BULLETIN DE LA S. M. F.

GASTON BENNETON

Arithmétique des quaternions

Bulletin de la S. M. F., tome 71 (1943), p. 78-111

<http://www.numdam.org/item?id=BSMF_1943__71__78_0>

ARITHMÉTIQUE DES QUATERNIONS;

PAR M. GASTON BENNETON.

INTRODUCTION.

Dans un récent Mémoire, publié dans les *Annales scientifiques de l'École Normale supérieure*, nous avons construit une arithmétique des quaternions basée sur la théorie des facteurs premiers. La divisibilité étudiée, nous avons indiqué deux façons de décomposer les quaternions en facteurs : un premier procédé inspiré du raisonnement de Lagrange sur la représentation des entiers par une somme de carrés; un second procédé, d'ordre plus général, valable pour des facteurs non nécessairement premiers.

Ce travail apporte les compléments suivants :

Le Chapitre I étudie les diviseurs communs et le plus grand commun diviseur.

Le Chapitre II se rapporte à la décomposition des quaternions en facteurs quelconques non nécessairement premiers.

Le Chapitre III établit une transition avec l'arithmétique de Hurwitz, dont la définition du quaternion entier est différente.

Le Chapitre IV fait l'application des quaternions aux matrices orthogonales d'ordre 4 à termes entiers et donne la solution d'un problème dû à Euler.

Nous prions le lecteur de se reporter aux *Annales* pour la démonstration des résultats de base et pour les références bibliographiques. Nous allons toutefois rappeler les définitions utiles et quelques propriétés.

CHAPITRE I.

Quaternions entiers. Diviseurs communs et P. G. C. D.

1. Définitions et premières propriétés. — 1° Nous appelons quaternion *entier* tout quaternion dont les composantes sont des nombres entiers.

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*.

Un quaternion est *premier* si sa norme est un nombre premier. La norme, somme des carrés des composantes, est aussi le produit du quaternion par son conjugué

$$A = x_0 + x_1 i + x_2 j + x_3 k, \qquad N(A) = A\overline{A} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

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

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

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

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.

Tout quaternion A admet comme diviseurs particuliers à gauche les huit unités J et les huit associés à gauche AJ; comme diviseurs à droite, les unités J et les associés à droite JA.

Un *facteur* est un quaternion défini au produit près par des unités à droite ou à gauche : le facteur $\mathfrak{A}$ est l'ensemble des quaternions associés JAJ′ (en général 32).

2° Tout quaternion primitif A dont la norme est multiple d'un nombre premier p impair a un diviseur à gauche P de norme p défini au produit près à droite par une unité.

Ce diviseur premier P s'obtient de deux manières. Un premier procédé permet de calculer, par divisions successives, une suite de quaternions A, A_1, ..., A_h de normes décroissantes pq, pq_1, ..., pq_h, admettant à gauche les mêmes diviseurs de norme p. Le dernier terme A_h est le diviseur cherché P.

Un *second procédé de décomposition* consiste à écrire une suite de quaternions A, R_1, R_2, ..., R_h de normes décroissantes pq, qq_1, q_1q_2, ..., $q_{h-1}q_h$, deux termes consécutifs R_i et R_{i+1} ayant les mêmes diviseurs à gauche de norme q_i. Le dernier quaternion R_h est l'une des huit unités J, ce qui détermine les diviseurs à gauche de proche en proche, notamment ceux de A. Ce deuxième procédé est d'une application plus étendue : il suppose seulement que p, q et le p. g. d. scalaire de 2A soient premiers entre eux dans leur ensemble.

3° *La norme d'un quaternion primitif* A *étant décomposée en facteurs premiers non nécessairement distincts rangés dans un certain ordre, le quaternion peut être décomposé en un produit de quaternions premiers correspondants*

$$N(A) = p_1p_2p_3\ldots. \qquad A = P_1P_2P_3\ldots.$$

La décomposition est unique, au produit près de chaque quaternion par une unité. Toutefois s'il y a deux normes égales à 2, pour la première d'entre elles le quaternion correspondant peut être remplacé indifféremment par un quaternion quelconque de norme 2.

Ce théorème permet de retrouver l'énoncé de Jacobi sur la représentation des nombres par une somme de quatre carrés. Nous désignerons par $r(n)$ le nombre des quaternions entiers de norme n et par $t(n)$ le nombre des quaternions primitifs de même norme.

2. Existence des diviseurs communs. — Le quaternion M est un diviseur commun à gauche de A et B s'il vérifie les égalités

$$A = MA_1, \qquad B = MB_1.$$

La norme de M divise à la fois les normes de A et de B; elle divise aussi le produit $\overline{A}B$. Nous allons établir que ces conditions caractérisent la norme des diviseurs communs.

1° Examinons d'abord le cas des diviseurs premiers communs, et montrons que la condition

$$N(A) \equiv N(B) \equiv \overline{A}B \equiv 0 \pmod{p}$$

entraîne que A et B ont au moins un diviseur commun à gauche de norme p, nombre premier.

Si l'un des quaternions est divisible par p, il admet comme diviseurs tous les quaternions de norme p, notamment les diviseurs de l'autre quaternion. De même si p vaut 2 et que les composantes soient toutes impaires.

Supposons maintenant que chaque quaternion admette à gauche un facteur unique de norme p

$$A = PA_1, \qquad B = P'B_1.$$

Les restes suivant le module p s'écrivent PA_0 et $P'B_0$, où les normes de A_0 et B_0, inférieures à p et non nulles, sont premières avec p. Il en résulte

$$\overline{A}B \equiv \overline{A}_0\overline{P}P'B_0 \equiv 0, \qquad \overline{P}P' \equiv 0 \pmod{p}.$$

Les quaternions P et P′ sont associés à gauche; ils divisent à gauche à la fois A et B.

