ANNALES SCIENTIFIQUES DE L'É.N.S.

GASTON BENNETON

Sur l'arithmétique des quaternions et des biquaternions

Annales scientifiques de l'É.N.S. 3^e série, tome 60 (1943), p. 173-214

<http://www.numdam.org/item?id=ASENS_1943_3_60__173_0>

SUR

L'ARITHMÉTIQUE DES QUATERNIONS

ET DES

BIQUATERNIONS

PAR M. GASTON BENNETON.

PRÉFACE.

Ce Mémoire comprend deux parties, dont on trouvera le résumé en plusieurs Notes dans les *Comptes rendus de l'Académie des Sciences* [17].

La première partie étudie les propriétés des quaternions entiers. On connaît les résultats essentiels obtenus dans ce domaine par Hurwitz [11] : son arithmétique des quaternions, dont l'ordonnance s'inspire de la théorie des corps de nombres algébriques, est basée sur l'existence d'un plus grand commun diviseur valable dans tous les cas; à cet effet sont considérés comme entiers non seulement les quaternions à composantes entières mais ceux dont les composantes sont des moitiés de nombres impairs. Nous suivons ici une méthode différente : nous définissons *a priori* les quaternions entiers comme ayant les composantes entières, puis nous construisons leur arithmétique en prenant pour base l'existence même des diviseurs premiers. L'étude des facteurs premiers y précède donc la théorie du plus grand commun diviseur.

Pour décomposer les quaternions en facteurs premiers, nous indiquons deux procédés de calcul effectif. Le premier, analogue au raisonnement de Lagrange [2] sur les sommes de quatre carrés, équivaut à la recherche, par divisions successives, des diviseurs communs à deux quaternions dont l'un est premier scalaire. Le second procédé, obtenu par itération, est d'ordre plus général et s'étend aisément au cas des facteurs non premiers.

Des résultats complémentaires seront publiés ultérieurement concernant la théorie des diviseurs et du plus grand commun diviseur, ainsi que l'application des quaternions à l'étude des matrices orthogonales d'ordre 4 à termes entiers.

La deuxième partie traite de l'arithmétique des biquaternions, nombres hypercomplexes d'ordre 8 comprenant les quaternions comme cas particulier. La multiplication n'y est pas associative et, dans la division par un nombre entier naturel, la notion de reste doit être sensiblement modifiée. La décomposition en facteurs premiers, généralement possible, s'obtient par un algorithme simple tout à fait semblable au second procédé des quaternions, qui ne suppose pas l'associativité du produit. Enfin le théorème de la décomposition des biquaternions permet de retrouver les énoncés de Jacobi sur la représentation des nombres entiers par une somme de huit carrés.

Je suis heureux de pouvoir exprimer ici mes sentiments de vive gratitude à mon maître M. Paul Montel et à M. A. Châtelet, dont les suggestions et les conseils m'ont été d'une aide précieuse.

NOTES BIBLIOGRAPHIQUES.

[1] L. Euler, *Œuvres*.

[2] J.-L. Lagrange, *Œuvres*, 3, Paris, 1869, p. 189.

[3] C. F. Gauss, *Disquisitiones arithmeticae*, Leipzig, 1801.

[4] A.-M. Legendre, *Théorie des Nombres*, 2, Paris, 1830, p. 144.

[5] C. G. Jacobi, *Fundamenta nova*, Königsberg, 1829, p. 106, 184; *Werke*, 1, Berlin, 1891, p. 239; *Werke*, 6, p. 245.

[6] A. Cayley, *Philos. Trans. London*, 148, 1858, p. 17; *Math. Papers*, 2, Cambridge, 1889, p. 475.

[7] A. Cayley, *London Edinb. Dublin philos. mag.*, 26, 1845, p. 210; *Math. Papers*, 1, Cambridge, 1889, p. 127, 301.

[8] F. Brioschi, *J. reine angew. Math.*, 52, 1856, p. 133.

[9] C. Jordan, *Traité des substitutions*, Paris, 1870, p. 156.

[10] R. Lipschitz, *Untersuchungen über die Summen von Quadraten*, Bonn, 1886; *J. Math. pures et appl.*, (4), 2, 1886, p. 373.

[11] A. Hurwitz. *Nachr. Ges. Göttingen*, 1896, p. 313, 336; *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, 1919.

[12] A. Hurwitz, *Nachr. Ges. Göttingen*, 1898, p. 309.

[13] G. Fontené, *Bull. Soc. math. France*, 27, 1899, p. 171.

[14] E. Dubois, *Intermédiaire des mathématiciens*, 18, 1911, p. 55.

[15] L. E. Dickson, *Proc. of the London math. Soc.*, 1921, p. 225.

[16] *C. R. Acad Sc.*, Paris, 212, 1941, p. 591, 637.

[17] *C. R. Acad. Sc.*, Paris, 207, 1938, p. 108; 214, 1942, p. 406, 459; 216, 1943, p. 262.

PREMIÈRE PARTIE.

LES QUATERNIONS ENTIERS.

CHAPITRE I.

GÉNÉRALITÉS.

1. *Définitions et formules.* — Les quaternions sont des nombres complexes d'ordre 4, c'est-à-dire des expressions linéaires de trois symboles i, j, k

$$A = x_0 + x_1 i + x_2 j + x_3 k,$$

dont les composantes x_α, ou coordonnées, seront dans cette étude des nombres entiers (éventuellement des fractions de dénominateur 2). L'addition et la multiplication se font comme celles de polynomes en i, j, k, compte tenu de la table de multiplication suivante

$$i^2 = j^2 = k^2 = -1, \qquad \begin{aligned} jk &= -kj = i, \\ ki &= -ik = j, \\ ij &= -ji = k. \end{aligned}$$

Rappelons quelques définitions et propriétés usuelles de l'algèbre de ces nombres.

La multiplication des quaternions est associative, distributive par rapport à l'addition, mais non commutative. Toutefois un nombre naturel x_0 peut être considéré comme un quaternion, dit *scalaire*, dont le produit avec tout autre quaternion est commutatif.

Deux quaternions ayant même première composante (partie scalaire) et dont les autres composantes sont opposées deux à deux sont dits *conjugués* :

$$A = x_0 + x_1 i + x_2 j + x_3 k, \qquad \overline{A} = x_0 - x_1 i - x_2 j - x_3 k;$$

leur produit est un nombre scalaire positif, qui est leur *norme* commune

$$N(A) = N(\overline{A}) = A\overline{A} = \overline{A}A = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Le conjugué d'un produit est le produit des conjugués changés d'ordre

$$\overline{AB} = \overline{B}\,\overline{A}.$$

La norme d'un produit se calcule immédiatement : elle vaut le produit des normes, comme il résulte aussi de l'identité de Lagrange

$$N(AB) = N(BA) = N(A)\,N(B).$$

Ceci montre qu'un produit est nul seulement si l'un des facteurs est nul, de sorte que, par exemple,

$$AB = AB' \quad (A \neq 0) \qquad \text{entraîne} \quad B = B'.$$

Notons que la division à droite ou à gauche est possible, sauf par zéro; elle donne en général des quaternions à composantes fractionnaires.

Il y a huit quaternions J entiers de norme 1

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k,$$

dont les inverses sont aussi des quaternions entiers (égaux ou opposés); ils constituent le groupe des *unités*. Multiplier par une unité ne change pas la norme.

Signalons enfin qu'on ne change pas la partie scalaire d'un produit en faisant une permutation circulaire des facteurs.

C'est essentiellement la propriété multiplicative de la norme qui justifie l'introduction des quaternions en arithmétique : *décomposer un nombre entier a en une somme de quatre carrés équivaut à trouver deux quaternions conjugués dont ce nombre est le produit*

$$a = A\bar{A} = N(A);$$

pour décomposer un produit ab en une somme de quatre carrés, on peut décomposer chaque facteur et composer les résultats obtenus soit par l'identité de Lagrange, soit par le produit des quaternions

$$ab = N(A)\,N(B).$$

Notations. — En principe nous désignons des quaternions de même norme par une même majuscule diversement accentuée, et la norme commune par la minuscule correspondante

$$a = N(A) = N(A') = N(A'') \ldots .$$

2. *Points de vue.* — Comme nous venons de le dire, l'arithmétique des quaternions est étroitement liée à la représentation des nombres par une somme de quatre carrés, et on peut étudier l'une afin de compléter l'autre.

En ce qui concerne l'étude des quaternions entiers; il existe plusieurs points de vue, d'ailleurs peu différents les uns des autres :

a. Définition *a priori* du *quaternion entier en tant que quaternion à composantes entières*. Pour de tels quaternions la théorie des diviseurs et du p. g. c. d. n'est pas valable dans tous les cas, et il faut étudier spécialement certaine classe où le facteur 2 joue un rôle particulier.

Cette définition, la première en date est celle de Lipschitz [10]. Elle a été reprise par L. E. Dickson [15].

b. Construction d'une arithmétique des quaternions basée, comme l'arithmétique élémentaire, sur l'existence d'un p. g. c. d. toujours valable. Ainsi

procède Hurwitz [11]; à cet effet il nomme *quaternions entiers* non seulement les quaternions à composantes entières mais encore ceux dont les composantes sont des moitiés de nombres impairs.

c. Étude d'un système de pseudo-quaternions, où la définition de base des produits unitaires est par exemple

$$1i = -i1 = i, \qquad i^2 = 1, \qquad jk = -kj = i,$$

où i, j, k désignent trois unités permutables circulairement. Une telle définition donne à la multiplication la presque-commutativité que ne possèdent pas les quaternions, $BA = AB1$. L'associativité par contre n'existe plus. L'arithmétique obtenue est presque identique à celle des quaternions; l'étude des produits de deux facteurs y est un peu plus simple [16].

d. Étude des quaternions d'après les vues de Cayley sur la théorie des matrices [6]. Les quaternions entiers sont représentés par des matrices carrées d'ordre 4 et correspondent à des substitutions linéaires orthogonales de quatre variables à coefficients entiers.

Nous choisissons le premier point de vue. D'ailleurs nous aurons recours aux considérations *b* et *d* pour étendre ou préciser certains résultats.

3. *Divisibilité des quaternions*. — La notion de divisibilité de l'arithmétique s'étend évidemment aux quaternions entiers à condition de distinguer les diviseurs à droite ou à gauche. On obtient ainsi les définitions et propriétés suivantes :

Un quaternion A est *divisible par un scalaire* entier m, à la fois à droite et à gauche, s'il existe un quaternion X tel que

$$A = mX = Xm.$$

Pour cela il faut et il suffit que les quatre composantes de A soient divisibles par m.

Un quaternion A est *divisible à gauche par un quaternion* B (ou à droite par un quaternion C) s'il existe un quaternion X (ou Y), qui est alors déterminé, tel que

$$A = BX \qquad \text{ou} \qquad A = YC.$$

Pour cela il faut et il suffit que

$$\bar{B}A = N(B)X \qquad \text{ou} \qquad \bar{B}A \textit{ divisible par } b,$$
$$A\bar{C} = YN(C) \qquad \text{ou} \qquad A\bar{C} \textit{ divisible par } c.$$

En particulier, comme il a été dit, tout quaternion divise sa norme, et divise un multiple quelconque de sa norme. *Pour qu'un scalaire m soit divisible par un quaternion* A, *à droite ou à gauche, il faut et il suffit que m soit divisible par la norme de* A :

$$m = aq \qquad \text{équivaut à} \quad m = A(q\bar{A}) = (q\bar{A})A.$$

Tout diviseur à droite d'un diviseur à droite est un diviseur à droite. De même à gauche. La divisibilité est unilatéralement *transitive*.

Les diviseurs scalaires jouant un rôle particulier, nous allons en indiquer quelques propriétés. Mais d'abord introduisons deux locutions (analogues à celles de l'arithmétique des polynomes) :

un quaternion est *primitif* si ses composantes sont premières entre elles dans leur ensemble;

tout quaternion est le produit d'un quaternion primitif par un entier positif qui est son *plus grand diviseur* (p. g. d.) *scalaire*.

Ceci posé :

les diviseurs scalaires d'un quaternion sont les diviseurs de son p. g. d. scalaire.

Si un nombre m divise le produit de deux quaternions AB *et s'il est premier avec la norme de l'un, il divise l'autre.* En effet m doit diviser

$$\overline{A}AB = N(A)\,(\text{p. g. d. scalaire B})\,B_1,$$

B_1 étant un quaternion primitif; donc m divise le p. g. d. scalaire de B.

De cet énoncé résulte que :

si deux quaternions ont des normes premières entre elles, le p. g. d. scalaire de leur produit est le produit des p. g. d. scalaires des facteurs.

En particulier, le produit de deux quaternions primitifs dont les normes sont premières entre elles est primitif. Il est aisé de voir sur des exemples que la propriété n'est plus vraie si les normes ne sont pas premières entre elles.

4. *Quaternions associés. Facteurs.* — 1° Un diviseur scalaire d'un quaternion est défini au produit près par ± 1. Un diviseur à gauche B (ou à droite C) est défini au produit près à droite (ou à gauche) par les huit unités J :

$$BJ \quad (\text{ou } JC).$$

Suivant une locution usuelle d'arithmétique générale, ces huit quaternions seront dits *associés à gauche* (ou à droite).

En particulier tout diviseur A admet comme diviseurs impropres (ou triviaux) :

des deux côtés, les huit unités J;
à gauche, les huit associés à gauche AJ;
à droite, les huit associés à droite JA.

Tout autre diviseur dont la norme est comprise entre 1 et N(A), est *diviseur propre*.

