$ à $\Lambda'_k$ $(k = 1, 2, 3)$, les lignes et les colonnes de

même rang sont transposées. L'ensemble des quaternions que l'on obtient en combinant ces deux genres d'opérations comprend 64 quaternions; il y a 32 substitutions linéaires correspondantes; on les obtient toutes, à l'aide de l'une d'entre elles, en faisant subir à ses lignes et colonnes les changements que nous venons d'indiquer, combinés de toutes les manières possibles.

## IV.

### *Quaternions entiers et classes de solutions de la congruence* $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^\nu}$.

Je considère maintenant spécialement les quaternions dont les quatre éléments réels $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ sont des nombres entiers; on nomme ces quaternions : *quaternions entiers*. La répartition en groupes, dont nous venons de parler, va ici nous être d'une grande utilité.

Pour que la norme d'un quaternion entier

$$\Lambda = \lambda_0 + i_{12}\lambda_{12} + i_{13}\lambda_{13} + i_{23}\lambda_{23} \tag{1}$$

soit égale à l'unité, il faut que l'un de ses quatre éléments réels soit égal à $\pm 1$ et que les trois autres soient nuls. Il n'y a donc que 8 quaternions entiers dont la norme est égale à l'unité; ce sont les quaternions

$$\pm 1, \quad \pm i_{12}, \quad \pm i_{13}, \quad \pm i_{23}, \tag{2}$$

que l'on nomme *unités*. Si I désigne l'une quelconque de ces 8 unités, on a l'équation

$$\mathfrak{N}(I\Lambda) = \mathfrak{N}(\Lambda),$$

dont il a déjà été fait usage plus haut.

On peut d'abord démontrer que les 8 quaternions entiers $I\Lambda$ sont tous inégaux, pourvu que la norme $\mathfrak{N}(\Lambda)$ soit différente de zéro. Si l'on avait, en effet, l'égalité

$$I^{(\alpha)}\Lambda = I\Lambda,$$

dans laquelle $I^{(a)}$ et I désignent deux unités différentes, on aurait aussi

$$(I^{(a)} - I)\Lambda = 0$$

et, par suite,

$$\mathfrak{N}(I^{(a)} - I)\,\mathfrak{N}\Lambda = 0;$$

donc, comme $\mathfrak{N}\Lambda$ n'est pas nulle, il viendrait

$$I^{(a)} - I = 0,$$

et l'unité $I^{(a)}$ ne serait pas différente de l'unité I.

Je nommerai quaternion entier *proprement dit* tout quaternion entier dont les quatre éléments $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ n'ont pas de diviseur commun, et quaternion entier *impropre* tout quaternion entier dont les quatre éléments $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ ont un diviseur commun. La norme d'un quaternion entier proprement dit ne peut être qu'un nombre entier impair ou le double ou le quadruple d'un nombre entier impair. Si, en effet, cette norme est paire, il faut que deux des entiers $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ soient impairs ou que ces quatre entiers soient tous impairs; or, dans le premier cas, la norme est un entier de la forme $4r + 2$ et, dans le second cas, la norme est un entier de la forme $8r + 4$.

Si un quaternion entier, dont la norme est un nombre premier, est le produit de deux quaternions entiers, l'un de ces derniers a nécessairement pour norme le nombre premier lui-même, tandis que l'autre a pour norme l'unité et est, par suite, égal à l'une des huit unités (2). On peut ainsi considérer chaque quaternion entier, dont la norme est un nombre premier, comme irréductible et dire qu'il est un *quaternion premier*.

Supposons que l'on nous donne un quaternion entier proprement dit $\Lambda$; soit $m$ la norme de ce quaternion; désignons par $p$ l'un quelconque des facteurs premiers impairs de $m$ et soit $p^\gamma$ la puissance à laquelle paraît $p$ dans $m$. Comme le quaternion donné est un quaternion proprement dit, les quatre nombres entiers $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ ne sont pas tous les quatre divisibles par $p$; on peut donc, quel que soit le quaternion entier proprement dit donné $\Lambda$, toujours trouver un

quaternion $I\Lambda$ dont la norme soit aussi égale à $m$ et dont la partie réelle (le coefficient de l'unité réelle) ne soit pas divisible par $p$; mais alors rien n'empêche de supposer que, déjà dans le quaternion entier proprement dit donné, le nombre entier $\lambda_0$ ne soit pas divisible par $p$. Dans cette hypothèse on peut former le système de congruences

$$(4)\qquad \left.\begin{aligned} &\lambda_0\,\xi_1 + \lambda_{21}\xi_2 + \lambda_{31}\xi_3 \equiv 0,\\ &\lambda_{12}\xi_1 + \lambda_0\,\xi_2 + \lambda_{32}\xi_3 \equiv 0,\\ &\lambda_{13}\xi_1 + \lambda_{23}\xi_2 + \lambda_0\,\xi_3 \equiv 0, \end{aligned}\right\} \pmod{p^\nu}$$

et montrer que ce système est vérifié par des nombres entiers $\xi_1$, $\xi_2$, $\xi_3$ non divisibles tous trois par $p$. A cet effet, formons le système des mineurs

$$(5)\qquad \left\{\begin{aligned} &\lambda_0^2 + \lambda_{23}^2; && \lambda_{32}\lambda_{13} - \lambda_{12}\lambda_0; && \lambda_{12}\lambda_{23} - \lambda_{13}\lambda_0;\\ &\lambda_{23}\lambda_{31} - \lambda_{21}\lambda_0; && \lambda_0^2 + \lambda_{31}^2; && \lambda_{13}\lambda_{21} - \lambda_{23}\lambda_0;\\ &\lambda_{21}\lambda_{32} - \lambda_{31}\lambda_0; && \lambda_{31}\lambda_{12} - \lambda_{32}\lambda_0; && \lambda_0^2 + \lambda_{12}^2. \end{aligned}\right.$$

Si les trois sommes de carrés qui paraissent dans l'une des diagonales de ce tableau (5) étaient divisibles par $p$, comme l'on a

$$(6)\qquad \lambda_0^2 + \lambda_{12}^2 + \lambda_{13}^2 + \lambda_{23}^2 = m,$$

les sommes de carrés

$$\lambda_{12}^2 + \lambda_{31}^2, \quad \lambda_{12}^2 + \lambda_{23}^2, \quad \lambda_{23}^2 + \lambda_{31}^2$$

seraient aussi divisibles par $p$; mais alors les nombres entiers

$$2\lambda_0^2, \quad 2\lambda_{12}^2, \quad 2\lambda_{13}^2, \quad 2\lambda_{23}^2$$

seraient eux-mêmes divisibles par $p$, et, par suite, $p$ étant impair, les quatre entiers

$$\lambda_0, \quad \lambda_{12}, \quad \lambda_{13}, \quad \lambda_{23}$$

contiendraient $p$ simultanément, ce qui n'est pas. Chaque ligne du tableau (5) nous fournit trois entiers $\xi_1$, $\xi_2$, $\xi_3$, vérifiant les con-

gruences (4); comme l'une au moins des trois sommes de carrés qui paraissent dans le tableau (5) n'est pas divisible par $p$, la ligne dans laquelle paraît cette somme de carrés nous fournira trois entiers $\xi_1, \xi_2, \xi_3$, qui ne seront pas tous trois multiples de $p$. Si, par exemple, $\lambda_0^2 + \lambda_{12}^2$ n'est pas divisible par $p$, on peut prendre à volonté pour $\xi_3$ un entier quelconque non divisible par $p$ et les deux nombres entiers $\xi_1$, $\xi_2$ sont ensuite déterminés sans ambiguïté, suivant le module $p^\gamma$, par les deux premières congruences (4). On obtient facilement, en désignant par $\omega_1$, $\omega_2$ les solutions, pour $\xi_3 = 1$, des deux premières congruences (4), les relations

$$\left.\begin{array}{l} \lambda_{21}\lambda_{32} - \lambda_{31}\lambda_0 \equiv \omega_1(\lambda_0^2 + \lambda_{12}^2) \\ \lambda_{31}\lambda_{12} - \lambda_{32}\lambda_0 \equiv \omega_2(\lambda_0^2 + \lambda_{12}^2) \end{array}\right\} \pmod{p^\gamma}, \tag{7}$$

$$\xi_1 \equiv \omega_1 \xi_3, \quad \xi_2 \equiv \omega_2 \xi_3 \pmod{p^\gamma}. \tag{8}$$

Dans le numéro précédent nous avons déduit des équations (9) une équation (10); en observant que $\lambda_0$ ne contient pas $p$ en facteur, nous déduisons, ici de même, des congruences (4) une congruence

$$\lambda_{23}\xi_1 + \lambda_{31}\xi_2 + \lambda_{12}\xi_3 \equiv 0 \pmod{p^\gamma}. \tag{9}$$

Si, outre le système $(\xi_1, \xi_2, \xi_3)$ que nous venons d'obtenir, un second système $(\xi_1^{(1)}, \xi_2^{(1)}, \xi_3^{(1)})$ dont les éléments $\xi_1^{(1)}$ $\xi_2^{(1)}$, $\xi_3^{(1)}$ ne sont pas tous trois divisibles par $p$, vérifie les congruences (4) et (9), on reconnaît facilement, d'après ce qui précède, qu'il existe un entier $g$, non divisible par $p$, qui vérifie les congruences

$$\xi_1^{(1)} \equiv g\xi_1; \quad \xi_2^{(1)} \equiv g\xi_2; \quad \xi_3^{(1)} \equiv g\xi_3 \pmod{p^\gamma}.$$

Deux semblables systèmes de nombres $(\xi_1, \xi_2, \xi_3)$ et $(\xi_1^{(1)}, \xi_2^{(1)}, \xi_3^{(1)})$ dont l'un peut se déduire de l'autre en le multipliant par un nombre non divisible par $p$, peuvent être appelés *équivalents* et réunis dans une même *classe*.