2° Supposons m entier quelconque et

$$N(A) \equiv N(B) \equiv \overline{A}B \equiv 0 \pmod{m}.$$

Décomposons m en facteurs premiers $p_1p_2p_3\ldots$. Les nombres divisibles par m le sont par le nombre premier p_1. Il en résulte

$$A = P_1Q_1, \qquad B = P_1R_1, \qquad N(P_1) = p_1,$$
$$N(Q_1) \equiv N(R_1) \equiv \overline{Q}_1R_1 \equiv 0 \pmod{p_2p_3\ldots}.$$

A leur tour Q_1 et R_1 ont un diviseur commun à gauche de norme p_2, et ainsi de suite jusqu'à l'épuisement des facteurs premiers de m. Nous obtenons

$$A = MA_1, \qquad B = MB_1, \qquad M = P_1P_2P_3\ldots.$$

L'étude des diviseurs à droite se ferait de la même manière; d'ailleurs si un quaternion est diviseur à gauche de A et B, son conjugué est diviseur à droite de $\overline{A}$ et $\overline{B}$. D'où l'énoncé :

THÉORÈME. — *Pour que* A *et* B *aient au moins un diviseur commun à gauche de norme m, il faut et il suffit que m divise à la fois* N(A), N(B) *et* $\overline{A}B$.

Pour que A *et* B *aient un même diviseur à droite, il faut et il suffit que m divise à la fois* N(A), N(B) *et* $A\overline{B}$.

3. **Étude du p. g. c. d.** — Nous appelons *p. g. c. d. à gauche de* A *et* B *tout diviseur* D *commun à gauche dont la norme d est le plus grand nombre scalaire divisant à la fois* N(A), N(B) *et* $\overline{A}B$.

$$A = DA_0, \qquad B = DB_0, \qquad \overline{A}B = lC,$$

l désignant le p. g. d. scalaire de $\overline{A}B$.

Les normes de A_0 et B_0 et le p. g. d. scalaire de $\overline{A_0}B_0$ sont premiers entre eux dans leur ensemble : tout scalaire premier diviseur de $\overline{A_0}B_0$ divise une seule des deux normes de A_0 ou B_0, et, par suite, divise l'un des quaternions A_0 ou B_0. Le p. g. d. scalaire est donc le produit de deux entiers $\alpha\beta$ divisant respectivement A_0 et B_0

$$A_0 = \alpha U, \qquad B_0 = \beta V, \qquad C = \overline{U}V.$$

Notons que $d\alpha$ et $d\beta$ sont respectivement égaux aux p. g. c. d. de N(A), l et de N(B), l.

Le problème se ramène à la décomposition du quaternion primitif C en produit de deux facteurs $\overline{U}V$ de normes connues. Nous décomposons ces dernières en facteurs premiers et nous considérons leur produit comme une décomposition de la norme de C.

Si la norme de C n'est pas multiple de 4, la décomposition en quaternions premiers est unique, donc aussi la décomposition de C en produit $\overline{U}V$. Le quaternion A_0 et, par suite, D sont déterminés au produit près par une unité.

Si la norme de C est multiple de 4, nous décomposons C en plaçant consécutivement les deux facteurs P, P′ de norme 2. Si le produit PP′ est tout entier dans $\overline{U}$ ou dans V, la décomposition de C en produit $\overline{U}V$ est unique; il n'existe qu'un seul D. Si P figure dans $\overline{U}$ et P′ dans V, il y a trois décompositions et, par

suite, lorsque d est pair, trois quaternions D ne différant entre eux que par un facteur de norme 2

$$D = D_0 P, \qquad N(P) = 2.$$

Ce dernier cas se présente si, d étant pair, N(U) et N(V) sont doubles de nombres impairs, c'est-à-dire si N(A), N(B) et $2l$ sont multiples d'une même puissance de 2 au moins égale à 2^2.

L'étude de la divisibilité à droite est identique.

Le cas du triple p. g. c. d. a lieu simultanément à droite et à gauche, car, en supposant N(A), N(B) et $2\overline{A}B$ divisibles par la même puissance de 2, on peut montrer qu'il en est de même de $2A\overline{B}$.

Résumons les résultats.

Le p. g. c. d. à gauche de A *et* B *est unique*, au remplacement près par ses associés à gauche. *Toutefois*, si N(A), N(B) et $2\overline{A}B$ sont multiples d'une même puissance de 2 au moins égale à 2^2, il existe trois p. g. c. d. non associés ne différant entre eux que par un facteur de norme 2.

Le cas particulier du triple p. g. c. d. a lieu simultanément à droite et à gauche.

Remarque. — Le calcul peut se faire indépendamment de la décomposition en facteurs premiers. En effet, le p. g. c. d. des trois nombres

$$N(A_0), \qquad N(B_0), \qquad \frac{2l}{d}$$

égale 1 ou 2. S'il vaut 1, le deuxième procédé de décomposition (§ 1) est directement applicable pour $\overline{A}_0$ diviseur à gauche de $\frac{\overline{A}B}{d}$, de norme égale à $\frac{N(A)}{d}$. S'il vaut 2, nous posons $\overline{A}_0 = \overline{A}_1 P$, où P a pour norme 2. Le diviseur à gauche $\overline{A}_1$ est calculable par le même procédé.

4. Propriétés du p. g. c. d. — 1° Théorème. — *Tout diviseur commun à gauche de* A *et* B *est un diviseur du p. g. c. d. à gauche, ou de l'un des trois p. g. c. d. à gauche.*

Considérons en effet un diviseur commun M de norme m; celle-ci divise nécessairement la norme du p. g. c. d.

$$A = MA_1, \qquad B = MB_1, \qquad d = mm_1.$$

Il s'ensuit

$$N(A_1) \equiv N(B_1) \equiv \overline{A}_1 B_1 \equiv 0 \pmod{m_1}.$$

A_1 et B_1 sont donc divisibles à gauche par un même quaternion M_1 de norme m_1. Le produit MM_1 divise à la fois A et B et n'est autre que l'un des p. g. c. d. à gauche.

Ainsi pour trouver tous les diviseurs communs à gauche de norme m, il suffit de chercher tous les quaternions de norme m diviseurs à gauche du p. g. c. d. à gauche.