2° Plus généralement appelons quaternions *associés* à A tous les produits de la forme JAJ', les unités pouvant être multipliées à droite et à gauche.

Si B est diviseur de A (à droite ou à gauche), tous les quaternions associés à B sont diviseurs d'un quaternion associé à A. En effet

$$A = BC \qquad \text{équivaut à} \quad JAJ' = JBJ''(J''CJ').$$

On peut donc se borner à étudier la divisibilité d'un quaternion défini à la multiplication près par une unité à droite ou à gauche. Un tel quaternion joint à tous ses associés sera appelé un *facteur*. Ainsi les quaternions JAJ', qui sont au nombre de 32 distincts ou non (*cf.* n° 18), constituent le facteur $\mathfrak{A}$ associé à A. L'égalité ci-dessus devient

$$\mathfrak{A} = \mathfrak{B}\mathfrak{C},$$

où les facteurs $\mathfrak{B}$ et $\mathfrak{C}$ ne sont d'ailleurs pas complètement indépendants.

Les huit unités forment le facteur unité $\mathfrak{I}$. Tout autre facteur a pour diviseurs impropres lui-même et le facteur unité. Tout facteur dont la norme est un nombre premier ne possède aucun diviseur propre.

Si deux quaternions A et $\overline{A}$ sont conjugués, tous leurs associés sont conjugués deux à deux; ils définissent deux facteurs $\mathfrak{A}$ et $\overline{\mathfrak{A}}$, encore appelés *conjugués* et tels que

$$\mathfrak{A}\overline{\mathfrak{A}} = a\mathfrak{I}.$$

5. *Restes des quaternions* (mod m). — Selon une locution usuelle, deux quaternions A et B sont *congrus* ou appartiennent à une *même classe* suivant le *module scalaire* m (entier positif), si leur différence est divisible par m :

$$A \equiv B \pmod{m} \qquad \text{équivaut à} \quad A - B = mU.$$

Les classes ainsi définies s'ajoutent, se retranchent et se multiplient (produit non-commutatif). La propriété dont nous ferons surtout usage est :

Tous les quaternions d'une même classe (mod m) *ont les mêmes diviseurs de norme m, à droite ou à gauche, si toutefois il en existe.*

En effet, avec les précédentes notations

$$A = MX \qquad \text{entraîne} \quad B = M(X - \overline{M}U),$$
$$A = X'M' \qquad \text{entraîne} \quad B = (X' - U\overline{M}')M'.$$

La classe nulle, contenant zéro, est l'ensemble des quaternions multiples de m.

D'importantes démonstrations de l'arithmétique élémentaire sont basées sur le fait que, dans toute classe d'entiers (mod m), il existe un entier (reste) compris entre zéro et m, ou encore compris entre $\frac{-m}{2}$ et $\frac{m}{2}$ (reste absolu minimum). Pour les quaternions la propriété analogue est celle-ci :

Dans une classe de quaternions (mod m), *il existe au moins un quaternion* R, que nous appelons *reste, dont la norme est au plus égale à* m^2, l'égalité n'ayant lieu que si m est pair.

En effet, parmi tous les quaternions congrus à A (mod$m$), considérons le quaternion R dont les composantes sont les restes minima absolus de celles de A : *chaque composante de* R *a une valeur absolue au plus égale à* $\frac{m}{2}$. La norme de R est au plus égale à m^2 ; elle n'égale m^2 que si A est de la forme

$$A = \frac{m}{2} C \qquad (m \text{ pair}),$$

les composantes de C étant toutes impaires.

CHAPITRE II.

DÉCOMPOSITION EN FACTEURS PREMIERS.

6. *Méthode de décomposition en facteurs premiers.* — Nous disons qu'un quaternion est *premier si sa norme est un nombre premier.* Il est nécessairement primitif et n'a pas de diviseur propre.

Dans ce Chapitre nous étudions d'abord la décomposition des quaternions primitifs. Nous montrons que tout quaternion primitif A est un produit de quaternions premiers P dont les normes sont les facteurs premiers de la norme de A, et nous indiquons le moyen de calculer les diviseurs P à partir de A. Puis nous étudions les quaternions scalaires et nous montrons qu'ils sont toujours décomposables en produit de quaternions premiers. De là nous passons aux quaternions quelconques, eux aussi décomposables.

Il en résulte alors que les quaternions premiers sont les seuls à n'avoir pas de diviseur propre, ce qui justifie leur nom. Quant à la propriété d'arithmétique élémentaire, à savoir qu'un nombre premier ne peut diviser un produit de deux entiers sans diviser l'un d'eux, elle n'a pas d'équivalent pour les quaternions en raison de la non-commutativité de la multiplication.

En fin de Chapitre nous recherchons les quaternions primitifs de norme donnée, et nous donnons une démonstration du théorème de Jacobi sur les sommes de quatre carrés.

Bien entendu la notion de facteur (ensemble de quaternions associés) permet de simplifier la plupart des énoncés.

Pour étudier la décomposition d'un quaternion primitif A, nous en calculerons d'abord un diviseur premier à gauche P dont la norme divise celle de A, c'est-à-dire que nous résoudrons l'égalité

$$A = PQ; \qquad N(A) = pq, \qquad N(P) = p.$$

Examinons en premier lieu le cas de $p = 2$ qui présente des anomalies.

7. *Existence d'un diviseur de norme* 2. — *Si* N(A) *est double de nombre impair,* A *est divisible à gauche* (*ou à droite*) *par un seul des trois quaternions*

de norme 2

$$1+i, \quad 1+j, \quad 1+k,$$

et par ses associés.

Si N(A) *est multiple de* 4, A *est divisible à droite et à gauche par tous les quaternions de norme* 2.

Remarquons d'abord qu'*il n'y a pas de quaternion primitif de norme divisible par* 8.

Le quaternion primitif A et son reste $A_0 \pmod 2$ ont les mêmes diviseurs à gauche de norme 2. Mais leurs normes sont congrues entre elles (mod 4) de sorte que, suivant le cas, la norme de A_0, au plus égale à 4 et non nulle, est 2 ou 4.

Dans le premier cas A_0 est la somme de deux unités, c'est donc l'associé d'un seul des trois quaternions $1+i$, $1+j$, $1+k$.

Dans le second cas les composantes de A_0 sont ± 1, et suivant le module 2, on peut les prendre positives. A_0 s'écrit alors

$$1+i+j+k=(1+i)(1+j)=(1+j)(1+k)=(1+k)(1+i).$$

En résumé, si la norme de A est paire :

$$N(A)\not\equiv 0 \pmod 4, \qquad A=(1+i)Q \text{ ou } (1+j)Q' \text{ ou } (1+k)Q'',$$
$$N(A)\equiv 0 \pmod 4, \qquad A=(1+i)Q=(1+j)Q'=(1+k)Q''.$$

Notons que si un quaternion a pour norme 2, chacun de ses associés est simultanément associé à droite et à gauche. Tout diviseur à gauche de norme 2 est aussi diviseur à droite, et inversement.

8. *Existence d'un diviseur premier de norme impaire. — Un quaternion primitif* A *dont la norme est multiple d'un nombre premier impair p a un diviseur à gauche (ou à droite)* P *de norme p et un seul, défini au produit près à droite (ou à gauche) par une unité.*

Remplaçons A par son reste A_0 suivant le module p. La norme de A_0, qui est encore multiple de p, est inférieure à p^2 et non nulle puisque A est primitif

$$A=pQ_0+A_0, \qquad N(A_0)=pq_1, \qquad 0<q_1<p.$$

Formons le reste R_1 de A_0 suivant le module q_1 ; sa norme est un multiple q_1q_2 au plus égal à q_1^2. Mais le quaternion q_2A_0 est divisible à droite par R_1 puisque (n° 3)

$$q_2A_0\overline{R}_1\equiv q_2A_0\overline{A}_0=q_2q_1p\equiv 0 \pmod{q_1q_2}.$$

D'où, en rassemblant les résultats

$$R_1\equiv A_0 \pmod{q_1}, \qquad \begin{matrix} N(A_0)=pq_1, \\ q_2A_0=A_1R_1, \\ N(R_1)=q_1q_2. \end{matrix} \qquad \begin{cases} N(A_1)=pq_2, \\ 0\leqq q_2\leqq q_1. \end{cases}$$

Faisons la même opération sur A_1. Nous en déduisons des quaternions R_2, A_2, et un nombre q_3 au plus égal à q_2. Ainsi de suite. Après h opérations nous obtenons

$$R_h \equiv A_{h-1} \pmod{q_h}, \qquad \begin{matrix} N(A_{h-1}) = pq_h, \\ q_{h+1} A_{h-1} = A_h R_h, \\ N(R_h) = q_h q_{h+1}. \end{matrix} \qquad \begin{cases} N(A_h) = pq_{h+1} \\ 0 \leqq q_{h+1} \leqq q_h. \end{cases}$$

Arrêtons le calcul lorsque pour la première fois q_{h+1} est égal à l'une de ses limites, ce qui a lieu notamment si $q_h = 1$, car le reste de A_{h-1} suivant le module 1 est nul.

1° Si q_{h+1} est nul, R_h est nul. A_{h-1} est divisible par q_h et sa norme pq_h est divisible par q_h^2. Le nombre p étant premier, il s'ensuit

$$q_h = 1, \qquad A_{h-1} = P, \qquad N(P) = p.$$

Éliminons les A_i entre les $h - 1$ premières égalités

$$q_2 q_3 \ldots q_{h-1} A_0 = P R_{h-1} \ldots R_2 R_1.$$

Le scalaire $q_2 q_3 \ldots q_{h-1}$, produit de nombres inférieurs à p, est premier avec la norme de P; il divise donc le produit des R_i de sorte que

$$A_0 = PR', \qquad A = P(R' + \overline{P} Q_0).$$

Nous avons construit un diviseur de A, à gauche, P de norme p.

Ce diviseur P est unique, au produit près par une unité à droite. En effet A et A_0 ont les mêmes diviseurs à gauche de norme p, et il en est ainsi pour deux quaternions successifs quelconques A_{i-1} et A_i, à partir de A_0. Pour cela comparons les divisibilités par p des produits $\overline{X} A_{i-1}$ et $\overline{X} A_i$:

$$q_{i+1}(\overline{X} A_{i-1}) = (\overline{X} A_i) R_i, \qquad N(R_i) = q_i q_{i+1}.$$

q_{i+1} et la norme de R_i sont des nombres premiers avec p : la divisibilité par p est bien identique pour les deux produits.

2° Si q_{h+1} était égal à q_h, ces nombres seraient pairs et R_h serait le produit de leur moitié par un quaternion C de norme 4; de sorte que A_{h-1} serait divisible par $\frac{q_h}{2}$ et sa norme pq_h le serait par $\frac{q_h^2}{4}$. Ceci entraînerait, p étant premier,

$$q_h = 4, \qquad A_{h-1} = 2P, \qquad P \equiv C \pmod 2, \qquad N(P) = p.$$

Mais P admettrait, comme C, un diviseur de norme 2 et la norme p serait paire. L'hypothèse envisagée est impossible.

Note. — La démonstration, basée sur la construction de nombres entiers décroissants q_i, est inspirée du raisonnement fait par Lagrange [2], par une méthode de descente, pour démontrer le théorème de Bachet. Nous établissons plus loin ce théorème, en prouvant que tout scalaire est la norme d'un quaternion entier.

9. *Deuxième procédé.* — Supposons la norme de A égale à pq_1 et formons le reste R_1 de $\overline{A}$ suivant le module q_1; la norme de R_1 est un multiple de q_1 au plus égal à q_1^2

$$R_1 \equiv \overline{A} \pmod{q_1}, \qquad N(R_1) = q_1 q_2, \qquad 0 \leqq q_2 \leqq q_1.$$

La recherche des diviseurs de A à gauche de norme p *équivaut* à la recherche des diviseurs (complémentaires) de A à droite de norme q_1, qui sont eux-mêmes les conjugués de diviseurs à gauche de R_1. Renouvelons l'opération en considérant

$$R_2 \equiv \overline{R}_1 \pmod{q_2}, \qquad N(R_2) = q_2 q_3, \qquad 0 \leqq q_3 \leqq q_2,$$

et ainsi de suite. Après h opérations nous obtenons

$$R_h \equiv \overline{R}_{h-1} \pmod{q_h}, \qquad N(R_h) = q_h q_{h+1}, \qquad 0 \leqq q_{h+1} \leqq q_h,$$

où il suffit d'étudier les diviseurs de R_h à gauche de norme q_h pour montrer l'existence des diviseurs de A de norme p.

Cessons le calcul lorsque pour la première fois q_{h+1} est égal à l'une de ses limites. Ceci correspond à (n° 5)

$$R_h = \varrho \quad \text{ou} \quad \frac{q_h}{2} C, \qquad\qquad q_{h+1} = 0 \quad \text{ou} \quad q_h,$$

la norme de C étant égale à 4.

D'une manière générale supposons

$$R_i = \frac{m}{2} C_i, \qquad q_{i+1} \equiv q_i \equiv 0 \pmod{m}$$

et montrons que ces conditions s'étendent à l'indice $i-1$:

$$R_{i-1} = \frac{m}{2} \overline{C}_i + q_i X, \qquad N(R_{i-1}) = N(R_i) + q_i \frac{m}{2} (X C_i + \overline{C}_i \overline{X}) + q_i^2 N(X),$$

X étant entier; ce qui entraîne bien

$$R_{i-1} = \frac{m}{2} C_{i-1}, \qquad q_{i-1} = q_{i+1} + \text{partie scalaire}\,(m X C_i) + q_i N(X) \equiv 0 \pmod{m},$$

les normes de C_i et de C_{i-1} étant multiples de 4.