En ajoutant les congruences (4) respectivement multipliées par $\xi_1, \xi_2, \xi_3$ et remarquant que $\lambda_0$ n'est pas divisible par $p$, on en déduit cette nouvelle congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^\gamma}. \tag{10}$$

Ainsi *les congruences* (4) *et* (9) *admettent une classe déterminée de solutions, laquelle constitue en même temps une classe de solutions de la congruence* (10).

Avec les trois entiers $\xi_1, \xi_2, \xi_3$ formons l'expression

$$\xi_1 + i_{12}\xi_2 + i_{13}\xi_3 = \Xi. \tag{11}$$

Alors les premiers membres des équations (4) et (9), respectivement multipliés par $1, i_{12}, i_{13}, i_{23}$ et ajoutés ensemble, donneront pour résultat le produit $\Lambda\Xi$. Si donc nous convenons de considérer un quaternion entier comme congru à zéro suivant un module donné réel lorsque chacun de ses coefficients est divisible par ce module, les congruences (4) et (9) pourront être condensées dans la congruence unique

$$\Lambda\Xi \equiv 0 \pmod{p^\nu}. \tag{12}$$

Il est aisé de voir que, si l'on remplace $\Lambda$ par $I\Lambda$, la congruence (12) est encore vérifiée, de sorte que les huit quaternions représentés par l'expression $I\Lambda$ appartiennent à la même classe de solutions $(\xi_1, \xi_2, \xi_3)$ de la congruence (10).

Les quaternions $\Lambda i_{12}, \Lambda i_{13}, \Lambda i_{23}$ appartiennent à des classes de solutions de la congruence (1) faciles à déterminer. De la congruence (12) on déduit, en effet,

$$\begin{cases} \Lambda i_{12}(i_{21}\Xi i_{12}) \equiv 0 \pmod{p^\nu}, \\ \Lambda i_{13}(i_{31}\Xi i_{13}) \equiv 0 \pmod{p^\nu}, \\ \Lambda i_{23}(i_{32}\Xi i_{23}) \equiv 0 \pmod{p^\nu}, \end{cases} \tag{12'}$$

et, comme

$$\begin{cases} i_{21}\Xi i_{12} = \xi_1 + i_{12}\xi_2 - i_{13}\xi_3, \\ i_{31}\Xi i_{13} = \xi_1 - i_{12}\xi_2 + i_{13}\xi_3, \\ i_{32}\Xi i_{23} = \xi_1 - i_{12}\xi_2 - i_{13}\xi_3, \end{cases} \tag{12''}$$

les classes cherchées sont déterminées par les systèmes

$$\begin{cases} (\xi_1, \quad \xi_2, -\xi_3) \text{ pour } \Lambda i_{12}, \\ (\xi_1, -\xi_2, \quad \xi_3) \text{ pour } \Lambda i_{13}, \\ (\xi_1, -\xi_2, -\xi_3) \text{ pour } \Lambda i_{23}. \end{cases} \tag{13}$$

Ces trois systèmes et le système $(\xi_1, \xi_2, \xi_3)$ appartiennent à quatre classes différentes lorsque aucun des trois nombres entiers $\xi_1$, $\xi_2$, $\xi_3$ n'est divisible par $p$; ils n'appartiennent qu'à deux classes différentes lorsqu'un de ces trois entiers est divisible par $p$.

Pour pouvoir étudier les quaternions proprement dits dont la norme est le double d'un nombre impair, il est nécessaire de considérer encore les congruences (4) et (9) par rapport au module 2. Nous avons déjà fait observer que, lorsque la norme d'un quaternion entier est le double d'un nombre impair, deux des entiers $\lambda_0, \lambda_{12}, \lambda_{13}, \lambda_{23}$ sont nécessairement pairs et les deux autres impairs; il en résulte qu'en prenant pour I une unité convenable, on peut toujours s'arranger de manière que la partie réelle $\lambda_0$ de $\Lambda$ soit un nombre impair. Mais alors deux des trois sommes de carrés contenues dans le Tableau (5) sont nécessairement des nombres impairs et la troisième est un nombre pair; supposons, pour fixer les idées, que $\lambda_0^2 + \lambda_{12}^2$ soit un nombre impair; on peut alors choisir pour $\xi_3$ un entier quelconque impair et $\xi_1, \xi_2$ sont ensuite déterminés sans ambiguïté suivant le module 2. On voit donc que les congruences (4) ne peuvent être vérifiées, suivant le module 2, que par un seul système de nombres entiers qui ne soient pas pairs tous les trois; ce même système vérifie aussi la congruence (9), ainsi que la congruence (10), prises toutes deux suivant le module 2. Les classes de solutions de la congruence (10) auxquelles appartiennent les quaternions entiers $\Lambda i_{12}$, $\Lambda i_{13}$, $\Lambda i_{23}$ sont encore représentées par les systèmes (13); mais ces systèmes, pris suivant le module 2, sont manifestement équivalents.

Ainsi, les résultats obtenus sont démontrés pour tout quaternion entier proprement dit lorsque le module est égal à une puissance d'un nombre premier impair contenue dans la norme du quaternion entier, et, en outre, pour les quaternions entiers proprement dits dont la norme est le double d'un nombre entier impair, lorsque le module est égal à 2.

## V.

### *Nombre de classes de solutions de la congruence* $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod{p^\gamma}$.

Lorsqu'une congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod{p^\gamma} \tag{1}$$

est vérifiée par un système d'entiers $(\xi_1, \xi_2, \xi_3)$ qui ne soient pas tous trois divisibles par le nombre premier impair $p$, nous dirons que ce système est une *solution proprement dite* de la congruence (1).

Nous avons démontré que la congruence (1) avait au moins une solution proprement dite lorsque le module $p^\gamma$ de cette congruence est un facteur de la norme $m$ d'un quaternion entier proprement dit. Nous allons maintenant étudier cette congruence (1) sans y associer aucune supposition particulière et déterminer *le nombre de classes de ses solutions proprement dites*.

Soit d'abord $\gamma = 1$. Nous commencerons par considérer les solutions pour lesquelles $\xi_3$ n'est pas divisible par $p$. Pour $\xi_3 = 1$, nous pouvons écrire au lieu de (1), en tenant compte de la définition de $\omega_1$ et $\omega_2$ donnée dans le numéro précédent, la congruence

$$\omega_1^2+\omega_2^2+1\equiv 0 \pmod{p}. \tag{2}$$

L'étude de cette congruence se ramène, comme je le montrerai tout à l'heure, à celle de la congruence

$$1+a^2\equiv b^2 \pmod{p}. \tag{3}$$

Cette dernière peut se mettre sous la forme

$$1\equiv(b-a)(b+a) \pmod{p}. \tag{4}$$

En posant

$$b-a=r, \qquad b+a=s, \tag{5}$$

on peut la remplacer par la congruence

$$1 \equiv rs \pmod{p}, \tag{6}$$

à laquelle il faut joindre, puisque $a$ et $b$ sont des nombres entiers, la congruence

$$r \equiv s \pmod{2}. \tag{6'}$$

La congruence (6) montre que le nombre entier $r$ ne peut être divisible par $p$; prenons pour $r$ successivement les $(p-1)$ restes incongrus suivant le module $p$, en excluant le reste 0; pour chacune de ces $(p-1)$ valeurs de $r$ déterminons la valeur correspondante de $s$, d'après la congruence (6), à un multiple de $p$ près, et fixons ce multiple de manière à vérifier la congruence (6'); nous obtiendrons ainsi $(p-1)$ paires de nombres entiers $(r, s)$ qui représenteront toutes les solutions des congruences (6) et (6'); nous en tirerons $(p-1)$ paires de nombres entiers $(a, b)$ à l'aide des relations

$$b = \frac{r+s}{2}, \qquad a = \frac{r-s}{2}, \tag{7}$$

et ces $(p-1)$ paires de nombres entiers $(a, b)$ représenteront toutes les solutions de la congruence (3). Ainsi la congruence (3) est toujours possible et a toujours $(p-1)$ solutions.

Pour passer de la congruence (3) à la congruence (2), nous allons distinguer le cas où l'on a $p \equiv 1 \pmod 4$, du cas où l'on a $p \equiv 3 \pmod 4$.

Si l'on a $p \equiv 1 \pmod 4$, $(-1)$ est résidu quadratique de $p$: il existe donc un nombre entier $\delta$ vérifiant la congruence

$$\delta^2 \equiv -1 \pmod{p}; \tag{8}$$

mais alors, pour chaque solution $(\omega_1, \omega_2)$ de la congruence (2), la congruence

$$1 + \omega_1^2 - \delta^2 \omega_2^2 \equiv 0 \pmod{p} \tag{9}$$

a lieu; cette dernière congruence montre que les nombres entiers

$$(10) \qquad a \equiv \omega_1, \qquad b \equiv \delta\omega_2 \qquad (\mathrm{mod}\, p)$$

vérifient la congruence (3). Inversement, à chaque solution $(a, b)$ de la congruence (3) correspond une paire d'entiers $(\omega_1, \omega_2)$, déterminés par les congruences (10), qui vérifient la congruence (2). Donc la congruence (2) a $(p-1)$ solutions.