2° Soit D l'un des p. g. c. d. à gauche de A et B,

$$A = DA_0, \qquad B = DB_0.$$

Les trois nombres suivants : norme de A_0, norme de B_0, p. g. d. scalaire de $2\overline{A}_0 B_0$, ont un p. g. c. d. égal à 1 ou à 2. Il existe donc des entiers x, y et un quaternion entier Z tels que

$$x\,N(A_0) + y\,N(B_0) + \text{partie scalaire } (2\overline{A}_0 B_0 Z) = 1 \text{ ou } 2,$$

c'est-à-dire

$$A_0(x\overline{A}_0 + \overline{Z}\overline{B}_0) + B_0(y\overline{B}_0 + B_0 Z) = 1 \text{ ou } 2.$$

Désignons les parenthèses par X_0 et Y_0 et multiplions à gauche par D. Nous voyons que *le p. g. c. d. à gauche ou son double est de la forme*

$$D \text{ ou } 2D = AX_0 + BY_0.$$

On peut encore dire : *suivant le cas, la somme d'idéaux*

$$AX + BY \qquad (X, Y \text{ quelconques})$$

est égale à l'idéal principal DX, est un diviseur de l'idéal 2DX, ou (dans le cas du triple p. g. c. d.) est un diviseur commun aux trois idéaux 2DX, 2D'X, 2D''X.

5. Quaternions premiers entre eux. — Deux quaternions A et B sont dits *premiers entre eux* s'ils n'ont aucun diviseur commun

ni à droite ni à gauche. Il existe alors des quaternions entiers X, Y, X′, Y′ tels que

$$AX + BY = X'A + Y'B = 1 \text{ ou } 2.$$

Nous allons établir la propriété de condition suivante :

THÉORÈME. — *Pour que* A *et* B *soient premiers entre eux, c'est-à-dire n'aient aucun diviseur commun ni à droite ni à gauche, il faut et il suffit que les normes de* A *et* B *et la partie scalaire de* $A\overline{B}$ *soient premières entre elles dans leur ensemble. Il suffit que les normes de* A, B *et* A + B *soient premières entre elles dans leur ensemble.*

COROLLAIRE. — Deux quaternions *orthogonaux*, c'est-à-dire tels que le produit de l'un par le conjugué de l'autre ait une partie scalaire nulle, ne sont premiers entre eux que si leurs normes sont premières entre elles.

Nous posons

$$A\overline{B} = x_0 + x_1 i + x_2 j + x_3 k, \qquad \overline{A}B = x_0 + x'_1 i + x'_2 j + x'_3 k,$$
$$N(A) \equiv N(B) \equiv x_0 \equiv 0 \qquad (\text{mod } p \text{ premier}).$$

On voit aisément que les trois produits $x_1 x'_1$, $x_2 x'_2$, $x_3 x'_3$ sont des combinaisons linéaires de N(A), N(B), x_0 à coefficients entiers; ces produits sont donc divisibles par p. L'un au moins des quaternions $A\overline{B}$, $\overline{A}B$ possède alors trois composantes divisibles par p; la norme étant aussi divisible, il en est de même de la quatrième composante

$$A\overline{B} \quad \text{ou} \quad \overline{A}B \equiv 0 \qquad (\text{mod } p).$$

Or cette condition exprime que A et B ont un diviseur commun de norme p, à droite ou à gauche. Si les quaternions sont premiers entre eux, p vaut nécessairement 1 : les trois nombres N(A), N(B), x_0 sont premiers entre eux dans leur ensemble. Et réciproquement.

Il suffit aussi bien que les normes de A, B, et A + B soient premières entre elles dans leur ensemble, car

$$N(A + B) = N(A) + N(B) + 2x_0.$$

Si A et B sont premiers entre eux et si leurs normes sont paires (doubles de nombres impairs), le p. g. c. d. des trois normes vaut 2.

6. **P. G. C. D. mixtes.** — Deux quaternions quelconques A et B peuvent être mis sous la forme

$$A = UA_1V, \qquad B = UB_1V,$$

où A_1 et B_1 sont premiers entre eux. *Pour les différentes solutions possibles les normes de* A_1 *et de* B_1 *restent les mêmes : le produit des normes* $N(U)N(V)$ *est égal au p. g. c. d. de*

$$N(A), \qquad N(B), \qquad \text{partie scalaire } (A\overline{B}).$$

Nous dirons que *le couple* U, V *est un p. g. c. d. mixte de* A *et* B, *dont la norme vaut* $N(U)N(V)$.

En effet les nombres

$$N(A_1), \qquad N(B_1), \qquad \text{partie scalaire } (A_1\overline{B}_1)$$

sont premiers entre eux dans leur ensemble. Le produit $N(U)N(V)$ est donc le plus grand nombre divisant à la fois

$$N(UA_1V), \qquad N(UB_1V), \qquad \text{partie scalaire } (A\overline{B}),$$

et dépend seulement de A et B. Il en est de même des normes de A_1 et de B_1.

En particulier on peut prendre pour V le p. g. c. d. à droite de A et B, soit V_0. Le premier facteur U_0 possède alors la norme minimum : c'est un diviseur à gauche de tous les quaternions possibles U. Pareillement on peut prendre pour U le p. g. c. d. à gauche de A et B.

7. **Cas d'un nombre quelconque de quaternions.** — Les résultats précédents s'étendent immédiatement au cas général.

1° Pour que n quaternions A, B, C, ... aient au moins un diviseur commun à gauche de norme m, il faut et il suffit que m divise à la fois les normes de A, B, C, ... et les $\frac{n(n-1)}{2}$ quaternions $\overline{A}B$, $\overline{A}C$, $\overline{B}C$, ...

D'ailleurs si A est primitif, il suffit que m divise les n normes et les $n-1$ quaternions $\overline{A}B$, $\overline{A}C$, ...

2° Pour que A, B, C, ... aient au moins un diviseur commun (à droite ou à gauche) de norme p nombre premier, il faut et il suffit que p divise les normes de A, B, C, ... et les parties scalaires de $A\overline{B}$, $A\overline{C}$, $B\overline{C}$, ..., soit au total $\frac{n(n+1)}{2}$ nombres.

3° Pour que A, B, C, ... aient au moins un diviseur commun de norme p premier impair, il faut et il suffit que les normes des $\frac{n(n+1)}{2}$ quaternions A, B, C, ..., $A+B$, $A+C$, ... soient divisibles par p.

4° Pour que A, B, C, ... soient premiers entre eux dans leur ensemble, il faut et il suffit que les normes de A, B, C, ... et les parties scalaires de $A\overline{B}$, $A\overline{C}$, $B\overline{C}$, ... soient premières entre elles dans leur ensemble. Il suffit que les normes de A, B, C, ..., $A+B$, $A+C$, ... soient premières entre elles dans leur ensemble.

CHAPITRE II.

Décomposition des quaternions en facteurs non premiers.