Or R_h est de la forme $\frac{m}{2} C$, et q_{h+1}, q_h sont divisibles par $m = q_h$. En raisonnant de proche en proche sur R_{h-1}, ..., R_2, R_1, A, nous voyons que q_h doit diviser en même temps $2A$, p et q_1; il vaut nécessairement 1 si l'on suppose A primitif et p premier impair. Donc

$$q_h = 1, \qquad q_{h+1} = 0.$$

Les diviseurs de R_{h-1} à gauche de norme q_{h-1} existent : ce sont les associés à gauche. Par conséquent A possède des diviseurs à gauche de norme p. Il en résulte des égalités de la forme

$$A = PQ_1, \qquad R_1 = \overline{Q}_1 Q_2, \qquad \ldots, \qquad R_{h-1} = \overline{Q}_{h-1} J,$$

où J est une unité. L'élimination des Q_i donne l'expression du diviseur P

$$q_1 q_2 \dots q_{h-1} P = A R_1 R_2 \dots R_{h-1} J,$$

diviseur unique, au produit près à droite par une unité J.

Remarques. — 1° Ce procédé de décomposition est plus général que celui du n° 8, car il ne suppose pas essentiellement p premier. Il suffit en effet que p, q_1 et le p. g. d. scalaire de 2A soient premiers entre eux dans leur ensemble. Nous reviendrons sur ce point.

2° Changeons l'ordre ou le signe des composantes de A. Les restes successifs R_i subissent la même permutation ou le même changement de signe de leurs composantes. Leurs normes sont les mêmes, leur nombre h ne varie pas.

En particulier aux divers quaternions associés à A correspond un même nombre de restes, h.

10. *Décomposition d'un quaternion primitif.* — Considérons un quaternion primitif A ayant pour norme un produit de facteurs premiers rangés dans un ordre choisi d'avance $p_1 p_2 p_3 \dots$. Nous savons calculer un diviseur à gauche P_1 de norme p_1, diviseur unique au produit près par une unité (sauf cas particulier relatif au facteur 2), de sorte que

$$A = P_1 Q_1, \qquad N(Q_1) = p_2 p_3 \dots.$$

A son tour le quaternion Q_1, nécessairement primitif, possède un diviseur à gauche P_2 de norme p_2

$$Q_1 = P_2 Q_2, \qquad A = P_1 P_2 Q_2, \qquad N(Q_2) = p_3 \dots.$$

Et ainsi de suite jusqu'à épuisement de tous les facteurs p_i; le dernier quotient Q_{h-1} sera nécessairement un diviseur premier P_h de norme p_h. Nous aboutissons au résultat suivant.

Théorème. — *La norme d'un quaternion primitif* A *étant décomposée en facteurs premiers non nécessairement distincts rangés dans un certain ordre*

$$N(A) = p_1 p_2 p_3 \dots$$

le quaternion peut être décomposé en un produit de quaternions premiers

$$A = P_1 P_2 P_3 \dots$$

dont les normes sont respectivement les nombres $p_1, p_2, p_3, \dots$. *La décomposition est unique*, au produit près de chaque quaternion par une unité. Toutefois s'il y a deux normes p_α et $p_{\alpha'}$ égales à 2, pour la première d'entre elles le quaternion correspondant peut être remplacé indifféremment par un quaternion quelconque de norme 2 (ce qui modifie alors tous les facteurs P_i situés entre P_α et $P_{\alpha'}$, à moins que ces deux derniers quaternions ne soient consécutifs).

L'utilisation des facteurs au lieu des quaternions donne à l'énoncé une forme plus concise :

A tout arrangement des facteurs premiers de la norme d'un *facteur primitif* $\mathfrak{A}$ correspond une seule décomposition de $\mathfrak{A}$ en facteurs premiers de normes rangées dans le même ordre

$$\mathrm{N}(\mathfrak{A}) = p_1 p_2 p_3 \ldots, \qquad \mathfrak{A} = \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3 \ldots, \qquad \mathrm{N}(\mathfrak{P}_i) = p_i.$$

Toutefois s'il y a deux facteurs $\mathfrak{P}$ de norme 2, le premier d'entre eux peut être remplacé par un facteur quelconque de norme 2; il y a alors trois décompositions distinctes.

Réciproque. — *Un produit de facteurs premiers*

$$\mathfrak{P}_1 \mathfrak{P}'_1 \mathfrak{P}''_1 \ldots \mathfrak{P}_2 \mathfrak{P}'_2 \ldots \mathfrak{P}_3 \mathfrak{P}'_3 \ldots, \qquad \mathrm{N}(\mathfrak{P}_i) = \mathrm{N}(\mathfrak{P}'_i) \ldots = p_i$$

dont les normes respectives aux indices sont les nombres premiers impairs distincts $p_1, p_2, p_3, \ldots$, *est un facteur primitif s'il n'y a pas de facteurs conjugués consécutifs.*

Raisonnons par l'absurde sur le produit $\mathfrak{Q}\mathfrak{P}\mathfrak{P}'\mathfrak{R}$, en supposant $\mathfrak{Q}\mathfrak{P}$ primitif et $\mathfrak{Q}\mathfrak{P}\mathfrak{P}'$ non primitif. $\mathfrak{P}'$ est le facteur situé le plus à gauche qui rende le produit non primitif. $\mathfrak{Q}\mathfrak{P}\mathfrak{P}'$ est alors divisible par la norme commune de $\mathfrak{P}$ et $\mathfrak{P}'$. Le facteur $\mathfrak{Q}\mathfrak{P}$ est divisible à droite par $\overline{\mathfrak{P}}'$; étant primitif il n'a qu'un seul diviseur à droite de norme p, à savoir

$$\mathfrak{P} = \overline{\mathfrak{P}}'.$$

Note. — Hurwitz [11], après Lipschitz [10], a énoncé le théorème de la décomposition d'un quaternion primitif; il l'a montré en établissant d'abord la théorie du p. g. c. d. Dans le présent travail, ce théorème résulte de la décomposition effective en facteurs premiers.

11. *Décomposition d'un nombre premier scalaire.*

Théorème. — *Tout nombre premier scalaire p est le produit de deux quaternions conjugués de* $8(p+1)$ *manières différentes.*

Corollaire. — *Tout scalaire entier est la norme d'un quaternion entier.* Ce qui équivaut au *théorème de Bachet* : tout nombre entier est une somme de quatre carrés.

Le théorème est évident pour $p = 2$

$$2 = (1+i)\mathrm{J}.\bar{\mathrm{J}}(1-i) = (1+j)\mathrm{J}.\bar{\mathrm{J}}(1-j) = (1+k)\mathrm{J}.\mathrm{J}(1-k),$$

où J est une des huit unités.

Pour un nombre premier impair p nous montrons d'abord l'existence d'un quaternion primitif de norme divisible par p, donc divisible à gauche par un quaternion premier P de norme p. Nous considérons ensuite l'ensemble des multiples du même quaternion premier

$$PX \qquad (X \text{ quaternion entier quelconque})$$

que nous appelons *idéal à droite* de norme p. Nous caractérisons cet ensemble en y distinguant un quaternion de forme simple, quaternion *réduit*. La détermination de tous les quaternions réduits correspondant au nombre premier p permet de trouver tous les idéaux à droite de norme p, et par suite toutes les décompositions de p.

12. *Ensemble des multiples d'un quaternion premier.* — 1° On sait depuis Euler que, pour tout nombre premier p, la congruence

$$1 + x^2 + y^2 \equiv 0 \pmod{p}$$

a au moins une solution x_0, y_0. (Nous reviendrons plus loin sur l'existence et la recherche de ces solutions.) Le quaternion primitif correspondant

$$A = 1 + x_0 j + y_0 k$$

a sa norme divisible par p, de sorte qu'il existe au moins un quaternion P de norme p.

2° Considérons l'ensemble des multiples

$$PX \qquad (X \text{ quaternion entier quelconque}).$$

L'ensemble contient la somme ou la différence de deux quelconques de ses termes et le produit de l'un quelconque par tout quaternion entier. C'est un *idéal à droite* au sens général de ce mot. Cet idéal est *principal* : il est engendré par l'un quelconque des huit associés PJ et ne renferme aucun autre quaternion de norme p. Il contient par ailleurs tout quaternion congru à chacun de ses termes, il est formé de classes (mod p) :

$$PX + pX_1 = P(X + \bar{P}X_1).$$

Nous allons montrer que :

Parmi les multiples d'un quaternion premier P *se trouve un quaternion simple, ou réduit, dont la partie scalaire vaut* 1 *et dont l'une des trois autres composantes est nulle.* Si cette composante est la seule nulle, elle peut être choisie arbitrairement, par exemple la seconde.

Il équivaut de dire :

un quaternion premier P *est diviseur à gauche d'un quaternion de l'une des formes*

$$1 + ai, \qquad 1 + bj + ck.$$

Pour définir l'ensemble des multiples choisissons un associé PJ dont la première composante ne soit pas nulle,

$$\mathrm{PJ} = x_0 + x_1 i + x_2 j + x_3 k \qquad (x_0 \not\equiv 0) \qquad (\mathrm{mod}\, p).$$

Si l'un des nombres x_2, x_3 n'est pas nul, nous considérons le multiple

$$\mathrm{PJ}(x_0 - x_1 i) = y_0 + y_2 j + y_3 k \qquad (y_0 = x_0^2 + x_1^2),$$

y_0, inférieur à p, n'est pas divisible par p et l'inégalité

$$\mathrm{N(P)}.(x_0^2 + x_1^2) > y_0^2$$

montre que y_2 ou y_3 n'est pas nul. Nous avons ainsi un quaternion de l'ensemble de la forme

$$x_0 + x_1 i \quad \text{ou} \quad y_0 + y_2 j + y_3 k \qquad (x_0 y_0 \not\equiv 0) \qquad (\mathrm{mod}\, p).$$

Il suffit de multiplier par l'inverse de la première composante x_0 ou y_0, suivant le module p, pour obtenir un quaternion congru à un quaternion de l'une des formes

$$1 + ai, \qquad 1 + bj + ck.$$

13. *Unicité des quaternions réduits.* — Vérifions maintenant que le quaternion réduit d'un même ensemble de multiples est unique (à un multiple près de p). De façon équivalente :

Pour que deux quaternions de l'une des formes

$$1 + ai, \qquad 1 + bj + ck$$

soient multiples (à droite) d'un même quaternion premier de norme p, il faut et il suffit qu'ils soient congrus $(\mathrm{mod}\, p)$.

La condition nécessaire et suffisante pour que

$$1 + bj + ck = \mathrm{PQ}, \qquad 1 + b'j + c'k = \mathrm{PQ_1}$$

est

$$(1 - bj - ck)(1 + b'j + c'k) = \overline{\mathrm{Q}}\,\overline{\mathrm{P}}\mathrm{PQ_1} \equiv 0 \qquad (\mathrm{mod}\, p),$$

ceci d'après la réciproque de la décomposition d'un quaternion primitif. Cette condition équivaut à

$$1 + bb' + cc' + (cb' - bc')i + (b' - b)j + (c' - c)k \equiv 0 \qquad (\mathrm{mod}\, p),$$
$$b \equiv b', \qquad c \equiv c' \qquad (\mathrm{mod}\, p),$$

en supposant bien entendu la norme de PQ divisible par p.

Comparons de même un quaternion de la première forme à un de la seconde. La condition

$$(1 - ai)(1 + bj + ck) \equiv 0 \qquad (\mathrm{mod}\, p)$$

est impossible, la partie scalaire du produit valant 1.

Enfin pour deux quaternions de la première forme la condition

$$(1 - ai)(1 + a'i) = 1 + aa' + (a' - a)i \equiv 0 \pmod{p}$$

équivaut à leur congruence suivant le module p.

Il y a donc une correspondance biunivoque entre les quaternions de norme p et les quaternions réduits de norme divisible par p.

Pour les quaternions de norme p, la construction des ensembles de multiples se ramène à la résolution de la congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{p};$$

à une solution (b, c) formée de deux entiers non nuls $(\mathrm{mod}\, p)$ correspond un ensemble défini par le quaternion réduit

$$1 + bj + ck = \mathrm{PQ};$$

à une solution comportant un entier nul $(0, a)$ correspondent trois ensembles définis par les quaternions réduits

$$1 + ai = \mathrm{P_1Q_1}, \qquad 1 + aj = \mathrm{P_2Q_2}, \qquad 1 + ak = \mathrm{P_3Q_3}.$$

On peut dire encore :

le nombre des quaternions de norme p vaut huit fois le nombre total des solutions des deux congruences (indépendantes)

$$x^2 + y^2 + 1 \equiv 0 \pmod{p},$$
$$x^2 + 1 \equiv 0 \pmod{p}.$$

14. *Formation des quaternions réduits.* — 1° Étudions d'abord la congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

Résoudre cette congruence c'est chercher les décompositions de -1 en nombres de Gauss [3] :

$$-1 \equiv (x + yi)(x - yi) \pmod{p}.$$

Premier cas. $p + 1$ est multiple de 4. L'entier p n'est pas décomposable, c'est un nombre de Gauss, premier. Il y a $p^2 - 1$ classes $(\mathrm{mod}\, p)$ premières avec p engendrées par les puissances de l'une d'elles (racine primitive)

$$\mathrm{G}^{\alpha} \qquad (\alpha \text{ défini, mod } p^2 - 1).$$

Le conjugué de G^{α} est la puissance $\mathrm{G}^{p\alpha}$. La décomposition de -1 est donnée par l'égalité

$$\mathrm{G}^{\alpha}\mathrm{G}^{p\alpha} \equiv \mathrm{G}^{\frac{p^2-1}{2}} \pmod{p}$$

ou

$$\alpha \equiv \frac{p-1}{2} \pmod{p-1}.$$

On obtient ainsi $p+1$ solutions

$$x+yi\equiv\left(G^{\frac{p-1}{2}}\right)^{2\lambda+1} \qquad (\mathrm{mod}\,p;\ \lambda=0,\ 1,\ \ldots,\ p),$$

qui sont les puissances impaires de l'une quelconques d'entre elles

$$x+yi\equiv(x_0+y_0i)^{2\lambda+1} \qquad (\mathrm{mod}\,p).$$

Il est à remarquer qu'aucun des nombres x, y n'est nul.