Si l'on a $p \equiv 3 (\mathrm{mod}\, 4)$, le nombre $(-1)$ est non-résidu quadratique de $p$; il est donc impossible que parmi les solutions de la congruence (3) il y ait des systèmes $(a, b)$ pour lesquels le nombre entier $b$ soit divisible par $p$; il y a par contre deux solutions de la congruence (3), $(a \equiv 0, b \equiv \pm 1)$, pour lesquelles $a$ est divisible par $p$; en mettant ces deux solutions à part, il reste $(p-3)$ solutions $(a, b)$ de la congruence (3) pour lesquelles aucun des deux nombres entiers $a$ et $b$ n'est divisible par $p$. Ces $(p-3)$ solutions se partagent en $\frac{p-3}{4}$ groupes contenant chacun quatre solutions correspondantes $(\pm a, \pm b)$; chacun de ces groupes représente un des cas où l'un des $\frac{p-1}{2}$ résidus quadratiques de $p$, augmenté d'une unité, est de nouveau égal à un résidu quadratique de $p$; et, par ces $\frac{p-3}{4}$ groupes, il est tenu compte de tous les cas dont nous parlons. Il y a donc exactement $\frac{p-3}{4}$ résidus quadratiques de $p$ qui, augmentés d'une unité, sont de nouveau résidus quadratiques de $p$. Si l'on augmente d'une unité l'un des $\frac{p+1}{4}$ autres résidus quadratiques de $p$, on obtient un nombre entier qui n'est ni divisible par $p$, ni résidu quadratique de $p$ et est donc nécessairement non-résidu quadratique de $p$. Comme chaque résidu quadratique de $p$ est congru, suivant le module $p$, au carré d'un entier $c$, et, dans le cas qui nous occupe, chaque non-résidu quadratique au carré d'un entier $d$ pris avec le signe moins; comme, de plus, les entiers $c$ et $d$ peuvent être remplacés par $(-c)$ et $(-d)$, on voit que chacun des $\frac{p+1}{4}$ résidus quadratiques dont nous avons parlé en dernier lieu donne quatre solu-

tions de la congruence

$$1 + c^2 \equiv -d^2 \pmod{p}, \tag{11}$$

qui est identique à la congruence (2). Donc la congruence (2) a $(p+1)$ solutions.

Les deux cas que nous avons distingués nous amènent ainsi à des résultats différents. Suivant que l'on a $p \equiv 1$ ou $p \equiv 3 \pmod 4$, la congruence (2) a $(p-1)$ ou $(p+1)$ solutions. Cette différence apparaît également dans la marche suivie par M. Hermite (*comparez* le Mémoire cité dans l'introduction). Mais nous allons montrer que cette différence s'évanouit lorsqu'on détermine le nombre de classes de solutions proprement dites de la congruence proposée.

Dans le cas où l'on a $p \equiv 1 \pmod 4$, la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p} \tag{12}$$

peut être vérifiée en prenant pour $\xi_3$ un entier divisible par $p$; mais alors ni $\xi_1$ ni $\xi_2$ ne peuvent être divisibles par $p$, sans quoi nous n'aurions plus de solution proprement dite. Pour $\xi_3 \equiv 0 \pmod p$ la congruence (12) se réduit à

$$\xi_1^2 + \xi_2^2 \equiv 0 \pmod{p}; \tag{12'}$$

comme $\xi_1$ et $\xi_2$ ne sont pas divisibles par $p$, cette congruence a deux classes de solutions proprement dites (*comparez* § II). Ces deux classes, jointes aux $(p-1)$ classes pour lesquelles $\xi_3$ n'est pas divisible par $p$, donnent $(p+1)$ classes de solutions proprement dites de la congruence (12).

Dans le cas où l'on a $p \equiv 3 \pmod 4$, il est, au contraire, impossible que $\xi_3$ soit divisible par $p$; en effet, la congruence (12') ne peut être résolue, dans ce cas, que si l'on a à la fois $\xi_1 \equiv 0$, $\xi_2 \equiv 0 \pmod p$; l'hypothèse $\xi_3 \equiv 0 \pmod p$ ne nous donne donc aucune solution proprement dite de la congruence (12). Aucune classe de solutions ne s'ajoute ainsi aux $(p+1)$ classes pour lesquelles $\xi_3$ n'est pas divisible par $p$.

Enfin, si l'on forme une congruence semblable à la congruence (12), mais prise suivant le module 2,

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod 2, \tag{13}$$

on voit immédiatement que cette congruence n'a que trois solutions proprement dites; ce sont les solutions

$$\left.\begin{array}{lll} \xi_1\equiv 0, & \xi_2\equiv 1, & \xi_3\equiv 1 \\ \xi_1\equiv 1, & \xi_2\equiv 0, & \xi_3\equiv 1 \\ \xi_1\equiv 1, & \xi_2\equiv 1, & \xi_3\equiv 0 \end{array}\right\} \pmod 2. \tag{14}$$

On a donc démontré dans toute sa généralité le théorème :

*Le nombre de solutions proprement dites de la congruence* $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0$, *prise suivant un module premier quelconque* $p$, *est toujours égal à* $(p+1)$.

L'absence d'exception à ce théorème est, si je ne m'abuse, un caractère spécifique de la congruence (12). Comme chaque classe de solutions proprement dites comprend $(p-1)$ solutions incongrues suivant le module $p$, le nombre de toutes les solutions incongrues proprement dites est égal à $(p^2-1)$; en y ajoutant l'unique solution impropre $(\xi_1\equiv 0, \xi_2\equiv 0, \xi_3\equiv 0) \pmod p$, on voit que *le nombre total des solutions de la congruence* (12) *est égal au carré* $p^2$ *du module premier* $p$ *de cette congruence.*

Connaissant le nombre de classes de solutions proprement dites de la congruence (12), nous allons chercher à déterminer par induction le nombre de classes de solutions proprement dites de la congruence (1), où le module est $p^\gamma$; $(\gamma>1)$.

Supposons, à cet effet, que nous connaissions un système de solutions proprement dites $(\xi_1, \xi_2, \xi_3)$ de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod{p^{\gamma-1}};$$

nous pouvons alors déterminer trois nombres entiers $t_1$, $t_2$, $t_3$ de ma-

nière que la somme des carrés des trois expressions

$$\xi_1 + t_1 p^{\gamma-1}, \quad \xi_2 + t_2 p^{\gamma-1}, \quad \xi_3 + t_3 p^{\gamma-1}$$

soit divisible par $p^\gamma$. En effet, comme $\gamma \geq 2$, on a $2(\gamma-1) \geq \gamma$; les termes contenant $p^{2(\gamma-1)}$ sont donc nécessairement divisibles par $p^\gamma$; en tenant compte de cette observation, on voit que la somme des carrés des trois expressions précédentes est ou n'est pas divisible par $p^\gamma$, suivant que l'expression

$$\frac{\xi_1^2 + \xi_2^2 + \xi_3^2}{p^{\gamma-1}} + 2(\xi_1 t_1 + \xi_2 t_2 + \xi_3 t_3) \tag{15}$$

est ou n'est pas divisible par $p$. Mais nous avons déjà observé que, dans un système de solutions proprement dites, un seul des trois entiers $\xi_1, \xi_2, \xi_3$ pouvait être divisible par $p$; supposons, pour fixer les idées, que $\xi_1$ et $\xi_2$ ne le soient pas. On peut assigner à $t_2$ une valeur fixe arbitraire et donner successivement à $t_3$ toute la série des valeurs incongrues suivant le module $p$. Les valeurs correspondantes de $t_1 \pmod p$ seront déterminées sans ambiguïté par la condition que l'expression (15) soit divisible par $p$. [On pourrait, au contraire, déterminer $t_1$ de telle sorte que (15) ne fût pas divisible par $p$, auquel cas la somme de trois carrés ne serait pas divisible par $p^\gamma$. Cette remarque nous servira plus tard.]

Les $p$ solutions proprement dites (pour le module $p^\gamma$) déduites de la solution $(\xi_1, \xi_2, \xi_3)$ pour une même valeur de $t_2$ et des valeurs différentes de $t_3$ appartiennent évidemment à des classes différentes. On voit donc que le nombre de classes de solutions proprement dites de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^\gamma}$$

est exactement $p$ fois plus grand que le nombre de classes de solutions proprement dites de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^{\gamma-1}}.$$

Il est donc égal à $p^{\gamma-1}(p+1)$.

Il se présente une exception pour le passage du nombre premier 2 à

son carré 4. Pour que la congruence

$$(16) \qquad \xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod 4$$

ait un système de solutions proprement dites $(\xi_1, \xi_2, \xi_3)$, il faut que l'un des trois nombres entiers $\xi_1, \xi_2, \xi_3$ soit pair et que les deux autres soient impairs; mais alors la somme des carrés de ces trois nombres est de la forme $4r+2$ et ne peut donc pas être divisible par 4. *La congruence* (16) *n'a donc aucun système de solutions proprement dites.*

## VI.

PROBLÈME. — *Trouver tous les quaternions entiers dont la norme soit égale à un nombre entier donné.*

Ce qui précède nous permet d'aborder le problème fondamental de la théorie des quaternions entiers. Un nombre entier $m$, impair ou double ou quadruple d'un nombre impair, étant donné, trouver tous les quaternions entiers proprement dits dont la norme soit égale au nombre $m$ et représenter, de toutes les manières possibles, chacun de ces quaternions comme produit de quaternions premiers.