8. Décomposition en deux facteurs. — Considérons un quaternion N dont la norme est égale au produit ab. Cherchons à le décomposer en produit de deux quaternions de normes respectives a, b

$$N = AB, \qquad \text{norme}(N) = ab.$$

Soit l le p. g. d. scalaire de N. En appelant D le p. g. c. d. à droite de A et $\overline{B}$, nous pouvons écrire, comme au paragraphe 3,

$$A = A_0 D, \quad B = \overline{D} B_0, \quad N = lC,$$
$$A_0 = \alpha U, \quad B_0 = \beta V, \quad C = UV.$$

Le calcul revient à la décomposition du quaternion primitif C en produit de deux facteurs UV de normes connues.

Si une au moins des normes de U ou V est impaire, la décomposition de C en produit UV est unique, à un facteur unité près

qui peut être incorporé à D. La solution s'écrit

$$A = A_0 D, \qquad B = \overline{D} B_0, \qquad \frac{N}{d} = A_0 B_0,$$

où $A_0 B_0$ est une décomposition particulière calculable par le second procédé du paragraphe 1, où D est un quaternion quelconque de norme d, p. g. c. d. de a, b, l. Il y a donc $r(d)$ décompositions de N.

Si les normes de U et V sont paires, c'est que a, b, $2l$ sont divisibles par la même puissance de 2. Détruisons cette symétrie en posant

$$2N = A(2B), \qquad \text{p. g. c. d. } (a, b, 2l) = 2d,$$

$$A = A_1 \Delta, \qquad 2B = \overline{\Delta} B_1, \qquad \frac{N}{d} = A_1 B_1,$$

où Δ désigne un quaternion quelconque de norme $2d$, et $A_1 B_1$ une décomposition particulière calculable par le second procédé. D'ailleurs si d est pair, les nombres $r(d)$ et $r(2d)$ sont égaux et les quaternions $A_1 \Delta$ sont à l'ordre près identiques aux quaternions $A_0 D$. Le seul cas distinct est donc celui de N non divisible par 2, a et b multiples impairs de 2.

Réunissons les conclusions dans un même énoncé.

Théorème. — *Soit un quaternion* N *de norme* ab *et de p. g. d. scalaire* l. *Le nombre des décompositions de* N *en produit de deux facteurs de normes respectives* a, b *est égal au nombre des quaternions de norme le p. g. c. d. de* a, b, $2l$:

$$\omega_2 = r(\delta), \qquad \delta = \text{p. g. c. d. } (a, b, 2l).$$

Tous les diviseurs de N, *à gauche, de norme* a *sont de la forme* $A = A_1 \Delta$, où A_1 est un quaternion particulier, et Δ un quaternion quelconque de norme δ.

Corollaire. — 1° Le moindre nombre de décompositions a lieu si a, b, $2l$ sont premiers entre eux dans leur ensemble. La décomposition du facteur $\mathfrak{N}$ en produit $\mathfrak{A}\mathfrak{B}$ est alors unique.

2° Pour que le quaternion N soit divisible par tous les quaternions de norme a, il faut et il suffit que les composantes de N soient multiples de a ou (a étant pair) soient des multiples impairs de $\frac{a}{2}$.

9. **Application.** — Partons encore de l'égalité

$$N = AB,$$

et utilisons de deux manières les résultats précédents en considérant, d'une part, tous les quaternions possibles N de norme donnée ab et, d'autre part, tous les diviseurs de N à gauche de norme indéterminée a.

1° *Multiplication de la fonction* $r(n)$. — Multiplions successivement tous les quaternions de norme a par les divers quaternions de norme b. Nous obtenons tous les quaternions de norme ab, où chacun d'eux N est répété $r(\delta)$ fois :

$$\delta = \text{p. g. c. d. } (a, b, 2l), \qquad l = \text{p. g. d. scalaire N.}$$

Il en résulte la formule, avec les notations du paragraphe 1,

$$r(a)\,r(b) = \sum r(\delta)\,t\left(\frac{ab}{l^2}\right),$$

somme étendue à tous les nombres l dont le carré divise ab.

Si a et b sont premiers entre eux, nous retrouvons $r(ab)$.

Si nous égalons a et b, nous obtenons

$$r^2(a) = \Sigma r(d) r(d'^2) \qquad (a \text{ impair}),$$
$$r^2(a) = \Sigma r(2d) r(d'^2) \qquad (a \text{ pair}),$$

d et d' désignant deux diviseurs conjugués quelconques de a.

Bien entendu ces égalités se retrouvent, ou plutôt se vérifient, à partir de l'expression connue de $r(n)$.

Pour que l'identité de Lagrange donne sans répétition les quaternions de norme ab à partir des quaternions non associés de norme a et des quaternions de norme b, il faut et il suffit que a et b soit premiers entre eux. En effet δ doit valoir l'unité pour chaque produit.

2° *Nombre total des diviseurs à gauche d'un quaternion.* — Soit n la norme de N. Le nombre total des diviseurs de N à gauche (ou à droite) est

$$\Sigma r(\delta),$$

somme étendue à tous les diviseurs conjugués a, b de n.

Pour chaque facteur premier de la norme n, appelons p^α la plus haute puissance divisant n, et p^β la plus haute puissance divisant le quaternion N. Le nombre cherché est une fonction factorable qui vaut, tous calculs faits,

$$8h\Pi(p-1)^{-2}[(\alpha-2\beta+1)p^{\beta+2}-(\alpha-2\beta-1)p^{\beta+1}-(\alpha+3)p+\alpha+1],$$

produit étendu à tous les diviseurs premiers impairs de n, le coefficient h valant 1 ou $3\alpha_0-1$ suivant que n est impair ou est multiple de 2^{α_0}.

Ce nombre est une fonction croissante de p, α, β. Pour une norme donnée, les quaternions dont le diviseur scalaire est minimum, en l'espèce les quaternions primitifs, possèdent la *moindre divisibilité* dans toute l'acception du terme.