Deuxième cas. $p-1$ est multiple de 4. L'entier p est décomposable

$$p=(a+bi)(a-bi).$$

Les classes $(\mathrm{mod}\,p)$ premières avec p se déduisent des classes prises suivant les modules respectifs $a+bi$ et $a-bi$. Pour chacun de ces modules, il y a $p-1$ classes, engendrées par les puissances d'une racine primitive.

Appelons G une racine primitive suivant le module $a+bi$. Les classes $(\mathrm{mod}\,p)$ premières avec p sont

$$G^\alpha\overline{G}^\beta \qquad (\alpha,\ \beta\ \text{définis, mod}\ p-1);$$

et la décomposition de -1 est donnée par l'égalité

$$G^\alpha\overline{G}^\beta.\overline{G}^\alpha G^\beta\equiv-1\equiv(G\overline{G})^{\frac{p-1}{2}} \qquad (\mathrm{mod}\,p)$$

ou

$$\alpha+\beta\equiv\frac{p-1}{2} \qquad (\mathrm{mod}\,p-1).$$

Posons

$$\alpha\equiv\frac{p-1}{4}+\lambda \quad (\mathrm{mod}\,p-1), \qquad \overline{G}G'\equiv1\ (\mathrm{mod}\,p).$$

Nous obtenons les $p-1$ solutions

$$x+yi\equiv(G\overline{G})^{\frac{p-1}{4}}(GG')^\lambda \qquad (\mathrm{mod}\,p;\ \lambda=1,\ 2,\ \ldots,\ p-1).$$

En considérant les solutions particulières correspondant à $\lambda=1$,

$$x_0+y_0i\equiv-mGG', \qquad m^2+1\equiv0 \qquad (\mathrm{mod}\,p),$$

nous pouvons écrire pour la solution générale

$$x+yi\equiv-m^{\lambda+1}(x_0+y_0i)^\lambda \qquad (\mathrm{mod}\,p).$$

Nous y retrouvons notamment les puissances impaires de x_0+y_0i.

2° A chaque solution $x+yi$ de la congruence correspond le quaternion réduit

$$1+(x+yi)j=1+xj+yk.$$

Et les formules précédentes en λ permettent d'exprimer tous les quaternions réduits $(\mathrm{mod}\,p)$ à partir de l'un d'eux.

Si $p-1$ est multiple de 4, il y a en outre deux quaternions réduits supplémentaires qui sont

$$1 \pm mi, \qquad m^2+1 \equiv 0 \pmod{p}.$$

Le nombre des quaternions réduits est donc, dans tous les cas,

$$p+1=(p-1)+2.$$

Le nombre de décompositions annoncé du scalaire premier p vaut bien $8(p+1)$.

15. *Décomposition d'un quaternion quelconque.* — Considérons un quaternion quelconque A ayant pour norme un produit de facteurs premiers rangés dans un ordre choisi d'avance :

$$N(A)=p_1p_2p_3\ldots, \qquad A=\pi_1\pi_2\ldots B, \qquad (B \text{ primitif}),$$

où $\pi_1\pi_2\ldots$ est la décomposition en facteurs premiers du p. g. d. scalaire de A.

Si A est divisible par p_1, il admet comme diviseurs à gauche les $8(p_1+1)$ quaternions de norme p_1. Si p_1, supposé impair, ne divise pas A, il existe 8 quaternions associés P_1 de norme p_1 diviseurs à gauche de B et par suite de A. Enfin si p_1 égale 2 et que les composantes de A soient toutes impaires, celles de B le sont aussi et A est divisible à gauche par tous les quaternions de norme 2. Nous pouvons écrire dans tous les cas

$$A=P_1Q_1, \qquad N(Q_1)=p_2p_3\ldots.$$

A son tour Q_1 est divisible à gauche par certains quaternions de norme p_2. Et ainsi de suite jusqu'à l'épuisement de tous les facteurs p_1. Il en résulte que :

Tout quaternion est décomposable en produit de quaternions premiers dont les normes sont rangées dans un ordre choisi d'avance.

Le nombre des décompositions (définies au produit près des quaternions par une unité) est

$$h_1h_2h_3\ldots, \qquad h_i=1 \quad \text{ou} \quad (p_i+1).$$

On montre d'ailleurs que ce nombre ne dépend pas de l'ordre des facteurs p_i.

Supposons alors, dans la décomposition de la norme de A, que les facteurs premiers égaux soient consécutifs, et considérons les décompositions correspondantes du quaternion A. Chacune d'elles comprend nécessairement (réciproque du n° 10) deux facteurs conjugués consécutifs, de norme π_1 par exemple. Faisons abstraction de ces deux facteurs. Le produit restant est le quaternion non primitif $\pi_2\ldots B$ et renferme à son tour deux facteurs conjugués consécutifs de norme π_2 par exemple. Ainsi de suite jusqu'à l'épuisement des facteurs du p. g. d. scalaire; le dernier produit est une décomposition du quaternion primitif B.

Le nombre des décompositions vaut donc

$$(\pi_1+1)(\pi_2+1)\ldots,$$

nombre qui doit être triplé si la norme de B est multiple de 4.

Bien entendu le raisonnement s'applique à la décomposition des scalaires non premiers, pour lesquels B égale 1.

16. *Décomposition en produit de quaternions réduits.* — 1° Considérons un quaternion premier P. Il lui correspond un quaternion réduit U admettant P comme diviseur à gauche

$$PQ = U.$$

Retrouvons le diviseur P à partir de U en utilisant le procédé du n° 9. Nous obtenons

$$q_1 q_2 \ldots q_{h-1} P = U R_1 R_2 \ldots R_{h-1} J.$$

Or les restes successifs R_i sont des quaternions réduits de la même forme que U. L'unité J, si elle est différente de 1, a pour double un produit de quaternions réduits

$$2J = (1+J)^2.$$

Par conséquent le quaternion premier P est décomposable en un produit de quaternions réduits, à un coefficient scalaire l près :

$$lP = UU_1U_2\ldots.$$

2° Le résultat s'étend immédiatement à tout quaternion non premier A; il suffit de considérer A comme un produit de quaternions premiers, et ces derniers comme des produits de quaternions réduits :

Tout quaternion A *est décomposable en un produit de quaternions réduits, à un coefficient scalaire l près*

$$lA = UU_1U_2U_3\ldots.$$

17. *Nombre des quaternions de norme n.* — Si p est premier, le nombre des quaternions de norme p vaut

$$r(p) = 8(p+1).$$

Pour n quelconque, le théorème du n° 10 et sa réciproque permettent d'obtenir, sans répétition, tous les quaternions primitifs de norme n par leur décomposition en facteurs premiers. Cherchons donc d'abord le nombre $t(n)$ des quaternions primitifs de norme n.

1° Appelons p un diviseur premier de $n = pn_1$. Comparons $t(n)$ à $t(n_1)$.

Si p ne divise pas n_1, tout quaternion primitif N_1 de norme n_1 engendre $r(p)$ quaternions primitifs PN_1 de norme n. Inversement tout quaternion primitif N

se décompose en produit PN_1 de 8 manières associées. D'où

$$t(n) = \frac{r(p)}{8} t(n_1) = (p+1)t(n_1).$$

Si p impair divise n_1, et si P_1 de norme p divise à gauche le quaternion primitif N_1, le produit PN_1 est primitif à condition que PP_1 ne soit pas divisible par p, c'est-à-dire que P et $\overline{P_1}$ ne soient pas associés à droite. Inversement tout quaternion primitif N provient ainsi de 8 quaternions N_1. D'où

$$t(n) = \frac{r(p)-8}{8} t(n_1) = pt(n_1).$$

Si $p=2$ divise n_1 sans diviser $\frac{n_1}{2}$, P et $\overline{P_1}$ ne doivent pas être associés à droite. Inversement tout quaternion primitif N provient de $r(p)=24$ quaternions N_1, d'où

$$t(n) = \frac{r(p)-8}{r(p)} t(n_1) = \frac{2}{3} t(n_1).$$

Si $\frac{n_1}{2}$ est pair, n est multiple de 8 et N est divisible par 2. Par conséquent, m étant impair

$$t(2m) = 3t(m), \qquad t(4m) = 2t(m), \qquad t(8m) = 0.$$

La valeur de $t(n)$ se déduit aussitôt.

Le nombre des quaternions primitifs de norme n est égal à

$$t(n) = 8hn \prod \left(1 + \frac{1}{p}\right),$$

produit étendu à tous les diviseurs premiers de n, le coefficient h valant zéro si n est multiple de 8, valant $\frac{1}{3}$ si n est quadruple de nombre impair, valant 1 dans tout autre cas.

2° Le nombre total des quaternions de norme n, primitifs ou non, se déduit du nombre des quaternions primitifs par l'égalité

$$r(n) = \sum t\left(\frac{n}{\delta^2}\right),$$

somme étendue à tous les carrés δ^2 diviseurs de n. Ce nombre est, comme $t(n)$, une fonction factorable. Si n est exactement divisible par p^α (p premier impair), le facteur correspondant de $t(n)$ vaut $p^\alpha + p^{\alpha-1}$, celui de $r(n)$ vaut donc

$$p^\alpha + p^{\alpha-1} \ldots + p + 1,$$

qui est aussi la somme des diviseurs de p^α. Si n est pair, quelle que soit la puissance de 2 qui divise n, le facteur correspondant de $r(n)$ vaut 3.

Le nombre total $r(n)$ s'obtient par multiplication et correspond au théorème suivant, dû à Jacobi [5] :

Le nombre $r(n)$ des quaternions de norme n vaut 8 fois ou 24 fois la somme des diviseurs impairs de n, suivant que n est impair ou pair.

18. *Nombre des facteurs de norme n.* — 1° Examinons d'abord le cas des facteurs premiers.

Tout facteur premier $\mathfrak{P}$ de norme p est diviseur à gauche d'un facteur réduit $\mathfrak{A}$ associé à un quaternion réduit A de la forme

$$A = 1 + xj + yk \qquad \text{ou} \qquad A = 1 + xi.$$

Inversement, pour que deux facteurs réduits $\mathfrak{A}$ et $\mathfrak{A}_1$ soient divisibles à gauche par le même facteur $\mathfrak{P}$, il faut et il suffit que

$$AJ\overline{A}_1 \equiv 0 \pmod{p},$$

J désignant une unité quelconque. Pour cela il faut et il suffit que les valeurs absolues des composantes de A et de A_1 soient respectivement congrues suivant le module p.

En outre chaque facteur réduit étant primitif n'est divisible que par un seul facteur de norme p.

Cette correspondance biunivoque entre $\mathfrak{A}$ et $\mathfrak{P}$ donne le nombre des facteurs de norme p : il est égal au nombre total des solutions des deux congruences (indépendantes)

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}, \qquad x^2 + 1 \equiv 0 \pmod{p},$$

solutions limitées à l'intervalle $0, \frac{p}{2}$.

Le nombre des facteurs premiers de norme p vaut donc

$$\frac{p+1}{4} \quad \text{ou} \quad \frac{p+7}{4},$$

suivant que p est un multiple de 4 diminué ou augmenté de 1. Il vaut 3 si p égale 2.

2° Les facteurs de norme composée n ne peuvent être étudiés aisément à partir de leur décomposition en facteurs premiers, car ces derniers sont liés entre eux et leur structure même intervient.

Pour abréger nous dirons qu'un facteur appartient à la forme $x^2+y^2+z^2+t^2$ si ses composantes sont en valeur absolue distinctes et positives ; qu'il appartient à $2x^2+y^2$ si deux composantes ont une même valeur absolue et qu'une troisième soit nulle, etc.

Tout facteur appartenant à x^2, $2x^2$ ou $4x^2$ comprend 8 quaternions distincts. On le voit en considérant par exemple les facteurs de norme 1, 2 ou 4.

Tout facteur appartenant à x^2+y^2 ou $2x^2+2y^2$ comprend 16 quaternions distincts; c'est le cas des facteurs de norme 5 ou 10.

Tout autre facteur comprend 32 quaternions distincts. On le voit par l'étude directe des facteurs appartenant à

$$3x^2,\quad 3x^2+y^2,\quad 2x^2+y^2,\quad 2x^2+y^2+z^2,\quad x^2+y^2+z^2,\quad x^2+y^2+z^2+t^2,$$

ou bien en considérant les normes premières 3, 7, 11, 23, 59, 71 qui appartiennent successivement aux formes précédentes et pour lesquelles le nombre des quaternions $8(p+1)$ vaut 32 fois celui des facteurs.