Considérons d'abord le cas particulier où le nombre entier donné est un nombre premier impair $p$. Soit alors $(\xi_1, \xi_2, \xi_3)$ un système représentant une classe déterminée de solutions de la congruence

$$(1) \qquad \xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod p.$$

Je vais démontrer qu'il existe un quaternion entier proprement dit dont la norme est égale à $p$ et qui appartient à la classe déterminée par le système $(\xi_1, \xi_2, \xi_3)$. A cet effet, déterminons les quatre entiers $\tau\rho_0$, $\tau\rho_{12}$, $\tau\rho_{13}$, $\tau\rho_{23}$ numériquement plus petits que $\frac{p}{2}$ qui vérifient les congruences

$$2) \quad \tau\rho_0 \equiv \xi_1, \qquad \tau\rho_{12} \equiv \xi_2, \qquad \tau\rho_{13} \equiv \xi_3, \qquad \tau\rho_{23} \equiv 0 \pmod p;$$

soit $\tau$ le plus grand commun diviseur de ces quatre entiers; $\tau$ ne peut

être divisible par $p$. Posons ensuite

$$\rho_0 + i_{12}\rho_{12} + i_{13}\rho_{13} + i_{23}\rho_{23} = \mathrm{P}, \tag{3}$$

$$\xi_1 + i_{12}\xi_2 + i_{13}\xi_3 = \Xi; \tag{4}$$

comme $\tau$ et $p$ sont premiers entre eux, le système des congruences (4) et (9) du § IV, qui est condensé dans la congruence (12) du même paragraphe, est vérifié pour les valeurs

$$\rho_0 = \lambda_0, \qquad \rho_{12} = \lambda_{12}, \qquad \rho_{13} = \lambda_{13}, \qquad \rho_{23} = \lambda_{23}.$$

Nous avons donc ici la congruence

$$\mathrm{P}\Xi \equiv 0 \pmod{p}. \tag{5}$$

La norme du quaternion P est égale à la somme de quatre carrés, chacun plus petit que $\frac{p^2}{4}$; elle est donc plus petite que $p^2$; comme elle est divisible par $p$, nous pouvons d'ailleurs écrire

$$\mathfrak{N}(\mathrm{P}) = pt, \tag{6}$$

et $t$ est alors nécessairement plus petit que $p$. Si $t$ est égal à l'unité, le problème est résolu par le quaternion P lui-même. Si $t$ est différent de l'unité, nous déterminerons quatre nombres entiers $\varphi_0$, $\varphi_{12}$, $\varphi_{13}$, $\varphi_{23}$, numériquement inférieurs ou au plus égaux à $\frac{t}{2}$ et vérifiant les congruences

$$\varphi_0 \equiv \rho_0, \qquad \varphi_{12} \equiv \rho_{12}, \qquad \rho_{13} \equiv \rho_{13}, \qquad \varphi_{23} \equiv \rho_{23} \pmod{t}. \tag{7}$$

Il est facile de s'assurer que les quatre nombres entiers $\varphi_0$, $\varphi_{12}$, $\varphi_{13}$, $\varphi_{23}$, ainsi obtenus, ne peuvent être tous les quatre numériquement égaux à $\frac{t}{2}$; lorsque $t$ est différent de 2, cela résulte simplement de ce que les quatre entiers $\rho_0$, $\rho_{12}$, $\rho_{13}$, $\rho_{23}$, auxquels $\varphi_0$, $\varphi_{12}$, $\varphi_{13}$, $\varphi_{23}$ sont congrus, n'ont, par définition, aucun diviseur commun; lorsque $t$ est

égal à 2, on aurait

$$\rho_0 \equiv 1, \qquad \rho_{12} \equiv 1, \qquad \rho_{13} \equiv 1, \qquad \rho_{23} \equiv 1 \pmod 2,$$

et, par suite,

$$\mathfrak{N}(P) \equiv 4 \pmod 8,$$

contrairement à l'égalité (6) qui, pour $t = 2$, est $\mathfrak{N}(P) = 2p$. La norme $\mathfrak{N}(\Phi)$ du quaternion

$$\Phi = \varphi_0 + i_{12}\varphi_{12} + i_{13}\varphi_{13} + i_{23}\varphi_{23} \tag{8}$$

est donc plus petite que $t^2$, et, comme elle est divisible par $t$, on a, en posant

$$\mathfrak{N}(\Phi) = tt^{(1)}, \tag{9}$$

l'inégalité $t^{(1)} < t$.

Si l'on multiplie le quaternion $\Phi'$, conjugué de $\Phi$, par le quaternion P, on obtient un nouveau quaternion dont les quatre éléments réels sont divisibles par $t$, comme il est facile de s'en assurer. Outre $t$, ces quatre éléments réels peuvent encore avoir un autre facteur commun; soit $\tau^{(1)}t$ leur plus grand commun diviseur; posons alors

$$\Phi' P = \tau^{(1)} t(\rho_0^{(1)} + i_{12}\rho_{12}^{(1)} + i_{13}\rho_{13}^{(1)} + i_{23}\rho_{23}^{(1)}), \tag{10}$$

$$P^{(1)} = \rho_0^{(1)} + i_{12}\rho_{12}^{(1)} + i_{13}\rho_{13}^{(1)} + i_{23}\rho_{23}^{(1)}; \tag{11}$$

$P^{(1)}$ sera un quaternion entier proprement dit. On a, d'après (6) et (9),

$$\mathfrak{N}(\Phi' P) = pt^2 t^{(1)};$$

comme $t$ et $t^{(1)}$ sont plus petits que $p$, cette norme ne peut être divisible par $p^2$; or, d'après (10) et (11), on a aussi

$$\mathfrak{N}(\Phi' P) = (\tau^{(1)})^2 t^2 \mathfrak{N}(P^{(1)});$$

donc $\tau^{(1)}$ ne peut être divisible par $p$.

On peut déduire facilement de la congruence (5), la congruence

$$\Phi' P \Xi \equiv 0 \pmod{p}, \tag{12}$$

en n'effectuant que des additions et des multiplications par des nombres entiers réels, opérations qui sont identiques dans le calcul des quaternions et dans le calcul ordinaire. Les relations (10) et (11) donnent

$$\Phi' P = \tau^{(1)} t P^{(1)};$$

la congruence (12) peut donc s'écrire

$$\tau^{(1)} t P^{(1)} \Xi \equiv 0 \pmod{p}$$

ou encore, comme les nombres entiers $\tau^{(1)}$ et $t$ ne sont pas divisibles par $p$,

$$P^{(1)} \Xi \equiv 0 \pmod{p}. \tag{13}$$

De l'égalité

$$\mathfrak{N}(\Phi' P) = t^2 t^{(1)} p = t^2 (\tau^{(1)})^2 \mathfrak{N}(P^{(1)})$$

on déduit d'ailleurs, comme $\tau^{(1)}$ et $p$ sont premiers entre eux, que $t^{(1)}$ est divisible par $(\tau^{(1)})^2$, et l'on a

$$\mathfrak{N}(P^{(1)}) = p \frac{t^{(1)}}{(\tau^{(1)})^2}. \tag{14}$$

Au lieu des relations (5) et (6), nous avons donc deux relations (13) et (14) dans lesquelles le quaternion entier proprement dit $P^{(1)}$ et le nombre entier $\frac{t^{(1)}}{(\tau^{(1)})^2}$ remplacent le quaternion proprement dit P et le nombre entier $t$; on a d'ailleurs manifestement l'inégalité $\frac{t^{(1)}}{(\tau^{(1)})^2} < t$.

Rien n'empêche de répéter le même raisonnement et de former successivement des quaternions $P^{(2)}$, $P^{(3)}$, ..., vérifiant les relations (5) et (6), comme P et $P^{(1)}$, et ayant dans l'équation (6) un coefficient entier de $p$ de plus en plus petit, jusqu'à ce que ce coefficient entier soit égal à l'unité. Nous arrivons ainsi à former un quaternion entier

proprement dit,

$$P^{(s)} = \rho_0^{(s)} + i_{12}\rho_{12}^{(s)} + i_{13}\rho_{13}^{(s)} + i_{23}\rho_{23}^{(s)}$$

vérifiant les relations

$$P^{(s)}\Xi \equiv 0 \pmod{p}, \tag{15}$$

$$\mathfrak{N}(P^{(s)}) = p. \tag{16}$$

Le problème posé est donc résolu pour tout nombre premier impair $p$. Le quaternion $P^{(s)}$ est un *quaternion premier* qui appartient à la classe donnée de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$. Les huit quaternions premiers $IP^{(s)}$ appartiennent à la même classe de solutions; nous choisirons arbitrairement l'un de ces huit quaternions et nous nous en servirons dans les calculs suivants. Nous aurons alors, par le procédé indiqué, $p+1$ quaternions premiers dont la norme est $p$, appartenant chacun à l'une des $p+1$ classes de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$.

A chaque quaternion premier P, dont la norme est un nombre premier impair, correspond un quaternion conjugué P′ qui a même norme que P et est donc aussi un quaternion premier. Nous allons démontrer que les deux quaternions conjugués P et P′ ne peuvent appartenir à la même classe de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$. Pour cela, formons, en suivant la méthode indiquée dans le § IV et remplaçant la lettre $\lambda$ par la lettre $\rho$, deux systèmes $(\xi_1, \xi_2, \xi_3)$ et $(\xi_1^{(1)}, \xi_2^{(1)}, \xi_3^{(1)})$ auxquels correspondent respectivement les quaternions P et P′. Nous pouvons supposer que $\rho_0$ et $\rho_0^2 + \rho_{12}^2$, par exemple, ne soient pas divisibles par $p$ et choisir alors pour $\xi_3$, comme pour $\xi_3^{(1)}$, un entier quelconque non divisible par $p$; nous prendrons

$$\xi_3 = \xi_3^{(1)} = \rho_0^2 + \rho_{12}^2;$$

nous aurons alors

$$\xi_1 = \rho_{21}\rho_{32} - \rho_{31}\rho_0, \qquad \xi_2 = \rho_{31}\rho_{12} - \rho_{32}\rho_0,$$
$$\xi_1^{(1)} = \rho_{12}\rho_{23} - \rho_{13}\rho_0, \qquad \xi_2^{(1)} = \rho_{13}\rho_{21} - \rho_{23}\rho_0.$$

Si les deux systèmes $(\xi_1, \xi_2, \xi_3)$ et $(\xi_1^{(1)}, \xi_2^{(1)}, \xi_3^{(1)})$ étaient équivalents,

il faudrait, comme $\xi_3$ et $\xi_3^{(1)}$ sont égaux et ne sont pas divisibles par $p$, que l'on eût

$$\xi_1^{(1)} - \xi_1 \equiv 2\rho_{31}\rho_0 \equiv 0, \qquad \xi_2^{(1)} - \xi_2 \equiv 2\rho_{32}\rho_0 \equiv 0 \qquad (\mathrm{mod}\, p);$$

il viendrait donc

$$\rho_{31} \equiv 0, \qquad \rho_{32} \equiv 0 \qquad (\mathrm{mod}\, p)$$

et, par suite, comme $\rho_0^2 + \rho_{12}^2 + \rho_{13}^2 + \rho_{23}^2 = p$,

$$\rho_0^2 + \rho_{12}^2 \equiv 0 \qquad (\mathrm{mod}\, p),$$

contrairement à l'hypothèse. Les deux quaternions premiers conjugués P et P′ appartiennent donc nécessairement à des classes différentes.