10. **Décomposition en deux facteurs primitifs.** — Soit un quaternion N de norme ab et de p. g. d. scalaire l. Cherchons à le décomposer en un produit de deux quaternions primitifs de normes respectives a et b

$$N = AB \qquad (A \text{ et } B \text{ primitifs}).$$

Mettons en évidence le p. g. c. d. à droite de A et $\overline{B}$

$$A = A_0D, \qquad \overline{B} = B_0D.$$

Tout diviseur scalaire de $A_0\overline{B}_0$ divise une seule norme de A_0 ou B_0 à l'exclusion de l'autre, divise par suite le quaternion primitif A_0 ou B_0 et ne peut être que 1. Le produit $A_0\overline{B_0}$ est donc primitif. La question se ramène à celle-ci :

Étant donnés deux quaternions A_0 *et* B_0 (*de normes* a_0, b_0) *correspondant à un produit* $A_0\overline{B}_0$ *primitif, trouver tous les quaternions* D *de norme donnée d qui rendent* A_0D *et* B_0D *simultanément primitifs.*

Les quaternions D peuvent être obtenus à partir de leur décomposition en facteurs premiers, par une méthode semblable à celle qui donne le nombre des quaternions primitifs de norme n. Le nombre des quaternions D ne dépend que des

normes a_0, b_0, d; il vaut

$$\theta(a_0, b_0, d) = 8hd\Pi\left(1+\frac{1}{p}\right)\left(1-\frac{1}{q}\right),$$

produit étendu à tous les nombres premiers p qui divisent d sans diviser $a_0 b_0$ et à tous les diviseurs premiers q communs à a_0, b_0, d. Le coefficient h est nul si $a_0 d$ ou $b_0 d$ sont multiples de 8, il vaut $\frac{1}{3}$ si d est multiple de 4 et $a_0 b_0$ impair, il vaut 1 dans tout autre cas.

Ceci posé nous revenons à A et B. Le produit $A_0\bar{B}_0$ étant primitif, la norme de D est égale à l. Le nombre des solutions est donné par la formule précédente en θ. Toutefois si a, b, $2l$ sont doubles de nombres impairs (§ 8), la décomposition utilise trois quaternions A_0 non associés et θ doit être triplé.

Par conséquent pour que N soit décomposable en produit de quaternions primitifs de normes a, b, *il faut que ces normes soient divisibles par l et qu'aucune d'elles ne soit multiple de* 8. Le nombre des décompositions vaut alors

$$\theta\left(\frac{a}{l}, \frac{b}{l}, l\right),$$

nombre qui doit être triplé lorsque a, b et $2l$ sont doubles de nombres impairs simultanément.

11. Décomposition en deux facteurs de p. g. d. scalaires donnés. — Soit un quaternion N ayant pour norme ab et pour p. g. d. scalaire l. Cherchons à le décomposer en deux facteurs de normes a et b, de p. g. d. scalaires λ et μ, respectivement.

$$N = \lambda\mu N_0 = \lambda A_0 \mu B_0.$$

Posons

$$a = 4^k a', \qquad b = 4^{k'} b' \qquad (a', b' \not\equiv 0 \bmod 8).$$

Les nombres λ et μ doivent être multiples de 2^k et $2^{k'}$, et l de la forme $2^{k+k'} l'$. Le même problème se pose alors pour un quaternion de norme $a'b'$ et de p. g. d. scalaire l'.

Considérons les p. g. c. d. scalaires

$$d = (a', b', l'), \qquad (a', l') = d\alpha, \qquad (b', l') = d\beta.$$

Les nombres λ, μ et d sont nécessairement de la forme

$$\lambda = 2^k \alpha cf, \qquad \mu = 2^{k'} \beta cg, \qquad d = c^2 fgh,$$

où f et g sont premiers entre eux et vérifient

$$a' = d\alpha^2 ff', \qquad b' = d\beta^2 gg'.$$

Le quaternion N_0, de p. g. d. scalaire h, est décomposable en produit de quaternions primitifs de normes respectives $fg'h$ et $f'gh$.

Le nombre des décompositions de N en produit de quaternions exactement divisibles par λ et μ est donc

$$\theta(fg', f'g, h),$$

nombre qui doit être triplé si fg', $f'g$ et $2h$ sont doubles de nombres impairs.

Le cas de la moindre divisibilité des facteurs λA_0 et μB_0 correspond à

$$\lambda = 2^k \alpha, \qquad \mu = 2^{k'} \beta;$$

le nombre des décompositions se réduit alors à $\theta(f', g', d)$ ou à son triple.

Les diviseurs scalaires λ et μ ont une seule valeur possible lorsque le p. g. c. d. de a', b', l' est un produit de nombres premiers dont aucun ne divise le quotient de ab par l^2.

12. Décomposition en h facteurs de normes données. — Appelons N un quaternion de p. g. d. scalaire l et de norme

$$n = a_1 a_2 \dots a_h \qquad (h \geq 3).$$

On peut le décomposer en deux facteurs de p. g. d. scalaires λ et μ, le second facteur ayant pour norme a_h

$$N = BA_h, \qquad N(B) = a_1 a_2 \dots a_{h-1}, \qquad N(A_h) = a_h.$$

Le nombre des décompositions de N en produit BA_h est une fonction factorable dépendant uniquement des normes et des p. g. d. scalaires,

$$\theta(a_1 a_2 \dots a_{h-1}, a_h, l, \lambda, \mu).$$

Le problème revient alors à décomposer le quaternion B de p. g. d. scalaire λ en produit de $h-1$ facteurs.

Nous allons montrer que *le nombre ω_h des décompositions de* N *en h facteurs est une fonction factorable de* $a_1, a_2, \ldots, a_h, l$, *symétrique en* $a_1, a_2, \ldots, a_h$.

Raisonnons par récurrence, en admettant la propriété pour la décomposition de B en $h-1$ facteurs. L'égalité qui donne ω_h est de la forme

$$\omega_h = \sum \omega_{h-1}(a_1, a_2, \ldots, a_{h-1}, \lambda)\,\theta(a_1 a_2 \ldots a_{h-1}, a_h, \lambda, \mu),$$

la somme s'étendant à toutes les valeurs possibles de λ et μ. Le nombre ω_h est une fonction factorable de $a_1, a_2, \ldots, a_h, l$, symétrique en $a_1, a_2, \ldots, a_{h-1}$. Il suffit de prouver la symétrie par rapport à a_{h-1}, a_h. Or si nous fixons les $h-2$ premiers facteurs, nous déterminons le produit des deux derniers, et le nombre des décompositions de ce produit en facteurs de normes a_{h-1}, a_h ne dépend pas de l'ordre des normes.