Par conséquent, si n n'est ni un carré ni une somme de deux carrés, le nombre des facteurs de norme n et celui des facteurs primitifs de même norme valent respectivement

$$\frac{r(n)}{32},\qquad \frac{t(n)}{32}.$$

Si n est représentable par une somme de deux carrés, nous désignons par $r'(n)$ le nombre des solutions de l'équation en nombres entiers $x^2+y^2=n$ et par $t'(n)$ le nombre des solutions primitives de la même équation. On trouve que le nombre des facteurs de norme n et celui des facteurs primitifs valent respectivement

$$\frac{1}{32}\big(r(n)+6r'(n)\big),\qquad \frac{1}{32}\big(t(n)+6t'(n)\big)\qquad (n\text{ impair}),$$

$$\frac{1}{32}\big(r(n)+18r'(n)\big),\qquad \frac{1}{32}\left(t(n)+6t'(n)+12t'\left(\frac{n}{2}\right)\right)\qquad (n\text{ pair}).$$

DEUXIÈME PARTIE.

UNE ARITHMÉTIQUE DES BIQUATERNIONS.

CHAPITRE III.

CONSTRUCTION DES BIQUATERNIONS.

19. *Généralités.* — Les quaternions, nombres hypercomplexes d'ordre 4, possèdent essentiellement l'associativité du produit et la propriété multiplicative de la norme. Cette seconde propriété, qui correspond à l'identité de Lagrange, joue le principal rôle dans l'étude arithmétique des quaternions.

Aussi bien nous chercherons à étendre les résultats uniquement pour les nombres hypercomplexes d'ordre n supérieur à 4 qui vérifient la propriété multiplicative de la norme (somme des carrés des composantes). Cette extension suppose une formule transformant le produit de deux sommes de n carrés en une seule somme de n carrés. La formule existe pour $n=8$, qui est l'iden-

tité de Brioschi [8]. En outre, un théorème de Hurwitz [12] démontre l'impossibilité d'une telle formule pour n supérieur à 8.

Retrouvons l'identité de Brioschi et étudions toutes les manières possibles de l'écrire en nombres entiers.

Considérons un nombre hypercomplexe d'ordre 8

$$A = [x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7]$$

que nous écrivons encore, par abréviation,

$$A = [U, V],$$

U et V étant les quaternions de composantes respectives x_0, x_1, x_2, x_3 et x_4, x_5, x_6, x_7. Définissons comme suit le produit de A par un nombre hypercomplexe B d'ordre 8

$$AB = \| x_0\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7 \|.S,$$

où S est une matrice carrée d'ordre 8 ayant ces propriétés : les termes de S dépendent linéairement des composantes de B, les composantes de AB sont entières s'il en est de même de A et B, la norme de AB est égale au produit des normes de A et B.

Chaque ligne de la matrice est une substitution linéaire orthogonale à coefficients entiers des composantes de B : elle contient donc ces composantes une fois, à l'ordre et au signe près. Chaque colonne de même, la matrice étant orthogonale.

Or on ne change pas le problème en permutant les composantes de A ou celles de AB, c'est-à-dire en permutant les lignes ou les colonnes de la matrice. Par de telles permutations, compte tenu de l'orthogonalité de la matrice, faisons en sorte que les quatre premiers termes de la première ligne se retrouvent à l'ordre et au signe près dans la première moitié des trois lignes suivantes. Ils figurent alors dans la seconde moitié des quatre dernières lignes. La matrice S se partage en quatre matrices orthogonales d'ordre 4, correspondant chacune à un produit de quaternions.

Les composantes du produit AB sont donc, à l'ordre près, celles de

$$[CE + DF, C'F' + D'E'],$$

où [C, D] et [E, F] sont respectivement *isomorphes* de A et B (c'est-à-dire diffèrent seulement par l'ordre et le signe de leurs composantes), où les quaternions C, D, E, F et C′, D′, E′, F′ sont isomorphes deux à deux et sont écrits à l'ordre près dans chacun des produits CE, DF, C′F′, D′E′.

Il reste à étudier la condition relative aux normes

$$N(AB) = N(A)N(B) + \text{partie scalaire}\left(2CE\overline{F}\,\overline{D} + 2C'F'\overline{E}'\overline{D}'\right).$$

Cette partie scalaire doit être nulle quels que soient les quaternions. Les produits $E\overline{F}\,\overline{D}$ et $F'\overline{E}'\overline{D}'$ sont alors isomorphes, ce qui entraîne que $E\overline{F}$ et $F'\overline{E}'$

soient associés; c'est impossible pour des quaternions quelconques. Il faut donc intervertir certains facteurs et choisir l'une des formes

$$[CE + FD,\ C'F' + E'D'],$$
$$[CE + FD,\ F'C' + D'E'].$$

Dans la première forme les produits $E\overline{D}F$ et $\overline{F}'\overline{D}'\overline{E}'$ sont isomorphes, $E\overline{D}$ et $E'D'$ sont associés; de même $\overline{D}\overline{F}C$ et $C'F'\overline{D}'$ sont isomorphes, $\overline{C}F$ et $C'F'$ sont associés. Dans la seconde forme, l'échange des facteurs revient à écrire les produits conjugués.

En conclusion, les composantes du produit AB sont, à l'ordre près, celles de

$$[CE + FD,\ H + K],$$

les quaternions H et K, ou leurs conjugués, étant respectivement associés à $\overline{C}F$ et $E\overline{D}$.

20. *Les biquaternions.* — Parmi tous les systèmes correspondant aux diverses formules de multiplication, choisissons les nombres hypercomplexes qui s'apparentent le plus aux quaternions.

Nous supposons d'abord que pour A, B et AB, quatre composantes d'un même rang, les quatre premières par exemple, correspondent respectivement à C, E et $CE + FD$. Le système comprend alors les quaternions comme cas particulier

$$[X,\ O] = X \qquad \text{(quaternion X quelconque)}.$$

Désignons par D_0 et F_0 les quaternions relatifs aux quatre dernières composantes de A et B. Les quaternions D et F seront pris non seulement isomorphes, mais égaux à D_0 et F_0, ou à leurs conjugués, au signe près. Les quaternions H et K seront pris non seulement associés mais égaux à $\overline{C}F$ et $E\overline{D}$, ou à leurs conjugués, au signe près.

Deux seulement de ces nouveaux systèmes possèdent une *unité principale* 1 telle que $A1 = 1A = A$, quel que soit A. Ils sont définis respectivement par

$$[C,\ D_0].[E,\ F_0] = [CE - \overline{F}_0D_0,\ F_0C + D_0\overline{E}],$$
$$[C,\ D_0].[E,\ F_0] = [CE - F_0\overline{D}_0,\ \overline{C}F_0 + ED_0].$$

D'ailleurs on passe d'une formule à l'autre en changeant de signe les trois dernières composantes des facteurs et du produit (ce qui revient à changer de signe les trois dernières unités du système). Nous choisissons la première formule, parce qu'elle permet également d'obtenir le système des quaternions à partir des nombres complexes ordinaires. Et nous posons la définition suivante :

Un biquaternion A *est un nombre hypercomplexe d'ordre* 8 *déterminé par deux quaternions* C, D *qui jouent des rôles différents*

$$A = [C,\ D].$$

L'addition et la multiplication sont définies par

$$A + B = [C, D] + [E, F] = [C + E, D + F],$$
$$AB = [C, D].[E, F] = [CE - \overline{F}D, FC + D\overline{E}].$$

La règle du produit permet d'établir la table de multiplication des huit unités de base

$$1, \quad i, \quad j, \quad k, \quad [0, 1], \quad [0, i], \quad [0, j], \quad [0, k],$$

que nous désignerons aussi par i_0, i_1, i_2, i_3, i_4, i_5, i_6, i_7. Les produits mutuels s'écrivent

$$J'[0, J] = -[0, J]J' = [0, JJ'],$$
$$[0, J][0, J'] = J'J, \qquad [0, J']^2 = -1,$$

J et J′ étant l'une ou l'autre des quatre premières unités, J′ étant toutefois différente de l'unité principale 1.

On voit ainsi que les sept dernières unités peuvent être groupées en *sept triades* où la loi de multiplication est vérifiée comme pour les quaternions unités i, j, k. Ce sont

$$(i_1, i_2, i_3), \quad (i_1, i_4, i_5), \quad (i_1, i_7, i_6), \quad (i_2, i_4, i_6), \quad (i_2, i_5, i_7), \quad (i_3, i_4, i_7), \quad (i_3, i_6, i_5).$$

Nous reconnaissons là une propriété des nombres étudiés par Cayley sous le nom d'*octaves* [7], eux-mêmes utilisés par G. Fontené sous le nom d'octants [13]. Notre système de biquaternions, à l'ordre près des unités, ne diffère pas des octaves de Cayley.

21. *Propriétés algébriques.* — 1° Le produit de deux biquaternions A et B est un biquaternion dont les composantes sont des formes bilinéaires des composantes de A et de B.

Remarquons que deux biquaternions, dont les quatre premières ou les quatre dernières composantes sont nulles, ont un produit de la même forme.

Le produit d'un nombre quelconque de biquaternions se calcule de proche en proche : on multiplie les deux premiers, on multiplie le résultat par le troisième, et ainsi de suite

$$ABCD = \big((AB)C\big)D.$$

La multiplication, distributive par rapport à l'addition, n'est *ni commutative, ni associative.*

Deux biquaternions ayant même première composante (partie scalaire), et dont les autres composantes sont opposées deux à deux, sont dits *conjugués*

$$A = [E, F], \qquad \overline{A} = [\overline{E} - F];$$

leur produit est un nombre scalaire égal à leur norme commune, somme des carrés des composantes

$$N(A) = N(\overline{A}) = A\overline{A} = \overline{A}A.$$

C'est là un cas particulier de produit commutatif, un autre cas simple étant le produit de deux biquaternions dont l'un est scalaire.

Rappelons que *la norme d'un produit est égale au produit des normes*, par construction même des biquaternions. Il en résulte qu'un produit est nul seulement si un des facteurs est nul (il n'y a pas lieu par conséquent d'étudier les diviseurs de zéro) :

$$AB = AB' \quad (A \neq 0) \qquad \text{entraîne} \qquad B = B'.$$

Le *conjugué d'un produit* de deux facteurs est le produit des conjugués changés d'ordre

$$\overline{AB} = \overline{B}\,\overline{A}.$$

On le vérifie en remplaçant chaque facteur par ses quaternions composants. Cependant le produit $\overline{C}\,\overline{B}\,\overline{A}$ n'est pas le conjugué de ABC, la multiplication n'étant pas associative.

Il y a 16 biquaternions entiers (à composantes entières) de norme 1, qui forment le groupe des *unités*; elles seront habituellement désignées par J

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \pm i_4, \quad \pm i_5, \quad \pm i_6, \quad \pm i_7.$$

Leurs inverses sont aussi des biquaternions entiers. Le produit par une unité J ne change pas la norme.

2° Revenons sur les propriétés de la multiplication, notamment sur l'associativité. Nous allons indiquer des conditions suffisantes simples pour que trois biquaternions A, B, C vérifient

$$(AB)C = A(BC).$$

Tout d'abord il suffit qu'un des biquaternions soit un scalaire, celui-ci pouvant être associé à un facteur quelconque du produit.

Par ailleurs, sept triades d'unités suivent la loi de multiplication des quaternions unités i, j, k, et créent une sorte d'*associativité partielle*. Il suffit que A, B, C appartiennent en même temps au sous-système de biquaternions relatif à l'une des triades; ce qui a lieu, par exemple, si les deuxième, troisième, cinquième et huitième composantes sont nulles pour chaque biquaternion.

On trouve encore de nouvelles conditions en remplaçant A, B, C par leurs quaternions composants, et en étudiant les relations obtenues :

Il suffit que les facteurs extrêmes A et C soient égaux et qu'ils aient leurs quatre premières ou dernières composantes nulles

$$ABA = A(BA), \qquad A = [A', 0] \quad \text{ou} \quad [0, A'].$$

Ce qui a lieu notamment si A est l'une des seize unités

$$JBJ = J(BJ), \qquad N(J) = 1.$$

Il suffit enfin, condition importante, que les deux derniers biquaternions B et C soient conjugués

$$AB\overline{B} = bA, \qquad b = N(B).$$

Autrement dit, *deux biquaternions conjugués consécutifs d'un produit peuvent être remplacés par leur norme commune*

$$AB\overline{B}D = bAD, \qquad b = N(B).$$

Remarque. — Observons la gradation des propriétés pour les nombres hypercomplexes d'ordre 2^h, chaque système d'ordre 2^h étant un sous-système du suivant d'ordre 2^{h+1} :

$h = 1$, nombres complexes ordinaires (formant un corps) : la multiplication est commutative et associative;

$h = 2$, quaternions (formant un corps gauche) : la multiplication est associative, non commutative;

$h = 3$, biquaternions : la multiplication n'est ni commutative, ni associative;

$h = 4$, la mutiplication ne possède pas la propriété des normes.

CHAPITRE IV.

LES BIQUATERNIONS ENTIERS.

22. *Divisibilité des biquaternions entiers.* — Nous appelons *biquaternions entiers* ceux dont les composantes sont des nombres entiers. Cherchons-en les propriétés.

La multiplication n'étant pas en général associative, plusieurs résultats de l'arithmétique des quaternions ne s'étendent pas directement aux biquaternions. Une autre difficulté se présente : dans la division d'un quaternion par un entier scalaire m, la norme du reste est généralement inférieure à m^2, et cette propriété a donné une méthode de descente largement utilisée dans les premiers numéros; or, pour les biquaternions, une définition semblable du reste conduit à une norme inférieure seulement à $2m^2$.