Si le nombre premier donné est le nombre 2, on a à vérifier l'équation

$$\lambda_0^2 + \lambda_{12}^2 + \lambda_{13}^2 + \lambda_{23}^2 = 2. \tag{17}$$

Pour cela, il faut et il suffit que deux des quatre carrés qui paraissent dans cette équation soient égaux à l'unité, et que les deux autres soient nuls. Les vingt-quatre quaternions premiers, dont les éléments vérifient cette condition, se répartissent entre les trois classes (14) de solutions proprement dites de la congruence (13) du § V. I représentant l'une quelconque des huit unités, les quaternions

$$(18)\quad \left\{\begin{array}{llll} \mathrm{I}(1+i_{23}) \text{ appartiennent à la classe} & \xi_1 \equiv 0, & \xi_2 \equiv 1, & \xi_3 \equiv 1 \\ \mathrm{I}(1+i_{31}) \qquad\qquad » & \xi_1 \equiv 1, & \xi_2 \equiv 0, & \xi_3 \equiv 1 \\ \mathrm{I}(1+i_{12}) \qquad\qquad » & \xi_1 \equiv 1, & \xi_2 \equiv 1, & \xi_3 \equiv 0 \end{array}\right\} (\mathrm{mod}\, 2).$$

Deux quaternions conjugués appartiennent ici à la même classe, comme on s'en assure facilement.

Afin de pouvoir passer du cas où le nombre donné est premier au cas où il est composé, il nous faut établir les conditions nécessaires et suffisantes pour qu'un produit de deux quaternions proprement

dits M et Λ soit divisible par une puissance déterminée $p^\gamma$ d'un nombre premier impair $p$.

De la congruence

$$\mathrm{M}\Lambda \equiv 0 \pmod{p^\gamma}, \tag{19}$$

on déduit les congruences

$$\begin{cases} \mathrm{M}'\mathrm{M}\Lambda = \mathfrak{N}(\mathrm{M})\Lambda \equiv 0 \pmod{p^\gamma}, \\ \mathrm{M}\Lambda\Lambda' = \mathrm{M}\mathfrak{N}(\Lambda) \equiv 0 \pmod{p^\gamma} \end{cases} \tag{20}$$

ou, comme Λ et M sont des quaternions proprement dits,

$$\mathfrak{N}(\mathrm{M}) \equiv 0, \qquad \mathfrak{N}(\Lambda) \equiv 0 \pmod{p^\gamma}.$$

Soient $p^{\gamma+l}$ la plus haute puissance de $p$ qui divise le nombre entier $\mathfrak{N}(\Lambda)$, et $p^{\gamma+m}$ la plus haute puissance de $p$ qui divise le nombre entier $\mathfrak{N}(\mathrm{M})$. Le quaternion Λ′ appartient alors à une classe de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^{\gamma+l}}$ ; soit $(\xi_1^{(1)}, \xi_2^{(1)}, \xi_3^{(1)})$ un système représentant cette classe. Le quaternion M appartient à une classe de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^{\gamma+m}}$; soit $(\eta_1, \eta_2, \eta_3)$ un système représentant cette classe. Si nous posons

$$\xi_1^{(1)} + i_{12}\xi_2^{(1)} + i_{13}\xi_3^{(1)} = \Xi^{(1)}, \tag{21}$$

$$\eta_1 + i_{12}\eta_2 + i_{13}\eta_3 = \mathrm{H}, \tag{22}$$

nous aurons alors

$$\Lambda'\Xi^{(1)} \equiv 0 \pmod{p^{\gamma+l}}, \tag{23}$$

$$\mathrm{MH} \equiv 0 \pmod{p^{\gamma+m}}. \tag{24}$$

Comme, d'après (19), on a

$$\mathrm{M}\Lambda \equiv 0 \pmod{p^\gamma},$$

il vient aussi, en prenant, au lieu du quaternion MΛ, son conju-

gué $\Lambda'M'$,

$$\Lambda'M' \equiv 0 \pmod{p^\gamma}. \tag{25}$$

On en déduit, en tenant compte de la congruence (24),

$$\Lambda'M'MH \equiv 0 \pmod{p^{2\gamma+m}};$$

mais, par hypothèse, $p^{\gamma+m}$ est la plus haute puissance de $p$ contenue dans la norme $M'M$; on a donc, en supprimant ce facteur, une nouvelle congruence

$$\Lambda'H \equiv 0 \pmod{p^\gamma}, \tag{26}$$

qui montre que le quaternion $\Lambda'$ appartient à la classe représentée par $(\eta_1, \eta_2, \eta_3)$.

Pour que le produit de deux quaternions proprement dits M et $\Lambda$ soit divisible par $p^\gamma$, il faut donc que les normes de chacun de ces quaternions soient divisibles par $p^\gamma$, et que les deux quaternions M et $\Lambda'$ appartiennent à une même classe de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^\gamma}.$$

Ces conditions nécessaires sont aussi suffisantes, car de la congruence (26) on déduit la congruence

$$H'\Lambda \equiv 0 \pmod{p^\gamma}, \tag{27}$$

qui, combinée à la congruence (24), donne une nouvelle congruence

$$MHH'\Lambda \equiv 0 \pmod{p^{2\gamma+m}}; \tag{28}$$

mais il résulte immédiatement d'une observation faite dans le § V, à propos du choix des entiers $t_1$, $t_2$, $t_3$ pour lesquels la congruence (15) n'est pas vérifiée, que l'on peut toujours choisir $\eta_1$, $\eta_2$, $\eta_3$ de manière que la norme $HH'$ ne soit pas divisible par une puissance de $p$ supérieure à $p^{\gamma+m}$; en divisant par $\mathfrak{N}(H)$, la congruence (28) devient

donc

$$M\Lambda \equiv 0 \pmod{p^\nu},$$

qui n'est autre que la congruence (19).

Un raisonnement semblable nous amène à reconnaître qu'un produit de deux quaternions proprement dits, M et Λ, ne peut être divisible par le nombre 2 que si la norme de chacun des deux facteurs est paire. En nous bornant, ce qui suffit pour l'objet que nous avons en vue, au cas où les deux normes $\mathfrak{N}(M)$ et $\mathfrak{N}(\Lambda)$ sont chacune le double d'un nombre impair, on verrait qu'il faut, en outre, que les deux quaternions M et Λ appartiennent à la même classe de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod 2$. Ces conditions nécessaires sont aussi suffisantes.

Ceci posé, passons au cas où le nombre entier donné est égal au carré $p^2$ d'un nombre impair $p$. Nous avons vu, dans le § V, que les quaternions proprement dits dont la norme est égale à $p^2$ peuvent appartenir à $p(p+1)$ classes de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^2}.$$

Nous allons montrer que, pour tout nombre premier $p$, à chacune de ces $p(p+1)$ classes appartiennent effectivement des quaternions proprement dits dont la norme est égale à $p^2$.

A une classe quelconque de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$$

appartient un quaternion P. Le quaternion P′ appartient à une autre classe qui diffère nécessairement de la première, comme nous l'avons remarqué. Considérons les $p$ quaternions dont la norme est égale à $p$ et qui appartiennent aux $p$ classes de solutions qui restent après la suppression de celle à laquelle appartient P′. Soit Θ l'un quelconque de ces $p$ quaternions; le produit

$$\Theta P \tag{29}$$

est alors, d'après le lemme démontré, un quaternion proprement dit.

Si l'on remplace P successivement par $p+1$ quaternions $P^{(a)}$ appartenant aux $p+1$ classes possibles et si, pour chaque quaternion $P^{(a)}$, on remplace successivement $\Theta$ par les $p$ quaternions $\Theta^{(b)}$ qu'il représente, on obtient $p(p+1)$ quaternions proprement dits $\Theta^{(b)}P^{(a)}$. Supposons que deux de ces quaternions, $\Theta^{(b)}P^{(a)}$ et $\Theta P$ par exemple, appartiennent à la même classe de solutions $(\zeta_1, \zeta_2, \zeta_3)$ de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod{p^2};$$

on aurait alors, en posant

$$Z=\zeta_1+i_{12}\zeta_2+i_{13}\zeta_3, \tag{30}$$

deux congruences

$$\Theta P Z\equiv 0 \pmod{p^2}, \qquad \Theta^{(b)}P^{(a)}Z\equiv 0 \pmod{p^2}. \tag{31}$$

De la première, on déduit la relation

$$Z'P'\Theta'\equiv 0 \pmod{p^2};$$

mais la seconde, multipliée par cette relation, donne

$$\Theta^{(b)}P^{(a)}ZZ'P'\Theta'\equiv 0 \pmod{p^4},$$

et, comme on peut choisir les $\zeta$ de telle sorte que la norme $ZZ'$, qui est divisible par $p^2$, ne soit pas divisible par une puissance supérieure de $p$, il vient, en divisant par $\mathfrak{N}(Z)$,

$$\Theta^{(b)}P^{(a)}P'\Theta'\equiv 0 \pmod{p^2}. \tag{32}$$

En multipliant cette congruence par $\Theta$, on aurait donc, comme $\Theta'\Theta=p$, la congruence

$$\Theta^{(b)}P^{(a)}P'\equiv 0 \pmod{p}.$$

Mais alors, d'après le lemme, les deux quaternions $\Theta^{(b)}P^{(a)}$ et P appartiennent nécessairement à la même classe de solutions de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod{p}.$$

On déduit de même des équations (31) que les deux quaternions $\Theta P$ et $P^{(a)}$ appartiennent à la même classe de solutions de la congruence précédente. Mais, par hypothèse, les deux quaternions $\Theta P$ et $\Theta^{(b)}P^{(a)}$ appartiennent à la même classe de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^2};$$

à plus forte raison appartiennent-ils à la même classe de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$. Donc les deux quaternions P et $P^{(a)}$ appartiennent à la même classe de solutions de la dernière congruence, ce qui revient à dire que P et $P^{(a)}$ sont identiques. L'égalité $P^{(a)}P' = PP' = p$ montre ensuite que la congruence (32) se réduit à

$$\Theta^{(b)}\Theta' \equiv 0 \pmod{p};$$

il en résulte que les deux quaternions $\Theta^{(b)}$ et $\Theta$ appartiennent à la même classe de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$, et sont, par suite, identiques. Nous arrivons ainsi à conclure que les deux quaternions $\Theta^{(b)}P^{(a)}$ et $\Theta P$ sont identiques. Il est donc impossible que deux des $p(p+1)$ quaternions proprement dits $\Theta^{(b)}P^{(a)}$ appartiennent à la même classe de solutions prises suivant le module $p^2$.