On montre aisément que le *minimum du nombre de décompositions* a lieu si

$$\frac{n}{a_1}, \frac{n}{a_2}, \ldots, \frac{n}{a_h}, 2l$$

sont premiers entre eux dans leur ensemble. Chaque facteur est alors déterminé à l'association près d'une unité. Les 8^{h-1} décompositions se déduisent d'une solution particulière par les égalités

$$A'_1 = A_1 J_1, \qquad A'_2 = \overline{J_1} A_2 J_2, \qquad \ldots \qquad A'_h = \overline{J}_{h-1} A_h,$$

où les J sont des unités quelconques. La décomposition en produit du facteur $\mathfrak{N}$ est alors unique

$$\mathfrak{N} = \mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_h.$$

Pour terminer indiquons la valeur exacte du nombre de décompositions dans le cas $h = 3$. Ce nombre, obtenu par un long calcul, est égal à

$$\omega_3 = 64\, h_0 \Pi (p-1)^{-2}[(\alpha - \beta + 1)p^{\beta+2} - (\alpha - \beta - 1)p^{\beta+1} - p^{\alpha'+1} - p^{\alpha''+1} - p^{\alpha'''+1} + 1],$$

produit étendu à tous les diviseurs premiers impairs p de n. Les nombres α, β, α', α'', α''' sont les exposants positifs ou nuls de p relatifs à la décomposition en facteurs premiers des p. g. c. d. suivants :

$$\frac{1}{7}(a_1, l)(a_2, l)(a_3, l), (a_2 a_3, a_3 a_1, a_1 a_2), (a_1, a_2 a_3, l), (a_2, a_3 a_1, l), (a_3, a_1 a_2, l);$$

le coefficient h_0 vaut 9, 3 ou 1 suivant qu'il y a trois, deux ou moins de deux nombres pairs parmi a_1, a_2, a_3.

13. **Note sur la représentation des quaternions par une somme de carrés.** — Le carré de tout quaternion entier ayant ses trois dernières composantes paires, il en est de même pour la somme de plusieurs carrés.

Tout quaternion N de norme impaire, dont les trois dernières composantes sont paires, est représentable par *une somme de deux carrés de quaternions entiers*

$$N \equiv 1 \pmod 2, \qquad N = U^2 + V^2.$$

En effet décomposons N en produit de deux facteurs AB. Ces facteurs sont congrus suivant le module 2 puisque

$$A \equiv \overline{A} \equiv \overline{A}N \equiv B \pmod 2.$$

Nous pouvons donc écrire ces égalités en U et V

$$U + iV = A, \qquad U - iV = B.$$

Le nombre des représentations de N par une somme de deux carrés est égal au nombre total des diviseurs à gauche de N (§ 9).

Tout quaternion N divisible par 2, dont la norme n'est pas un multiple impair de 8, est aussi représentable par une somme de deux carrés. Décomposons $\frac{N}{2}$ en produit de deux facteurs $A_1 B_1$,

$$N = A_1 P . \overline{P} B_1 \qquad \text{(norme de P = 2)}.$$

Les facteurs $A_1 P$ et $B_1 P$ sont congrus suivant le module 2 si $A_1 - B_1$ est divisible par P. Pour cela il faut et il suffit que les normes de A_1 et de B_1 soient de même parité et que P soit un

diviseur de $A_1 - B_1$. Les égalités

$$U + iV = A_1P_1 \qquad U - iV = \overline{P}B_1$$

sont alors possibles.

Remarquons que tout quaternion dont les trois dernières composantes sont paires est la somme de trois carrés de quaternions d'une infinité de manières.

14. Note sur les quaternions à composantes positives distinctes. — Voici des résultats numériques sur la représentation des entiers par une somme de quatre carrés scalaires, c'est-à-dire sur les normes de quaternions. Nous ne mentionnons pas les calculs qui ne procèdent pas directement de l'arithmétique des quaternions.

Tous les nombres naturels sont des sommes de quatre carrés (sont des normes de quaternions entiers).

Tous les nombres naturels non multiples de 8 sont des sommes de quatre carrés premiers entre eux dans leur ensemble (sont des normes de quaternions primitifs).

Tous les nombres naturels sont des sommes de quatre carrés positifs, excepté les douze nombres

$$1,\ 2,\ 3,\ 5,\ 6,\ 8,\ 9,\ 11,\ 14,\ 17,\ 29,\ 41$$

et les produits de 2, 6, 14 par une puissance de 2.

Sont représentables par une somme de quatre carrés positifs distincts (sont des normes de quaternions à composantes positives distinctes) :

les nombres impairs supérieurs à 157, plus exactement tous les nombres impairs positifs à l'exception de trente-neuf dont les plus grands sont 103, 115, 157;

les nombres divisibles par 2^h et supérieurs à $41 . 2^h$;

les nombres divisibles par 4^h et supérieurs à $103 . 4^h$.

Sont représentables par une somme de quatre carrés positifs distincts premiers entre eux dans leur ensemble tous les nombres naturels non multiples de 8 à l'exception de soixante-quatorze nombres dont les plus grands sont 292, 388, 412.

Toute somme de quatre carrés positifs distincts qui n'est pas multiple de 8 est représentable par une somme de quatre carrés

positifs distincts premiers entre eux dans leur ensemble, c'est-à-dire peut être considérée comme la norme d'un quaternion primitif à composantes positives distinctes.

CHAPITRE III.

Passage à l'arithmétique de Hurwitz.

15. **Introduction de nouvelles unités.** — 1° Nous savons le rôle particulier joué par le nombre 2 dans la décomposition en facteurs premiers et dans la théorie du p. g. c. d. Ainsi tout facteur primitif à composantes impaires admet comme diviseurs plusieurs facteurs de norme 2. Ainsi encore il y a un triple p. g. c. d. à A et B lorsque N(A), N(B) et $2\overline{A}B$ sont divisibles par la même puissance de 2.

Nous allons montrer qu'on peut obtenir une décomposition unique de tous les facteurs primitifs et un p. g. c. d. unique dans tous les cas, en complétant le système des quaternions entiers par l'adjonction de nouveaux termes, c'est-à-dire par une extension du domaine d'intégrité.