Nous définissons, comme pour les quaternions (n° 3), la divisibilité à droite ou à gauche, en remarquant toutefois que le produit ABC, s'il est divisible à droite par C, n'est pas en général divisible à gauche par A. Nous obtenons la même condition de divisibilité suivante :

Pour que A *soit divisible par* B *à gauche* (*ou à droite*), *il faut et il suffit que* $\overline{B}A$ (ou $A\overline{B}$) *soit divisible par la norme de* B.

En effet, eu égard à l'associativité des facteurs conjugués,

$$A = BX \quad \text{équivaut à} \quad \overline{B}A = N(B)X,$$
$$A = YC \quad \text{équivaut à} \quad A\overline{C} = N(C)Y.$$

On démontre comme au n° 3 que, si deux biquaternions ont des normes premières entre elles, le p. g. d. scalaire de leur produit est le produit des p. g. d. scalaires des facteurs.

La notion d'associés à gauche (ou à droite) est moins utile, la divisibilité n'étant pas transitive pour les biquaternions. Toutefois nous conservons la définition : les *associés* à gauche de A sont les seize biquaternions AJ, où J désigne une unité quelconque. Inversement A est associé à AJ puisque $A = AJ\bar{J}$. Mais deux biquaternions associés à un même troisième ne sont pas nécessairement associés.

23. *Classes de biquaternions* (mod m). — Deux biquaternions A et B sont congrus suivant le module scalaire positif m, si leur différence est divisible par m

$$B \equiv A \pmod{m}.$$

Plus généralement nous dirons que A et B appartiennent à une *même classe* suivant le module m s'il existe un nombre entier u *premier avec* m tel que, suivant le cas,

$$B \equiv uA \pmod{m \text{ impair}},$$

$$B \equiv uA + \frac{m}{2}K \pmod{m \text{ pair}},$$

K désignant un biquaternion de norme o ou 8, dont toutes les composantes sont égales à o ou à 1. Ces deux congruences se réduisent d'ailleurs à la seconde, pour une valeur paire ou impaire de m. La définition est bien réciproque puisque

$$A \equiv u'B + \frac{m}{2}K, \qquad uu' \equiv 1 \pmod{m}.$$

Les classes, suivant le module m, s'ajoutent, se retranchent et se multiplient (produit non associatif). Leur principale propriété est celle-ci :

Tous les biquaternions d'une même classe (mod m) *ont les mêmes diviseurs de norme* m, *à droite ou à gauche, si toutefois il en existe.*

En effet appelons M un biquaternion de norme m, et comparons les caractères de divisibilité de A et B, à droite par exemple. Si m est pair, toute forme linéaire des composantes de $\bar{M}$ dont les coefficients sont tous pairs ou tous impairs est divisible par 2; le produit $K\bar{M}$ est donc divisible par 2. Dans tous les cas nous pouvons écrire

$$B\bar{M} \equiv uA\bar{M} + \frac{m}{2}K\bar{M} \equiv uA\bar{M} \pmod{m}.$$

Si M est diviseur à droite de A, il l'est de B.

La *classe nulle,* contenant o, est l'ensemble des biquaternions divisibles par m, auxquels il convient d'ajouter, lorsque m est pair, tous ceux dont les compo-

santes sont des multiples impairs de $\frac{m}{2}$. Tout biquaternion de la classe nulle $(\mathrm{mod}\, m)$ est divisible à droite et à gauche par tous les biquaternions de norme m.

24. *Restes des biquaternions* $(\mathrm{mod}\, m)$. — Considérons un biquaternion A et prenons les restes minima absolus de ses composantes suivant le module m. Nous obtenons un biquaternion R de la même classe que A, dont les composantes ont une valeur absolue au plus égale à $\frac{m}{2}$, dont la norme est au plus égale à $2m^2$. Nous l'appelons *reste de* A suivant le module m :

$$\mathrm{R} \equiv \mathrm{A} \pmod{m}, \qquad \mathrm{N}(\mathrm{R}) \leqq 2m^2.$$

La même opération peut être faite sur tous les biquaternions d'une même classe. Nous allons montrer que,

dans une classe $(\mathrm{mod}\, m)$ *définie par le biquaternion* A, *il existe au moins un biquaternion* R_0 *dont la norme est au plus égale à* m^2 ; nous l'appelons *reste de la classe* ou *moindre reste de* A $(\mathrm{mod}\, m)$:

$$\mathrm{R}_0 \equiv u\,\mathrm{A} + \frac{m}{2}\mathrm{K} \pmod{m}, \qquad \mathrm{N}(\mathrm{R}_0) \leqq m^2.$$

1° Supposons m pair. En remarquant que $u = 1$ est le seul nombre qui soit premier avec tous les nombres pairs, nous considérons les deux restes

$$\mathrm{R} \equiv \mathrm{A}, \qquad \mathrm{R}' \equiv \mathrm{A} + \frac{m}{2}\mathrm{K} \pmod{m}.$$

Si x est une des composantes du premier reste, la composante de même rang du second est $x \pm \frac{m}{2}$; la somme de leurs carrés est au plus égale à $\frac{m^2}{4}$, l'égalité n'ayant lieu que si x vaut 0 ou $\frac{m}{2}$. La somme des deux normes est donc inférieure à $2m^2$; elle égale $2m^2$ si quatre composantes sont nulles et que les quatre autres vaillent $\frac{m}{2}$.

Un au moins des deux restes R, R′ *a une norme au plus égale à* m^2, certainement inférieure si A est primitif.

2° Supposons m impair. Les puissances de 2 sont les seuls nombres premiers avec tous les nombres impairs. Étudions donc les restes des multiples suivants de A :

$$\mathrm{R} \equiv \mathrm{A}, \quad \mathrm{R}_1 \equiv 2\mathrm{A}, \quad \ldots, \quad \mathrm{R}_\alpha \equiv 2^\alpha \mathrm{A} \pmod{m}.$$

Soient $x, x_1, \ldots, x_\alpha$ les valeurs absolues des composantes d'un même rang des divers restes. x_1^2 est égal à $(2x)^2$ ou à $(m-2x)^2$ suivant que x se trouve dans l'intervalle $\left(0, \frac{m}{4}\right)$ ou dans $\left(\frac{m}{4}, \frac{m}{2}\right)$. Supposons un instant que x prenne

toutes les valeurs rationnelles de chaque intervalle, entières ou non. A deux valeurs de x symétriques par rapport à $\frac{m}{4}$ correspond le même x_1. Le maximum de la somme $x^2+x_1^2$ a donc lieu dans l'intervalle $\left(\frac{m}{4}, \frac{m}{2}\right)$; la somme s'exprime alors par $x^2+(m-2x)^2$, trinome du second degré borné supérieurement par la plus grande des valeurs prises aux limites de l'intervalle : le maximum a lieu pour $x=\frac{m}{4}$.

Le raisonnement se poursuit pareillement : à deux valeurs de x_1 ayant pour somme $\frac{m}{4}+\frac{m}{2}$ correspond la même valeur de x_2. Le maximum de $x^2+x_1^2+x_2^2$ a lieu dans la première moitié de l'intervalle $\left(\frac{m}{4}, \frac{m}{2}\right)$, c'est-à-dire $\left(\frac{m}{4}, \frac{3m}{8}\right)$. La somme s'écrit alors

$$x^2+(m-2x)^2+(4x-m)^2.$$

Son maximum s'obtient à l'une des limites de l'intervalle, ici $\frac{3m}{8}$.

Par le même procédé dichotomique, en étudiant la formation des termes, on aboutit à la borne supérieure de

$$z=x^2+x_1^2+\ldots+x_\alpha^2.$$

Les intervalles successifs sont limités par les fractions

$$u_1=\frac{m}{2}, \qquad u_2=\frac{m}{4}, \qquad u_3=\frac{3m}{8}, \qquad \ldots, \qquad u_\alpha=\frac{2^\alpha-(-1)^\alpha}{3.2^\alpha}m,$$

où chaque fraction est la moyenne arithmétique des deux précédentes. Par récurrence on prouve que la somme z est maximum à l'une des limites de l'intervalle $(u_\alpha, u_{\alpha+1})$ et qu'elle s'écrit alors

$$z=x^2+4\left(x-\frac{m}{2}\right)^2+4\left(x-\frac{m}{4}\right)^2+\ldots+4^\alpha(x-u_\alpha)^2.$$

La valeur relative à $x=u_{\alpha+1}$ est supérieure à celle qu'on obtient pour $x=u_\alpha$.

Par conséquent, quel que soit x et particulièrement pour x entier, la somme z est inférieure à la valeur qu'elle prendrait pour $x=u_{\alpha+1}$, c'est-à-dire, tous calculs faits,

$$x^2+x_1^2+\ldots+x_\alpha^2<\left(\frac{\alpha+2}{9}+\frac{1}{27.(-2)^\alpha}-\frac{1}{108.4^\alpha}\right)m^2.$$

Nous obtenons notamment

$$x^2+x_1^2+\ldots+x_7^2<m^2.$$

Ajoutons maintenant les carrés des huit composantes; nous voyons que les normes de R, R_1, ..., R_7 ont une somme inférieure à $8m^2$. Une au moins des normes est donc inférieure à m^2 :

Si m est impair, un au moins des huit multiples A, 2A, 2^2A, ..., 2^7A *a pour reste* (mod m) *un biquaternion de norme inférieure à* m^2.

Augmentons indéfiniment le nombre α. La norme moyenne

$$\frac{1}{\alpha+1}[N(R)+N(R_1)+\ldots+N(R_\alpha)]$$

reste inférieure à un nombre qui tend vers $\frac{8}{9}m^2$. Appelons h le plus petit exposant vérifiant

$$2^h \equiv \pm 1 \pmod{m},$$

qui est d'ailleurs un diviseur de l'indicateur d'Euler $\frac{1}{2}\varphi(m)$. La norme de R_α redevient la même lorsque α augmente d'un multiple de h. Il s'ensuit que la norme moyenne des h premiers restes ne dépasse pas $\frac{8}{9}m^2$.

Si h est le plus petit nombre vérifiant $4^h \equiv 1 \pmod{m}$ impair), un au moins des h multiples A, 2A, ..., 2^{h-1}A *a pour reste* (mod$m$) *un biquaternion de norme inférieure à* $\frac{8}{9}m^2$. Le moindre reste de A (mod$m$) a une norme inférieure à $\frac{8}{9}m^2$.

En particulier si s composantes de A sont nulles, la borne supérieure $\frac{8}{9}m^2$ s'abaisse à $\frac{8-s}{9}m^2$. Ainsi *pour les quaternions, au moins un des h multiples donne un reste de norme inférieure à* $\frac{4}{9}m^2$.

25. *Étude des diviseurs de norme* 2. — Le facteur 2 jouit de propriétés spéciales, celle-ci d'abord :

Tout diviseur à droite de norme 2 *est un diviseur à gauche, et inversement.*

En effet si P est un diviseur de A, à droite, de norme 2, il vérifie

$$A\overline{P} \equiv \overline{A}P \equiv \overline{P}A \equiv 0 \pmod{2},$$

et est aussi un diviseur à gauche.

Considérons un biquaternion A de norme paire. Son moindre reste R (mod 2) a une norme au plus égale à 4. Plusieurs cas se présentent.

1° Si R est nul, les huit composantes de A sont de même parité. A appartient à la classe nulle (mod 2) et est divisible par tous les biquaternions P de norme 2; ceux-ci sont au nombre de 16.7.

2° Si la norme de R vaut 2, deux ou six composantes de A sont impaires. A et R sont divisibles à droite et à gauche par les mêmes biquaternions de norme 2, qui sont les 16 biquaternions associés RJ.

3° Si la norme de R vaut 4, c'est que A contient quatre composantes impaires.

Considérons, par exemple, les quatre premières ou dernières composantes impaires :

$$R = \pm 1 \pm i_1 \pm i_2 \pm i_3 \qquad \text{ou} \qquad R = \pm i_4 \pm i_5 \pm i_6 \pm i_7.$$

Pour que le biquaternion P de norme 2 soit un diviseur de R, il faut et il suffit que $R\overline{P}$ soit divisible par 2, c'est-à-dire que les deux composantes unitaires de P soient en même temps dans les quatre premiers rangs ou dans les quatre derniers. R est alors divisible par 16.3 biquaternions P formant trois groupes de diviseurs associés.

Comme deuxième exemple, prenons

$$R = \pm 1 \pm i_2 \pm i_5 \pm i_7 \qquad \text{ou} \qquad R = \pm i_1 \pm i_3 \pm i_4 \pm i_6.$$

R est divisible par **P** à condition que les deux composantes unitaires de P soient en même temps dans les premier, troisième, sixième, huitième rangs, ou en même temps dans les quatre autres rangs. R admet 16.3 diviseurs de norme 2, plus exactement trois groupes de diviseurs associés.

Le même raisonnement s'applique aux biquaternions R, et aux complémentaires, dont les trois composantes unitaires autres que la première forment l'une des triades du n° 20. Ces biquaternions sont au nombre de 16.14.

Tous les autres biquaternions R, au nombre de 16.70, sont *indécomposables*, c'est-à-dire n'admettent aucun diviseur de norme 2.