Le même procédé qui vient de nous permettre de passer du cas où le nombre entier donné est égal à $p$ au cas où il est égal à $p^2$, nous permet de passer du cas où il est égal à $p^2$ au cas où il est égal à $p^3$, et ainsi de suite jusqu'à une puissance quelconque $p^\gamma$ de $p$. Nous multiplierons chaque fois, de droite à gauche, les expressions analogues à (29) par un nouveau quaternion, à norme égale à $p$, appartenant successivement à $p$ des $p+1$ classes de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p};$$

la classe à exclure est chaque fois celle à laquelle appartient le conjugué du facteur voisin de droite, comme c'était le cas dans les expressions (29). Nous obtiendrons ainsi, pour chacune des $p^{\gamma-1}(p+1)$ classes possibles de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^\gamma}$, un quaternion appartenant à cette classe.

En considérant le produit de deux quelconques des quaternions

premiers dont la norme est égale à 2, quaternions que nous avons formés plus haut (18), on reconnaîtra qu'il est égal à un quaternion proprement dit ou à un quaternion impropre suivant que les deux quaternions premiers appartiennent à des classes de solutions différentes ou à la même classe. Ce fait est d'accord avec celui que nous avons déjà mentionné, que les quaternions conjugués appartiennent ici à la même classe de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod 2.$$

Les quaternions proprement dits, dont la norme est égale à 4, sont, comme chaque unité peut être prise positive ou négative, au nombre de 16, et se répartissent, d'après les notations précédemment employées, en deux groupes

$$(34) \qquad \mathrm{I}(1 + i_{23} + i_{31} + i_{12}), \quad \mathrm{I}(1 + i_{32} + i_{13} + i_{21}),$$

I désignant, comme précédemment, une unité quelconque. On peut obtenir les quantités entre parenthèses, paraissant dans ces quaternions (34), à l'aide des quaternions dont la norme est égale à 2, de plusieurs manières, comme le montrent les relations suivantes :

$$(35) \quad \begin{cases} (1 + i_{23})(1 + i_{31}) = (1 + i_{31})(1 + i_{12}) \\ \qquad\qquad = (1 + i_{12})(1 + i_{23}) = 1 + i_{23} + i_{31} + i_{12}, \\ (1 + i_{13})(1 + i_{32}) = (1 + i_{21})(1 + i_{13}) \\ \qquad\qquad = (1 + i_{32})(1 + i_{21}) = 1 + i_{32} + i_{13} + i_{21}. \end{cases}$$

Je passe enfin au cas où le nombre entier donné $m$ est un nombre composé. Pour représenter tous les quaternions entiers proprement dits dont la norme est $m$, nous commencerons par décomposer $m$ en ses facteurs premiers; soient $m = \sigma p^\gamma q^\delta, \ldots, p, q, \ldots$ étant les facteurs premiers impairs contenus dans $m$; d'après le § IV, $\sigma$ est alors nécessairement l'un des nombres 1, 2, 4. Nous formerons ensuite pour chacune des $p^{\gamma-1}(p+1)$ classes de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p^\gamma},$$

un quaternion $\Lambda^{(a)}$ appartenant à cette classe; pour chacune des $q^{\delta-1}(q+1)$ classes de solutions de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \qquad (\mathrm{mod}\, q^\delta),$$

un quaternion $\mathrm{M}^{(b)}$ appartenant à cette classe, etc., et nous multiplierons de droite à gauche ces quaternions $\Lambda^{(a)}$, $\mathrm{M}^{(b)}$, ...; le produit

$$\Omega^{(a,b,\ldots)}=\ldots \mathrm{M}^{(b)}\Lambda^{(a)} \tag{36}$$

représentera alors $p^{\gamma-1}(p+1)q^{\delta-1}(q+1)\ldots$ quaternions. Nous multiplierons enfin chaque quaternion $\Omega^{(a,b,\ldots)}$, à gauche, successivement par chacune des huit unités I, quand $\sigma=1$; par chacun des vingt-quatre quaternions proprement dits (18) dont la norme est égale à 2, quand $\sigma=2$; par chacun des seize quaternions proprement dits (34) dont la norme est égale à 4, quand $\sigma=4$. Nous obtiendrons ainsi, pour $\sigma=1,2,4$, un nombre de quaternions dont la norme est égale à $m$. respectivement égal à

$$\left\{\begin{array}{l} 8p^{\gamma-1}(p+1)q^{\delta-1}(q+1)\ldots, \\ 8.3p^{\gamma-1}(p+1)q^{\delta-1}(q+1)\ldots, \\ 8.2p^{\gamma-1}(p+1)q^{\delta-1}(q+1)\ldots. \end{array}\right. \tag{37}$$

Je vais démontrer que ces quaternions représentent *tous les quaternions proprement dits, dont la norme est égale à m, chacun pris une seule fois.*

En effet, ces quaternions sont d'abord des quaternions proprement dits; car les normes des quaternions proprement dits $\Lambda^{(a)}$, $\mathrm{M}^{(b)}$, ... sont des puissances de nombres premiers impairs différents. Ces quaternions proprement dits appartiennent, de plus, à des classes de solutions de la congruence $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0$ qui ne sont pas les mêmes pour tous les modules $p^\gamma$, $q^\delta$, ...; car, si deux quaternions, ... $\mathrm{M}^{(b)}\Lambda^{(a)}$ et ... $\mathrm{M}\Lambda$ par exemple, appartenaient à une même classe représentée par $(\zeta_1,\zeta_2,\zeta_3)$, nous aurions, en formant comme plus haut l'expression (30)

$$\mathrm{Z}=\zeta_1+i_{12}\zeta_2+i_{13}\zeta_3,$$

les deux congruences

$$(38)\quad \ldots M\Lambda Z \equiv o \pmod{p^\gamma}; \qquad \ldots M^{(b)}\Lambda^{(a)}Z \equiv o \pmod{p^\gamma};$$

nous aurions donc

$$Z'\Lambda'M'\ldots \equiv o \pmod{p^\gamma},$$

puis

$$\ldots M^{(b)}\Lambda^{(a)}ZZ'\Lambda'M'\ldots \equiv o \pmod{p^{2\gamma}}$$

et, comme on peut faire en sorte que le nombre réel $ZZ'$, divisible par $p^\gamma$, ne soit divisible par aucune puissance de $p$ supérieure à $p^\gamma$, il viendrait, en divisant par $N(Z)$,

$$\ldots M^{(b)}\Lambda^{(a)}\Lambda'M'\ldots \equiv o \pmod{p^\gamma}.$$

En multipliant, à droite, par les quaternions conjugués aux quaternions $\ldots M'$, et en divisant par les normes $\ldots \mathfrak{N}(M)$ qui sont des nombres premiers à $p$, on obtient la congruence

$$\ldots M^{(b)}\Lambda^{(a)}\Lambda' \equiv o \pmod{p^\gamma};$$

en multipliant ensuite, à gauche, par les quaternions conjugués aux quaternions $\ldots M^{(b)}$, et en divisant par les normes $\ldots \mathfrak{N}(M^{(b)})$ qui sont premières à $p$, on obtient la congruence

$$\Lambda^{(a)}\Lambda' \equiv o \pmod{p^\gamma},$$

de laquelle on conclut que les deux quaternions $\Lambda^{(a)}$ et $\Lambda$ appartiennent à la même classe de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv o \pmod{p^\gamma}.$$

On démontre ensuite, de même, que si les congruences (38), prises suivant le module $q^\delta$, sont vérifiées, les deux quaternions $M^{(b)}$ et $M$ appartiennent à la même classe de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv o \pmod{q^\delta},$$

et l'on continue ainsi jusqu'à ce que l'on ait épuisé tous les facteurs premiers contenus dans $m$. Deux quelconques des quaternions obtenus, dont le nombre est indiqué par les équations (37), ne peuvent donc appartenir à la même classe de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0,$$

prise suivant tous les modules $p^\gamma, q^\delta, \ldots$.