2° Nous voulons que le facteur primitif

$$\pm 1 \pm i \pm j \pm k$$

soit décomposable d'une seule manière en produit de facteurs de norme 2. Pour cela il est nécessaire que tous les quaternions de norme 2 forment un seul et unique facteur et se déduisent l'un de l'autre par multiplication par une *unité* ε, quaternion de norme 1. En admettant la règle habituelle de la multiplication résolvons donc

$$P' = P\varepsilon, \qquad 2\varepsilon = \overline{P}P',$$

où P et P′ sont des quaternions quelconques de norme 2. Le dernier produit représente un quaternion quelconque de norme 4. Si celui-ci est divisible par 2, ε est une unité ordinaire; sinon ε est une unité comprise dans la formule

$$\frac{1}{2}(\pm 1 \pm i \pm j \pm k).$$

Parmi ces seize nouvelles unités, celle qui correspond aux quatre signes + sera désignée par ρ.

Le système comprend alors 24 unités qui multipliées par 2 redonnent tous les quaternions entiers de norme 2. Ces unités sont des combinaisons linéaires à coefficients entiers rationnels de quatre d'entre elles convenablement choisies, par exemple i, j, k, ρ, qu'on peut appeler unités de base.

L'ensemble des 24 unités ε constitue le *facteur unité*.

16. **Quaternions entiers.** — Un quaternion entier, selon Hurwitz, est une combinaison linéaire des quatre unités de base i, j, k, ρ à coefficients entiers; les composantes (que nous continuons de rapporter au premier système d'unités 1, i, j, k) sont des entiers ou des moitiés de nombres impairs, simultanément. La norme est toujours un nombre entier.

Tout quaternion entier est le produit d'un quaternion entier ordinaire par une unité ε.

Considérons en effet un quaternion dont les composantes sont des moitiés de nombres impairs. Son double est un quaternion ordinaire A divisible (à droite ou à gauche) par un quaternion primitif de norme 4 valant lui-même 2ε. Le quaternion entier est donc de chacune des deux formes

$$A\varepsilon, \qquad \varepsilon' A.$$

Remarquons que si les composantes sont des moitiés de nombres impairs, la norme est impaire; si la norme est paire, les composantes sont entières.

Les produits du quaternion entier $A\varepsilon$, à droite et à gauche, par toutes les unités possibles, constituent le *facteur* $\varepsilon' A \varepsilon''$. Il contient entièrement le facteur $\mathfrak{A}$ associé au quaternion ordinaire A.

La somme, le produit de deux quaternions entiers sont encore des quaternions entiers : la somme est bien une combinaison linéaire de i, j, k, ρ, et le produit s'écrit

$$\varepsilon A . B \varepsilon' = \varepsilon (AB) \varepsilon'.$$

Un tel ensemble de quaternions contenant la somme et le produit de deux quelconques de ses termes constitue un *anneau*.

Note. — Il serait impossible de compléter cet anneau par de nouveaux termes, car l'ensemble obtenu par additions et multiplications mutuelles de tous les termes ne pourrait plus être engendré par la combinaison linéaire d'un nombre fini d'entre eux.

Ainsi le système de quaternions ayant pour base i, j, k, ρ correspond au *plus grand domaine d'intégrité* qui contienne les quaternions à composantes entières d'unités 1, i, j, k.

17. **Divisibilité. Diviseurs communs.** — Les propriétés de la divisibilité, des diviseurs communs, des p. g. c. d. s'étendent immédiatement aux nouveaux quaternions entiers. Les énoncés se simplifient en raison de l'unicité du facteur de norme 2.

Dans ce paragraphe, les majuscules désigneront des quaternions entiers quelconques, au nouveau sens du mot.

Voici les principaux résultats.

Si un quaternion donné A vérifie

$$A = mX,$$

nous disons que le nombre scalaire m divise A. Pour cela il faut et il suffit que les composantes de A soient multiples de m, ou soient multiples impairs de $\frac{m}{2}$. Si la seule valeur possible de m est l'unité, A est primitif. Par exemple, le quaternion $1+i+j+k$ est divisible par 2. Avec ces conventions le critère de divisibilité du paragraphe 1 reste valable.

La décomposition d'un facteur primitif en produit de facteurs premiers est unique, l'ordre des normes des facteurs premiers étant choisi d'avance.

Le nombre des quaternions de norme n vaut

$$r(n) \quad \text{ou} \quad 3r(n),$$

suivant que n est pair ou impair.

Le p. g. c. d. à gauche D *de deux quaternions* A *et* B *a pour norme le plus grand entier scalaire qui divise à la fois*

$$N(A),\ N(B),\ \overline{A}B.$$

D *est unique au remplacement près par ses associés à gauche. Tout diviseur commun à gauche de* A *et* B *est un diviseur à gauche de* D.

Le p. g. c. d. à gauche est de la forme

$$D = AX_0 + BY_0.$$

La somme d'idéaux $AX + BY$ est égale à l'idéal principal DX. (X, Y étant quelconques.)

Pour que deux quaternions soient premiers entre eux à droite et à gauche, il faut et il suffit qu'il existe des quaternions X, Y, X', Y' *tels que*

$$AX + BY = X'A + Y'B = 1.$$

Il faut et il suffit que les normes de A, B *et* $A + B$ *soient premières entre elles dans leur ensemble.*

Les énoncés précédents s'étendent à un nombre quelconque de quaternions.

CHAPITRE IV.

Sur les matrices orthogonales d'ordre 4.

18. Quaternions et matrices. — L'application des quaternions aux transformations de coordonnées est connue, et l'on peut même dire que c'est leur origine géométrique. Ces transformations à leur tour font intervenir le calcul des matrices. Il semble donc utile de représenter les quaternions par des matrices.

Désignons par I la matrice d'une colonne

$$I = \begin{vmatrix} 1 \\ i \\ j \\ k \end{vmatrix}$$

et considérons, pour tout quaternion A, ses deux tables de multiplication à gauche et à droite par I, que nous transformons

aussitôt en produit de matrices

$$AI = \left\| \begin{matrix} A \\ Ai \\ Aj \\ Ak \end{matrix} \right\| = A_g . I, \qquad IA = \left\| \begin{matrix} A \\ iA \\ jA \\ kA \end{matrix} \right\| = A_d . I.$$

A tout quaternion A on fait ainsi correspondre deux matrices carrées d'ordre 4, l'une à gauche et l'autre à droite, définies par les égalités précédentes. Elles s'écrivent comme suit :

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

$$A_g = \left\| \begin{matrix} x_0 & x_1 & x_2 & x_3 \\ -x_1 & x_0 & x_3 & -x_2 \\ -x_2 & -x_3 & x_0 & x_1 \\ -x_3 & x_2 & -x_1 & x_0 \end{matrix} \right\|, \qquad A_d = \left\| \begin{matrix} x_0 & x_1 & x_2 & x_3 \\ -x_1 & x_0 & -x_3 & x_2 \\ -x_2 & x_3 & x_0 & -x_1 \\ -x_3 & -x_2 & x_1 & x_0 \end{matrix} \right\|.$$

Ces expressions montrent qu'au quaternion conjugué $\overline{A}$ correspondent les matrices *conjuguées* $\overline{A}_g$ et $\overline{A}_d$, obtenues par l'échange des lignes et des colonnes. La surligne indique donc sans ambiguïté les quaternions conjugués et les matrices conjuguées.