Vérifions-le en dénombrant les produits de la forme

$$PP' = A, \qquad N(P) = N(P') = 2.$$

Aux 16 biquaternions A divisibles par 2 et aux 16.14 biquaternions A relatifs aux triades correspondent respectivement

$$16.7.16 = 16^2.7, \qquad 16.3.16.14 = 16^2.42.$$

décompositions PP'. Tous les produits possibles PP' ont été considérés puisque leur nombre total vaut $16^2.7^2$. Il n'y a donc pas de décomposition en dehors des précédentes.

26. *Décomposition en facteurs.* — Nous avons établi pour les quaternions (n^{os} 8 et 9) deux procédés de décomposition en produit de facteurs. Seul le second procédé peut être étendu aux biquaternions, car il n'exige pas l'associativité du produit; en outre, il est valable pour des facteurs quelconques, premiers ou non.

Supposons la norme de A égale à qq_1 et formons un *moindre reste* R_1 de $\overline{A}$ suivant le module q_1. La norme de R_1 est un multiple de q_1 au plus égal à q_1^2

$$R_1 \equiv u_1\overline{A} + \frac{q_1}{2}K \pmod{q_1}, \qquad N(R_1) = q_1 q_2,$$

$$q_2 = u_1^2 q + \text{partie scalaire}\,(u_1 KA) + \frac{q_1}{4}N(K), \qquad 0 \leqq q_2 \leqq q_1,$$

u_1 et K ayant la même signification qu'au n° 24. La recherche des diviseurs de A à gauche de norme q équivaut à la recherche des diviseurs à droite de norme q_1, eux-mêmes conjugués des diviseurs à gauche de R_1.

Renouvelons l'opération en considérant le moindre reste R_2 de $\overline{R_1}$ suivant le module q_2. Et ainsi de suite, jusqu'à

$$R_h \equiv u_h \overline{R}_{h-1} + \frac{q_h}{2} K \pmod{q_h}, \qquad N(R_h) = q_h q_{h+1}, \qquad 0 \leqq q_{h+1} \leqq q_h.$$

Il suffit en définitive d'étudier les diviseurs de R_h à gauche de norme q_h.

Nous supposons que pour la première fois q_{h+1} est égal à l'une de ses limites, ce qui correspond à (n° 24)

$$R_h = \frac{q_h}{2} C, \qquad q_{h+1} = 0 \quad \text{ou} \quad q_h,$$

C étant nul ou primitif de norme 4.

D'une manière générale, écrivons

$$R_i = \frac{m}{2} C_i, \qquad q_{i+1} \equiv q_i \equiv 0 \pmod{m},$$

la norme de C_i étant multiple de 4, et montrons que ces conditions s'étendent aux indices supérieurs et inférieurs :

$$R_{i+1} = u_{i+1} \overline{R}_i + \frac{q_{i+1}}{2} (K + 2X) = \frac{m}{2} C_{i+1},$$

$$R_{i-1} = u_i' \overline{R}_i + \frac{q_i}{2} (K + 2Y) = \frac{m}{2} C_{i-1} \qquad (u_i u_i' \equiv 1 ; \bmod q_i),$$

$$q_{i+2} = u_{i+1}^2 q_i + \text{partie scalaire} \left(m u_{i+1} \frac{KC_i}{2} + m u_{i+1} X C_i \right) + \frac{q_{i+1}}{4} N(K + 2X) \equiv 0 \pmod{m},$$

$$q_{i-1} = u_i'^2 q_{i+1} + \text{partie scalaire} \left(m u_i' \frac{KC_i}{2} + m u_i' Y C_i \right) + \frac{q_i}{4} N(K + 2Y) \equiv 0 \pmod{m}.$$

Les normes de $K + 2X$, $K + 2Y$ et C_i sont en effet multiples de 4 et le produit KC_i est divisible par 2.

Ceci posé, le dernier reste est de la forme

$$R_h = \frac{m}{2} C, \qquad m = q_h, \qquad N(C) = 0 \quad \text{ou} \quad 4,$$

et le scalaire m divise à la fois $2R_h$, q_{h+1}, q_h. En raisonnant de proche en proche sur $R_{h-1}, \ldots, R_2, R_1, A$, dans les deux sens, nous voyons que m divise à la fois $2A$, q et q_1, et qu'il est le plus grand nombre tel.

En outre, si m est impair, tous les biquaternions C_i sont divisibles par 2, notamment le premier qui est $\frac{2A}{m}$, et le dernier C qui est nul. Si m est pair, tous les C_i appartiennent à la même classe suivant le module 2, comme le montre l'expression de R_{i+1}. Dans les deux cas on peut dire que C est le moindre reste de $\frac{2A}{m}$ suivant le module 2.

Le problème est alors ramené à la recherche des biquaternions de norme m, diviseurs à gauche de $\frac{m}{2} C$. Examinons les cas possibles.

Premier cas. — Le dernier reste est nul, $C = o$. Il est divisible par tous les biquaternions de norme m. Le nombre des décompositions de A en produit de facteurs de normes q, q_1 est donc égal au nombre des biquaternions de norme m. Tous les restes R_i sont eux-mêmes décomposables sous la forme

$$A = QQ_1, \qquad R_1 = \overline{Q}_1 Q_2, \qquad \ldots, \qquad R_{h-1} = \overline{Q}_{h-1} M,$$

où M est un biquaternion quelconque de norme m. L'élimination des Q_i donne l'expression du facteur Q_1,

$$q_2 \ldots q_{h-1} q_h Q_1 = M \overline{R}_{h-1} \overline{R}_{h-2} \ldots \overline{R}_2 \overline{R}_1.$$

d'où l'on tire l'expression de Q.

Deuxième cas. — Si C n'est pas nul, il est primitif de norme 4. Le dernier reste R_h a quatre composantes nulles et les quatre autres égales à $\pm \frac{m}{2}$. Le scalaire m est pair. Les diviseurs à gauche de R_h, dont la norme égale m, vérifient nécessairement

$$\overline{M} R_h \equiv o \pmod{m}, \qquad \overline{M} C \equiv o \pmod{2}.$$

Examinons deux nouveaux cas.

a. Si $\frac{m}{2}$ est impair, le reste de $M \pmod 2$ est un biquaternion P de norme 2. Pour que $\overline{P}C$ soit divisible par 2, il faut et il suffit que M et C aient un diviseur commun de norme 2.

Si C est indécomposable, il en est de même de R_h et de A.

Si C est décomposable, il est divisible (n° 25) par trois biquaternions P non associés, lesquels divisent M. En multipliant tous les biquaternions de norme $\frac{m}{2}$ par ces trois biquaternions P, on obtient sans répétition tous les M : il y a alors trois fois plus de décompositions pour A que de biquaternions de norme $\frac{m}{2}$.

b. Si $\frac{m}{2}$ est pair, il existe des biquaternions M divisibles par 2, et ceux-ci rendent divisible le produit $\overline{M}C$. La décomposition est donc possible. Le nombre des solutions se calcule moins aisément; notons seulement qu'il surpasse le nombre des biquaternions de norme $\frac{m}{4}$.

La formule donnant Q_1 est encore valable, à condition que M soit remplacé par les biquaternions appropriés.

Résumons les résultats obtenus.

27. Théorème. — *Soit un biquaternion* A *de norme* qq_1 *que l'on cherche à décomposer en produit de facteurs* $N = QQ_1$ *de normes respectives* q *et* q_1. *Soit* m *le plus grand nombre scalaire qui divise à la fois* 2A, q *et* q_1.

Le moindre reste C *de* $\frac{2A}{m} \pmod 2$ *a pour norme* 0 *ou* 4.

Si C *est nul,* A *est décomposable en autant de produits qu'il y a de biquaternions de norme m. Les facteurs* Q *et* Q_1 *calculables par l'algorithme du* n° 26, *sont de la forme*

$$lQ_1 = MS_1S_2\ldots S_\alpha, \qquad lq_1\overline{Q} = MS_1S_2\ldots S_\alpha\overline{A},$$

l étant un entier scalaire, M *un biquaternion quelconque de norme m, et* S_1, S_2, ..., S_α *certains biquaternions de normes croissantes.*

Si la norme de C *vaut* 4, A *est décomposable d'autant de manières qu'il y a de biquaternions* M *de norme m rendant le produit* MC *divisible par* 2. *Alors,* M *vérifiant cette condition, les facteurs* Q *et* Q_1 *ont la forme indiquée pour* C *nul.*

Le biquaternion A *ne peut être décomposé en facteurs de normes q et* q_1 *dans le seul cas où m est le double d'un nombre impair,* C *étant un biquaternion indécomposable de norme* 4.

Corollaires. — 1° Si q et q_1 sont premiers entre eux, tout biquaternion A de norme qq_1 est décomposable en produit $A = QQ_1$ de 16 manières.

2° La norme d'un biquaternion quelconque A étant décomposée en produit de h puissances de nombres premiers distincts, le biquaternion A peut être décomposé en produit correspondant de 16^{h-1} manières

$$N(A) = q_1q_2\ldots q_h, \qquad A = Q_1Q_2\ldots Q_h.$$

3° La norme d'un biquaternion A primitif, supposée non divisible par 4, étant décomposée en produit de k facteurs premiers non nécessairement distincts rangés dans un certain ordre, le biquaternion A peut être décomposé en produit de 16^{k-1} manières

$$N(A) = p_1p_2\ldots p_k, \qquad A = P_1P_2\ldots P_k.$$

4° Les seuls biquaternions *indécomposables* en produit de facteurs (dont aucun n'est unitaire) sont :

les biquaternions premiers, dont la norme est un nombre premier,

les biquaternions primitifs ayant pour norme une puissance de 2, et pour reste (mod 2) un biquaternion indécomposable de norme 4.

Exemple :

$$A = [7, 6, 5, 3, 2, 2, 1, 0].$$

5° Soit A un biquaternion de norme qq_1 indécomposable en facteurs de normes q et q_1. En permutant deux composantes convenablement choisies, on obtient un biquaternion décomposable.

Ainsi

$$A = [7, 6, 3, 5, 2, 2, 1, 0]$$

est décomposable en deux facteurs de normes quelconques ayant 128 pour produit.

28. *Ensemble des multiples d'un biquaternion premier.* — Étant donné un biquaternion premier P de norme p, l'ensemble de ses multiples

$$PX \qquad (X \text{ biquaternion entier quelconque})$$

ne constitue plus un idéal : il n'est pas conservé par multiplication à droite par un biquaternion. Cet ensemble est formé de classes suivant le module p :

$$uPX + pX_1 = P(uX + \overline{P}X_1).$$

Nous allons montrer que, parmi les multiples d'un biquaternion premier P, se trouve un biquaternion simple, ou *réduit*, dont la partie scalaire vaut 1 et dont trois composantes sont nulles. D'une manière plus précise :

Tout biquaternion premier est diviseur à gauche d'un biquaternion réduit de l'une des formes

$$1 + x_1 i_1, \quad 1 + x_2 i_2 + x_3 i_3, \quad 1 + x_4 i_4 + x_5 i_5 + x_6 i_6 + x_7 i_7,$$

les deux premières formes étant, si l'on veut, des quaternions réduits.

Prenons d'abord le cas particulier d'un biquaternion premier ayant ses quatre dernières ou ses quatre premières composantes nulles :

$$P = [P, 0], \qquad P' = [0, \overline{P}].$$

Le quaternion P est diviseur à gauche d'un quaternion réduit U. Il en résulte que P et P′ sont diviseurs à gauche des deux biquaternions réduits conjugués

$$U = PQ, \qquad \overline{U} = P'[0, -Q].$$

Pour le cas général nous posons

$$P = [A, B], \qquad N(P) = p.$$

La norme de A, inférieure à p, première avec p, a pour inverse un entier a', suivant le module p. Écrivons

$$a' P \overline{A} = [a' A\overline{A}, a' BA] \equiv [1, a' BA] \pmod{p}.$$

Ce dernier biquaternion réduit admet bien P comme diviseur à gauche.

29. *Décomposition d'un biquaternion réduit.* — Considérons un biquaternion premier P, diviseur à gauche d'un biquaternion réduit U :

$$U = PQ.$$

Retrouvons P à partir de U, par l'algorithme du n° 26, en utilisant les seuls restes normaux, sans multiplicateur : c'est ici possible car l'existence des composantes nulles diminue la norme. Nous obtenons

$$R_i \equiv \overline{R}_{i-1} \pmod{q_i}, \qquad N(R_i) = q_i q_{i+1}.$$

Les restes successifs sont des biquaternions réduits de la même forme que U. Leurs normes sont décroissantes puisque

$$N(R_i) \leqq 1 + \left(\frac{q_i}{2}\right)^2 + \left(\frac{q_i}{2}\right)^2 + \left(\frac{q_i}{2}\right)^2 + \left(\frac{q_i - 1}{2}\right)^2 < q_i^2, \qquad q_{i+1} < q_i$$

(sauf peut-être si q_i valait 2; mais R_i serait un biquaternion réduit de norme 4, nécessairement indécomposable, contrairement à l'hypothèse faite sur U). La dernière norme non nulle q_h est donc obligatoirement égale à 1.

Le diviseur à gauche P prend finalement la forme

$$q q_1 \dots q_{h-1} \overline{P} = J \overline{R}_{h-1} \dots \overline{R}_1 \overline{R}_0 \overline{U}.$$

L'unité J, si elle est différente de 1, a pour double le carré du biquaternion réduit $1 + J$. Le second membre de l'égalité devient un produit de biquaternions réduits.