Enfin, tout quaternion proprement dit A dont la norme est égale à $\sigma p^\gamma q^\delta \ldots$ est contenu dans le système de quaternions que nous avons formé. En effet, comme par rapport à chacun des entiers $p^\gamma, q^\delta, \ldots$, pris comme module, A appartient à une classe déterminée de solutions de la congruence

$$\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0,$$

on peut choisir, parmi les quaternions représentés par l'équation (36), un quaternion $\Omega$ appartenant, pour chacun des modules $p^\gamma, q^\delta, \ldots$ à la même classe que A. Si alors on multiplie A par le quaternion $\Omega'$, conjugué de $\Omega$, on obtient un quaternion $A\Omega'$ qui, d'après le lemme, est divisible par chacun des facteurs $p^\gamma, q^\delta, \ldots$, et, par suite, est divisible par le produit $p^\gamma q^\delta \ldots$. Comme $\mathfrak{N}(\Omega')$ est un nombre impair, le quaternion $A\Omega'$ ne peut d'ailleurs jamais être divisible par 2, que $\sigma$ soit égal à 1, 2 ou 4. De l'équation

$$\mathfrak{N}(A\Omega') = \sigma p^{2\gamma} q^{2\delta} \ldots$$

nous tirons

$$\mathfrak{N}\left(\frac{A\Omega'}{p^\gamma q^\delta \ldots}\right) = \sigma.$$

Pour $\sigma = 1$, la norme du quaternion entier proprement dit $\frac{A\Omega'}{p^\gamma q^\delta \ldots}$ est donc égale à l'unité; ce quaternion entier est, par suite, égal à l'une des huit unités I. Pour $\sigma = 2$, le quaternion entier proprement dit $\frac{A\Omega'}{p^\gamma q^\delta \ldots}$ est égal à l'un des vingt-quatre quaternions (18); pour $\sigma = 4$, il est égal à l'un des seize quaternions (34). Nous désignerons par E, pour $\sigma = 2$, l'un quelconque des vingt-quatre quaternions (18); pour

$\sigma = 4$, l'un quelconque des seize quaternions (34). Nous aurons alors

$$(39)\qquad \begin{cases} \text{Pour } \sigma = 1 \ldots\ldots\ldots & A\Omega' = I p^{\gamma} q^{\delta} \ldots \\ \text{Pour } \sigma = 2, 4 \ldots\ldots\ldots & A\Omega' = E p^{\gamma} q^{\delta} \ldots \end{cases}$$

En multipliant ces équations par $\Omega$, il vient

$$(40)\qquad \begin{cases} \text{Pour } \sigma = 1 \ldots\ldots\ldots\ldots\ldots & A = I\Omega \\ \text{Pour } \sigma = 2, 4 \ldots\ldots\ldots\ldots\ldots & A = E\Omega \end{cases}$$

Nous avons déjà montré que les huit quaternions $I\Omega$, correspondant aux huit valeurs de I, sont différents; on montrerait, de même, que les vingt-quatre ou seize quaternions $E\Omega$, correspondant aux vingt-quatre ou seize valeurs de E, sont différents.

Ainsi, le quaternion donné A, à norme $m$, est égal à un et à un seul des quaternions proprement dits différents qui composent le système de quaternions, à norme $m$, que nous avons formé.

Connaissant, par les relations (37), le nombre de quaternions proprement dits dont la norme est égale à un nombre entier donné $m$, on peut trouver facilement le nombre total de quaternions, tant proprement dits qu'impropres, dont la norme est égale à $m$, en tenant compte de tous les diviseurs communs possibles. On obtient alors le résultat, dû à Jacobi et déjà mentionné plus haut, que ce nombre total est, pour une norme impaire, égal à huit fois la somme de tous les diviseurs de la norme, et, pour une norme paire, égal à huit fois la somme de tous les diviseurs de la norme qui sont impairs ou égaux au double d'un nombre impair.

## VII.

Problème. — *Représenter, de toutes les manières possibles, un quaternion proprement dit donné, par un produit de quaternions premiers.*

C'est dans la résolution de ce problème que la différence entre la théorie des entiers complexes de Gauss et celle des quaternions entiers va nettement s'accuser.

Une fois que l'on a représenté, d'une certaine manière, un nombre complexe entier proprement dit par un produit de nombres premiers complexes pris dans un ordre déterminé, on sait que, pour le représenter de toutes les manières possibles, il suffit de permuter de toutes les manières possibles les nombres premiers complexes. Au contraire, une fois que l'on a trouvé tous les quaternions premiers dont les normes sont des diviseurs de la norme d'un quaternion entier proprement dit donné, on peut fixer arbitrairement un certain ordre pour les normes de ces quaternions premiers, et cet ordre détermine, comme nous allons le montrer, ceux de ces quaternions premiers dont le produit, pris dans cet ordre, est égal au quaternion proprement dit donné.

En effet, soit A un quaternion entier proprement dit donné dont la norme $\mathfrak{N}(A)$ est un nombre impair ou le double d'un nombre impair et soit $p$ un nombre premier, pair ou impair, arbitrairement choisi parmi les facteurs de $\mathfrak{N}(A)$; A appartient à une classe déterminée $(\xi_1, \xi_2, \xi_3)$ de solutions de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$. Soit P un quaternion premier dont la norme soit égale à $p$ et qui appartienne à la même classe de solutions $(\xi_1, \xi_2, \xi_3)$. Le produit AP′ est alors divisible par $p$; en désignant par G un quaternion entier, on peut donc écrire

$$AP' = pG. \tag{1}$$

Comme $\mathfrak{N}(P') = p$, on déduit de cette égalité la suivante :

$$A = GP. \tag{2}$$

Le quaternion proprement dit donné A est ainsi mis sous la forme d'un produit dont le facteur de gauche est un quaternion entier proprement dit G, et le facteur de droite un quaternion premier P, à norme $p$, appartenant à la classe de solutions $(\xi_1, \xi_2, \xi_3)$ de la congruence $\xi_1^2 + \xi_2^2 + \xi_3^2 \equiv 0 \pmod{p}$ à laquelle appartient le quaternion A lui-même. On reconnaît aussi, en raisonnant comme nous l'avons déjà fait plusieurs fois, que si l'on demande de mettre un quaternion entier proprement dit donné A sous la forme d'un produit de deux facteurs dont le premier, celui de gauche, soit un quaternion entier et le second,

celui de droite, un quaternion premier à norme $p$, ce dernier appartient nécessairement à la même classe de solutions de la congruence $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod p$ que le quaternion donné A. Dans l'équation (2), le quaternion premier P est donc entièrement déterminé; on peut toutefois remplacer P par un des huit quaternions IP.

Répétons maintenant sur le quaternion entier proprement dit G le raisonnement que nous venons de faire sur le quaternion entier proprement dit donné A. Nous commençons par choisir arbitrairement parmi les facteurs de $\frac{\mathfrak{N}(A)}{p}$ un nombre premier $q$ qui peut d'ailleurs être différent de $p$ ou égal à $p$. La classe de solutions de la congruence $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod q$ à laquelle appartient G détermine entièrement, à des facteurs près I, le quaternion premier dont la norme est égale à $q$ et qui est facteur de droite de G. Si, au lieu de P, on avait choisi précédemment, dans l'équation (2), le quaternion IP, il faudrait, pour former la classe de solutions de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod q,$$

prendre, au lieu de G, le quaternion GI; il en résulterait un changement de classe donné par les équations (12′) du § IV.

On peut continuer ainsi jusqu'à ce qu'on ait déterminé le dernier quaternion premier, avec l'unité qui doit le multiplier à gauche, et reconstitué ainsi le quaternion A.

Dans le cas où la norme $\mathfrak{N}(A)$ du quaternion entier proprement dit donné est divisible par 4, on peut appliquer la même méthode tant que l'on choisit des facteurs premiers *impairs* de $\mathfrak{N}(A)$ pour les normes des facteurs premiers cherchés de A, comptés de la droite vers la gauche. Mais, lorsqu'on fixe, pour la première fois, le nombre entier 2 comme norme du facteur premier à former, on peut choisir pour ce facteur premier *l'un quelconque* des 24 quaternions premiers E qui appartiennent cependant aux trois classes différentes de solutions de la congruence $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod 2$. En effet, soit B le quaternion entier proprement dit dont la norme est divisible par le nombre entier 4 et que l'on veut mettre sous la forme d'un produit de deux facteurs dont le second (celui de droite) soit un quaternion premier ayant une norme égale au nombre entier 2. Soit E l'un quel-

conque des quaternions premiers de norme 2. Le produit BE est un quaternion dont la norme est divisible par 8, mais n'est divisible par aucune puissance plus élevée de 2. Ce produit ne peut donc être que le double d'un quaternion entier proprement dit C. De l'équation

$$BE = 2C$$

nous déduisons, en multipliant, à droite, par le quaternion premier E′ conjugué de E et en tenant compte de ce que C est un quaternion proprement dit, l'équation

$$B = CE';$$

E′ est, comme E, l'un quelconque des 24 quaternions premiers dont la norme est égale à 2, et C est un quaternion entier proprement dit dont la norme est impaire ou égale au double d'un nombre impair. La détermination des facteurs de C rentre donc dans le cas précédent.

Nous avons ainsi obtenu le résultat suivant :

*On peut toujours représenter un quaternion entier proprement dit donné, dont la norme est un nombre impair ou le double d'un nombre impair, par un produit de quaternions premiers, en imposant à ces quaternions de se suivre, de droite à gauche, dans un ordre tel que leurs normes suivent un ordre fixé arbitrairement pour les facteurs premiers de la norme du quaternion donné. Chacun des quaternions premiers qui figurent dans le produit appartient alors à une classe de solutions déterminée, de proche en proche, sans ambiguïté. Tout se passe de même pour les quaternions entiers proprement dits dont la norme est divisible par 4 jusqu'à ce que l'ordre fixé pour les facteurs de cette norme amène pour la première fois le nombre 2. On peut alors choisir arbitrairement, comme facteur premier, l'un quelconque des 24 quaternions premiers dont la norme est égale à 2. Ce choix une fois fait, les classes de solutions auxquelles appartiennent les quaternions premiers dont les normes sont les nombres premiers suivants, pris dans l'ordre indiqué, sont déterminées, de proche en proche, sans ambiguïté, jusqu'à la fin.*

Prenons comme exemple le quaternion

$$-1+3i_{12}+i_{13}+2i_{23}$$

dont la norme est égale à 15. Il appartient à la classe de solutions de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod 3$$

qui est représentée par le système

$$\xi_1\equiv 1, \qquad \xi_2\equiv 2, \qquad \xi_3\equiv 2 \pmod 3$$

et à la classe de solutions de la congruence

$$\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod 5$$

qui est représentée par le système

$$\xi_1\equiv 0, \qquad \xi_2\equiv 1, \qquad \xi_3\equiv 2 \pmod 5.$$

Les quaternions

$$1+i_{12}+i_{13}, \quad 1+i_{12}-i_{13}, \quad 1-i_{12}+i_{13}, \quad 1-i_{12}-i_{13},$$

dont la norme est 3, appartiennent aux quatre classes de solutions possibles de la première des deux congruences précédentes.