En remarquant que le calcul peut se faire pour $\overline{P}$ comme pour P, et que, d'autre part, tout biquaternion est en général un produit de biquaternions premiers, nous aboutissons au résultat :

Tout biquaternion premier P *est décomposable en produit de biquaternions réduits, à un coefficient scalaire l près,*

$$l P = U_1 U_2 U_3 \dots.$$

Tout biquaternion A, de norme non divisible par 4, est décomposable en produits composés de biquaternions réduits, à un coefficient scalaire près,

$$l A = (U_1 U_2 U_3 \dots)(U_4 U_5 \dots) \dots.$$

30. *Unicité des biquaternions réduits.* — 1° Montrons que *le biquaternion réduit d'un même ensemble de multiples* PX *est unique* (à un multiple près de la norme p). Nous représentons le biquaternion P par ses quaternions composants :

$$P = [A, B], \qquad N(P) = p.$$

Supposons d'abord que l'ensemble des multiples contienne un biquaternion réduit U de l'une des deux premières formes, c'est-à-dire

$$U = [V, o] = P X_0.$$

Il en résulte

$$\overline{P} U \equiv o, \qquad \overline{A} V \equiv V \overline{B} \equiv o \pmod{p}.$$

Le quaternion V étant primitif, il faut que les normes de A et B soient divisibles par p. Le biquaternion P a donc ses quatre premières ou dernières composantes nulles

$$P = [A, o] \quad \text{ou} \quad P = [o, B].$$

Suivant le cas, V est l'unique quaternion réduit divisible à gauche par A, ou à

droite par B. Le biquaternion U est bien déterminé d'une manière unique à partir de P, à un multiple près de p.

Supposons maintenant que le biquaternion réduit U soit de la troisième forme, c'est-à-dire

$$U = [1, V] = PX_0.$$

Il en résulte

$$\overline{P}U \equiv 0, \qquad A + \overline{B}V \equiv B - V\overline{A} \equiv 0 \pmod{p}.$$

Aucun des quaternions A ou B n'est congru à zéro, car l'autre le serait également, ce qui est impossible. La norme de A est donc première avec p et a pour inverse un entier a'. Nous obtenons

$$a'N(A) \equiv 1, \qquad V\overline{A}A \equiv BA, \qquad V \equiv a'BA \pmod{p}.$$

L'expression de V, et celle de U, sont alors définies en fonction de P, à un multiple près de la norme p.

2° La propriété d'unicité établit une correspondance entre les biquaternions de norme p et les biquaternions réduits de norme divisible par p. A tout biquaternion réduit de l'une des trois formes, c'est-à-dire à toute solution d'une certaine congruence suivant le module p, correspondent 16 biquaternions premiers. Cependant à un biquaternion réduit de norme 4, nécessairement indécomposable, ne correspond aucun biquaternion de norme 2. D'où l'énoncé relatif aux normes impaires :

Le nombre des biquaternions de norme p premier impair vaut 16 *fois le nombre total des solutions des trois congruences indépendantes*

$$x^2 + y^2 + z^2 + t^2 + 1 \equiv 0 \pmod{p},$$
$$x^2 + y^2 + 1 \equiv 0 \pmod{p},$$
$$x^2 + 1 \equiv 0 \pmod{p}.$$

Ces nombres de solutions résultent d'ailleurs de formules plus générales établies par V.-A. Lebesgue [9]. Étudions la première congruence en partant de la seconde :

Si $p - 1$ est multiple de 4, les congruences

$$x^2 + y^2 \equiv m, \qquad z^2 + t^2 \equiv m' \pmod{p}$$

ont chacune $p - 1$ solutions. Toutefois si m est nul, ou m', le nombre des solutions devient $2p - 1$. En faisant $m + m' = -1$, nous obtenons le nombre cherché

$$(p-2)(p-1)^2 + 2(p-1)(2p-1) = p^3 - p.$$

Si $p + 1$ est multiple de 4, nous avons respectivement comme nombres de solutions $p + 1$ et 1, au lieu de $p - 1$ et $2p - 1$. Le nombre cherché reste le même.

Le nombre total vaut dans les deux cas

$$16(p^3-p)+16(p+1)=16(p^3+1).$$

Le nombre des biquaternions de norme p premier impair est

$$r(p)=16(p^3+1).$$

31. *Nombre des biquaternions de norme n.* — Ce nombre vient d'être calculé pour n premier.

Pour n quelconque, nous suivons une méthode semblable à celle du n° 17, en recherchant d'abord les biquaternions primitifs de norme n. Nous utilisons le théorème du n° 27 et son corollaire 3°.

1° Cherchons le nombre $t(n)$ des biquaternions primitifs de norme impaire donnée n. Appelons p un diviseur premier de $n=pn_1$, et comparons $t(n)$ à $t(n_1)$.

Si p ne divise pas n_1, tout biquaternion primitif N_1 de norme n_1 engendre $r(p)$ biquaternions primitifs PN_1 de norme n. Inversement tout biquaternion primitif N se décompose en produit PN_1 de 16 manières. D'où

$$t(n)=\frac{r(p)}{16}t(n_1)=(p^3+1)t(n_1).$$

Si p divise n_1, tout biquaternion primitif N_1 est divisible à gauche par 16 biquaternions P_1 de norme p. Le produit PN_1 n'est primitif que si $\overline{P}$ n'est pas diviseur à gauche de N_1, c'est-à-dire si P n'est égal à aucun des 16 biquaternions $\overline{P_1}$. Inversement tout biquaternion primitif N provient ainsi de 16 biquaternions N_1. D'où

$$t(n)=\frac{r(p)-16}{16}t(n_1)=p^3t(n_1).$$

Il en résulte que *le nombre des biquaternions primitifs de norme impaire n vaut*

$$t(n)=16n^3\prod\left(1+\frac{1}{p^3}\right),$$

produit étendu à tous les diviseurs premiers de n.

2° Le nombre total des biquaternions de norme n se déduit du nombre des biquaternions primitifs par l'égalité

$$r(n)=\sum t\left(\frac{n}{\delta^2}\right),$$

somme étendue à tous les carrés δ^2 diviseurs de n. Ce nombre est, comme $t(n)$, une fonction factorable (n° 27, corollaire 2°). Si n impair est exactement divisible par p^α (p premier), le facteur correspondant de $t(n)$ vaut $p^{3\alpha}+p^{3(\alpha-1)}$; celui de $r(n)$ vaut donc

$$p^{3\alpha}+p^{3(\alpha-1)}+p^{3(\alpha-2)}\ldots+p^3+1,$$

qui est aussi la somme des cubes des diviseurs de p^α. Par multiplication on obtient le nombre $r(n)$, ce qui démontre le second théorème de Jacobi [3] :

Le nombre des biquaternions de norme impaire n vaut seize fois la somme des cubes des diviseurs de n.

3° Le diviseur premier $p = 2$ exige une étude spéciale; la structure des biquaternions y intervient comme au n° 25.

Rappelons d'abord qu'il y a 16.7 biquaternions de norme 2.

Cherchons le nombre $t(n)$ des biquaternions primitifs de norme $n = 2n_1$ à partir de $t(n_1)$. Les lettres P, P′, P_1 désignent ci-après des biquaternions de norme 2.

Si n est double de nombre impair, $N = PN_1$ donne aussitôt

$$t(n) = \frac{r(2)}{16} t(n_1) = 7\, t(n_1).$$

Si n est quadruple de nombre impair, chaque biquaternion N_1 de norme n_1 est divisible à gauche par 16 biquaternions P_1. Le produit PN_1 est primitif si P n'est égal à aucun des seize $\overline{P_1}$. Inversement tout biquaternion N primitif et décomposable provient ainsi de 16.3 biquaternions N_1. Le nombre des biquaternions primitifs N admettant un diviseur de norme 2 est donc

$$\frac{r(2) - 16}{3.16} t(n_1) = 2\, t(n_1).$$

Le nombre des biquaternions indécomposables est quadruple, c'est-à-dire vaut $8\, t(n_1)$. En effet, dans un biquaternion N ayant quatre composantes paires et quatre impaires, permutons les composantes inégales de toutes les manières possibles. Puis fixons arbitrairement le rang des composantes paires. A ce choix correspond un certain nombre de permutations (égal au nombre de permutations des composantes paires multiplié par celui des composantes impaires). A tout autre choix correspond un nombre égal de permutations. Or il y a 70 manières de choisir la parité des composantes : 14 manières conduisent à des biquaternions décomposables, 56 à des biquaternions indécomposables.

Supposons enfin n multiple de 8 et considérons tous les produits PN_1 primitifs. Désignons par $u(n)$ le nombre des biquaternions primitifs de norme n ayant quatre composantes impaires et admettant un diviseur de norme 2, par $v(n)$ le nombre des biquaternions primitifs à composantes toutes impaires :

$$t(n) = 5\, u(n) + v(n).$$

Tout biquaternion N_1 primitif de norme n_1, ayant quatre composantes impaires et admettant un diviseur de norme 2, est divisible à gauche par 16.3 biquaternions P_1 ; il donne 16.4 produits primitifs PN_1, le biquaternion P devant être distinct de $\overline{P_1}$. Tout biquaternion N_1 primitif, sans diviseur de norme 2, multiplié par un biquaternion P quelconque, engendre 16.7 produits primitifs.

Enfin tout biquaternion N_1 à composantes impaires donne un produit divisible par 2. Inversement, tout biquaternion de norme n ayant quatre composantes impaires et admettant un diviseur de norme 2 se décompose en produit PN_1 de 16.3 manières; tout biquaternion de norme n à composantes impaires se décompose en produit de 16.7 manières. Il en résulte l'égalité

$$16.4u(n_1)+16.7.4u(n_1)=16.3u(n)+16.7\varphi(n).$$

En particulier tout biquaternion de norme n à composantes impaires se décompose en un produit $P'N'_1$, où P' a ses deux premières composantes unitaires et les six autres nulles. Alors N'_1 doit avoir ses deux premières composantes de parités contraires, ainsi que les suivantes deux à deux; ce qui correspond à 16 manières de choisir la parité des composantes, sur un total de 70 manières. Le nombre des biquaternions N'_1, égal à $\varphi(n)$, vaut donc

$$\varphi(n)=5u(n_1).\frac{16}{70}.$$

Nous obtenons ainsi

$$u(n)=8u(n_1)=7\varphi(n), \qquad t(n)=36\varphi(n).$$

D'où l'énoncé :

Le nombre des biquaternions primitifs de norme n est égal à

$$t(n)=16hn^3\prod\left(1+\frac{1}{p^3}\right),$$

produit étendu à tous les diviseurs premiers de n, *le coefficient* h *valant* $\frac{7}{9}$ *pour* n *double de nombre impair, valant* $\frac{35}{36}$ *pour* n *quadruple de nombre impair, valant* 1 *dans tout autre cas.*

Si n *est multiple de* 4, *le nombre des biquaternions primitifs ayant seulement quatre composantes impaires vaut*

$$\frac{140}{9}n^3\prod\left(1+\frac{1}{p^3}\right).$$

Si n *est multiple de* 8, *le nombre des biquaternions primitifs à composantes toutes impaires vaut*

$$\frac{4}{9}n^3\prod\left(1+\frac{1}{p^3}\right).$$

4° Comme au 2°, dénombrons les biquaternions de norme n, primitifs ou non, en considérant les diviseurs de la forme $\frac{n}{\delta^2}$. D'une part, n supposé exactement divisible par 2^α, le facteur correspondant de $r(n)$ est, selon la parité de α,

$$8^\alpha+8^{\alpha-1}+\ldots+8^3+70+1 \qquad \text{ou} \qquad 8^\alpha+8^{\alpha-1}+\ldots+8^3+8^2+7,$$

c'est-à-dire dans les deux cas

$$8^x + 8^{x-1} + \ldots + 8^3 + 8^2 + 8 - 1.$$

D'autre part, le nombre des biquaternions à composantes impaires vaut la somme des cubes des diviseurs impairs de n multipliée par

$$\frac{4}{9} \cdot 8^x \cdot \left(1 + \frac{1}{8}\right) = \frac{8^x}{2},$$

il est donc égal à la demi-somme des cubes des diviseurs de n dont les diviseurs conjugués sont impairs.

D'où la conclusion :

Le nombre des biquaternions de norme n vaut 16 *fois l'excès de la somme des cubes des diviseurs pairs de n sur la somme des cubes des diviseurs impairs.*

La norme n supposée multiple de 4, *le nombre des biquaternions ayant seulement quatre composantes impaires est égal à* $\frac{35}{2}$ *fois la somme des cubes des diviseurs de n dont les conjugués sont impairs.*

La norme n supposée multiple de 8, *le nombre des biquaternions à composantes toutes impaires est égal à la demi-somme des cubes des diviseurs de n dont les conjugués sont impairs.*

32. *Note sur les biquaternions à composantes positives distinctes.* — Le calcul donne les résultats suivants concernant les normes :

Tous les nombres entiers naturels, à l'exception de

1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 13, 15, 18, 21,

sont représentables par une somme de huit carrés positifs; ils correspondent, si l'on veut, à des biquaternions à composantes positives.

Tous les nombres entiers suffisamment grands sont représentables par une somme de huit carrés positifs distincts. Les nombres naturels qui ne peuvent être représentés de cette manière sont au nombre de 305, dont les plus grands sont 406, 418, 462.

Tous les nombres naturels sont des sommes de huit carrés premiers entre eux dans leur ensemble et correspondent ainsi à des biquaternions primitifs.

La suite des nombres représentables par une somme de huit carrés positifs distincts est identique à la suite des nombres représentables par une somme de huit carrés positifs distincts premiers entre eux dans leur ensemble. Tous les nombres naturels, excepté 305 nombres, peuvent être considérés comme des normes de biquaternions primitifs à composantes positives distinctes.