Les quaternions

$$1+2i_{12}, \quad 1-2i_{12}, \quad 1+2i_{13}, \quad 1-2i_{13}, \quad 1+2i_{23}, \quad 1-2i_{23},$$

dont la norme est 5, appartiennent aux six classes de solutions possibles de la seconde des deux congruences précédentes.

Pour mettre le quaternion donné, dont la norme est égale à 3.5, sous la forme d'un produit de deux facteurs, nous pouvons demander que la norme du facteur de droite soit égale à 3; nous obtenons alors la solution

$$-1+3i_{12}+i_{13}+2i_{23}=(1+2i_{12})(1+i_{12}+i_{13});$$

mais nous pouvons aussi demander que la norme du facteur de droite soit égale à 5 : nous obtenons alors la solution

$$-1+3i_{12}+i_{13}+2i_{23}=-(1-i_{12}+i_{13})(1-2i_{23}).$$

Dans les deux manières précédentes de représenter le même quaternion, les facteurs premiers qui correspondent à chacune des deux normes appartiennent à des classes de solutions différentes.

## VIII.

*Substitutions, à coefficients rationnels, qui transforment une somme de trois carrés en elle-même. Composition de ces substitutions.*

La théorie que nous venons de développer, de la décomposition des quaternions entiers en quaternions premiers, nous permet d'écrire toutes les substitutions, à coefficients rationnels, qui transforment une somme de trois carrés en elle-même. Euler a, le premier, appelé l'attention sur ces substitutions dans son Mémoire déjà cité : *Problema algebraicum ob affectiones prorsus singulares memorabile*. On peut, comme nous l'avons montré dans le § III, passer de toute substitution à coefficients rationnels transformant une somme de trois carrés en elle-même et ayant un déterminant égal à $+1$ à une autre substitution semblable pour laquelle le déterminant (3) est différent de zéro. Les équations (7) du § III nous montrent que la substitution rationnelle choisie conduit à quatre nombres entiers réels $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$, n'ayant aucun diviseur commun, entièrement déterminés, au même facteur $\pm 1$ près. A cette substitution rationnelle correspond donc un quaternion entier proprement dit, déterminé au facteur $\pm 1$ près,

$$(1) \qquad \pm(\lambda_0+i_{12}\lambda_{12}+i_{13}\lambda_{13}+i_{23}\lambda_{23}).$$

Quatre des huit quaternions

$$(2) \qquad 1(\lambda_0+i_{12}\lambda_{12}+i_{13}\lambda_{13}+i_{23}\lambda_{23}),$$

qui appartiennent à la même classe de solutions, nous donnent ensuite

les substitutions provenant de la substitution choisie en changeant les signes des coefficients de deux quelconques des trois colonnes. Pour obtenir toutes les substitutions rationnelles, il faut donc considérer tous les quaternions entiers proprement dits.

Les équations (25) du § III nous donnent les coefficients $\alpha_{11}$, $\alpha_{12}$, ..., $\alpha_{33}$ de la substitution correspondant à un quaternion entier proprement dit donné $\Lambda$, sous forme de fractions dont le dénominateur commun est $\mathfrak{N}(\Lambda)$. Nous pouvons nous demander si le dénominateur et tous les numérateurs de ces fractions ont des diviseurs communs. Le plus grand commun diviseur T des quatre nombres entiers

$$(3)\qquad \begin{cases} \lambda_0^2-\lambda_{12}^2-\lambda_{13}^2+\lambda_{23}^2, & \lambda_0^2-\lambda_{12}^2+\lambda_{13}^2-\lambda_{23}^2; \\ \lambda_0^2+\lambda_{12}^2-\lambda_{13}^2-\lambda_{23}^2, & \lambda_0^2+\lambda_{12}^2+\lambda_{13}^2+\lambda_{23}^2, \end{cases}$$

divise nécessairement les quatre nombres entiers

$$4\lambda_0^2,\quad 4\lambda_{12}^2,\quad 4\lambda_{13}^2,\quad 4\lambda_{23}^2;$$

donc, comme $\Lambda$ est un quaternion proprement dit, T ne peut être qu'un diviseur de 4, c'est-à-dire l'un des nombres 1, 2, 4. Si le nombre entier $\mathfrak{N}(\Lambda)$ est impair, il vient $T=1$ et l'on ne peut amener les expressions précédentes des coefficients $\alpha_{11}$, $\alpha_{12}$, ..., $\alpha_{33}$ à avoir un dénominateur commun plus petit que $\mathfrak{N}(\Lambda)$. Si $\mathfrak{N}(\Lambda)$ est le double d'un nombre impair, deux des quatre nombres $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ sont pairs et deux sont impairs; les numérateurs des expressions trouvées pour $\alpha_{11}$, ..., $\alpha_{33}$ sont donc tous pairs; il vient $T=2$ et l'on peut simplifier chacune des fractions par 2. Si $\mathfrak{N}(\Lambda)$ est le quadruple d'un nombre impair, les quatre nombres $\lambda_0$, $\lambda_{12}$, $\lambda_{13}$, $\lambda_{23}$ sont impairs; leurs carrés sont, par suite, congrus à 1 suivant le module 8; les numérateurs des expressions trouvées pour $\alpha_{11}$, ..., $\alpha_{33}$ sont donc tous divisibles par 4; il vient $T=4$ et l'on peut simplifier chacune des fractions par 4. On voit donc que, si l'on ramène au plus petit dénominateur commun possible les coefficients des substitutions rationnelles qui transforment une somme de trois carrés en elle-même, ce dénominateur est nécessairement un nombre impair.

Il en est de même, comme nous l'avons vu, pour les substitutions

rationnelles qui transforment une somme de deux carrés en elle-même. Mais dans ces dernières le dénominateur réduit ne peut contenir en facteur que des nombres premiers de la forme $4r+1$, tandis que dans les substitutions rationnelles qui transforment une somme de trois carrés en elle-même, le dénominateur réduit peut être un nombre impair quelconque.

A la multiplication des quaternions correspond la composition des substitutions. Comme tout quaternion entier proprement dit peut, par le procédé indiqué, être obtenu en multipliant dans un ordre fixé arbitrairement des quaternions premiers entièrement déterminés par cet ordre, la substitution rationnelle correspondant à un quaternion entier proprement dit pourra être obtenue en composant dans le même ordre les substitutions rationnelles qui correspondent à ces quaternions premiers. Les trois quaternions premiers

$$(4) \qquad 1+i_{23}, \quad 1+i_{31}, \quad 1+i_{12},$$

dont la norme est égale à 2, appartiennent aux trois classes possibles de solutions de la congruence $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod 2$ [*comparez* (18), § VI]. Ces trois quaternions déterminent les trois substitutions

$$(5_a) \qquad x_1=y_1, \quad x_2=y_3, \quad x_3=-y_2;$$

$$(5_b) \qquad x_1=-y_3, \quad x_2=y_2, \quad x_3=y_1;$$

$$(5_c) \qquad x_1=y_2, \quad x_2=-y_1, \quad x_3=y_3.$$

Les coefficients de ces substitutions sont des nombres entiers, ce qui est d'accord avec ce que nous disions tout à l'heure du dénominateur commun réduit, des substitutions rationnelles qui transforment une somme de trois carrés en elle-même. Si, au contraire, la norme est un nombre premier impair $p$, chaque quaternion premier appartenant à l'une des $(p+1)$ classes possibles de solutions de la congruence $\xi_1^2+\xi_2^2+\xi_3^2\equiv 0 \pmod p$ détermine une substitution rationnelle dont le dénominateur commun réduit autant que possible est le nombre $p$ lui-même.

Nous avons déterminé, dans le § VI, le nombre des quaternions proprement dits dont la norme est un nombre entier donné, impair, ou

double, ou quadruple d'un nombre impair. Il est facile d'en déduire le nombre des substitutions rationnelles dont les coefficients ont pour dénominateur commun réduit autant que possible un nombre impair donné. Comme la norme de tout quaternion correspondant aux substitutions rationnelles dont on cherche le nombre est égale au nombre impair donné ou au double ou au quadruple de ce nombre impair, et comme deux quaternions $\Lambda$ et $-\Lambda$ déterminent la même substitution, le nombre cherché est égal à la moitié de la somme des nombres exprimant le nombre de quaternions entiers proprement dits dont la norme est l'entier impair donné, le nombre de quaternions entiers proprement dits dont la norme est le double de cet entier donné, et le nombre de quaternions entiers proprement dits dont la norme est le quadruple de cet entier donné.

Nous avons donné, dans le § VII, un procédé qui permet de représenter un quaternion entier proprement dit quelconque donné par un produit de quaternions premiers; nous avons vu que l'ordre de succession des normes de ces quaternions premiers étant une fois fixé, les quaternions premiers sont déterminés. On en déduit immédiatement le procédé qui permet de représenter une quelconque des substitutions rationnelles qui nous occupent, en composant des substitutions rationnelles dont les dénominateurs soient les facteurs premiers impairs contenus dans le dénominateur de la substitution rationnelle donnée que l'on cherche à représenter; l'ordre de succession de ces facteurs premiers impairs, auxquels il faut ajouter parfois une ou deux fois le facteur 2, étant une fois fixé, les substitutions composantes sont déterminées; celles qui correspondent au facteur 2 sont les substitutions entières $(5_a)$ ou $(5_b)$ ou $(5_c)$.

Les problèmes résolus pour les quaternions entiers trouvent donc une application immédiate et complète dans la théorie arithmétique des substitutions à coefficients rationnels qui transforment une somme de trois carrés en elle-même.