A une somme de quaternions correspond la somme des matrices

$$(A + B)_g = A_g + B_g, \qquad (A + B)_d = A_d + B_d.$$

A un produit de quaternions correspond le produit des matrices

$$(AB)_g = A_g B_g, \qquad (AB)_d = A_d B_d.$$

En effet les égalités de définition de A_g ou B_d restent vraies si l'on remplace I par une colonne de quatre quaternions quelconques, par exemple par BI ou IB. Compte tenu de l'associativité, il en résulte la règle de multiplication.

En particulier la norme d'un quaternion A est représentée par une matrice scalaire dont tous les termes de la diagonale principale valent N(A), les autres termes étant nuls

$$A_g \overline{A}_g = A_d \overline{A}_d = \text{scalaire } N(A).$$

On retrouve ainsi la propriété multiplicative de la norme,

$$N(AB) = (AB)_d \left(\overline{AB}\right)_d = A_d B_d \overline{B}_d \overline{A}_d = N(A)\, N(B).$$

Considérons enfin la colonne AIB et écrivons-la des deux manières différentes

$$\begin{aligned} AIB &= (AI)B = A_g IB = A_g B_d I \\ &= A(IB) = AB_d I = B_d A_g I. \end{aligned}$$

Nous constatons que *le produit* $A_g B_d$ *est commutatif*

$$A_g B_d = B_d A_g.$$

Par conséquent, en associant les facteurs, on peut remplacer le produit d'un nombre quelconque de matrices de quaternions par une seule matrice, ou par le produit de deux matrices l'une à gauche, l'autre à droite. Ainsi

$$A_g B_d C_g D_d = (AC)_g (BD)_d.$$

Une égalité de produits telle que

$$A_g B_d = A'_g B'_d$$

exige *l'égalité des matrices* deux à deux, à un coefficient scalaire près. Il faut en effet

$$(\overline{A}A')_g = (B\overline{B}')_d = 1, \qquad A = A', \qquad B = B',$$

au produit près de chaque membre par un scalaire.

Remarque. — Dans les formules de définition, on peut substituer à I une colonne quelconque de quatre quaternions indépendants

$$\Sigma I \qquad (\text{déterminant } \Sigma \neq 0),$$

Σ désignant une matrice carrée d'ordre 4. La formule devient

$$A(\Sigma I) = \Sigma A_g I = (\Sigma A_g \Sigma^{-1})(\Sigma I).$$

Tout quaternion A peut donc être représenté par les matrices

$$\Sigma A_g \Sigma^{-1}, \qquad \Sigma A_d \Sigma^{-1}.$$

Si les quaternions sont entiers et si le déterminant de Σ vaut ± 1, les nouvelles matrices sont encore à termes entiers.

19. Substitutions et matrices orthogonales d'ordre 4. — 1° Une substitution linéaire orthogonale d'ordre 4 (à coefficients quelconques, rationnels ou irrationnels) peut être définie comme laissant invariable la forme $x_0^2 + x_1^2 + x_2^2 + x_3^2$. La matrice carrée S d'ordre 4 relative à la substitution doit vérifier

$$\| y_0\ y_1\ y_2\ y_3 \| = \| x_0\ x_1\ x_2\ x_3 \| .S,$$
$$y_0^2 + y_1^2 + y_2^2 + y_3^2 = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Il en résulte immédiatement la condition

$$S.\overline{S} = 1,$$

la matrice conjuguée $\overline{S}$ étant obtenue par l'échange des lignes et des colonnes.

Si la forme n'est pas conservée, mais est multipliée par un coefficient,

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 = m(x_0^2 + x_1^2 + x_2^2 + x_3^2),$$

l'équation du problème est

$$S.\overline{S} = m.$$

Toute matrice S satisfaisant à cette dernière condition sera dite *matrice orthogonale de norme m* : le scalaire m est la somme commune des carrés des termes d'une même ligne, et les produits des termes deux à deux ont une somme nulle pour deux lignes quelconques.

2° L'introduction des quaternions permet de ramener le problème à l'invariance d'une forme quadratique décomposée en facteurs linéaires. La substitution correspondant à S est telle que

$$(y_0 + y_1 i + y_2 j + y_3 k)(-y_0 + y_1 i + y_2 j + y_3 k)$$
$$= m(x_0 + x_1 i + x_2 j + x_3 k)(-x_0 + x_1 i + x_2 j + x_3 k).$$

Pour cela il faut et il suffit que

$$y_0 + y_1 i + y_2 j + y_3 k = U(\pm x_0 + x_1 i + x_2 j + x_3 k)V,$$

U et V étant deux quaternions vérifiant $N(U)N(V) = m$.

Notons d'ailleurs qu'un changement de signe ou une permutation des variables de la forme linéaire $x_0 + x_1 i + x_2 j + x_3 k$ transforme cette dernière en elle-même ou en sa conjuguée, au produit

près par des quaternions U, V (dont les composantes sont rationnelles de dénominateur 1 ou 2); ainsi, par exemple,

$$x_0 + x_1 i + x_2 j + x_3 k = -i(x_0 + x_1 i + x_2 j + x_3 k)i,$$
$$x_0 + x_2 i + x_1 j + x_3 k = (i - j)(-x_0 + x_1 i + x_2 j + x_3 k)\left(\frac{i-j}{2}\right).$$

Si nous posons

$$\mathrm{I} = \begin{Vmatrix} 1 \\ i \\ j \\ k \end{Vmatrix}, \qquad \mathcal{J}_0 = \begin{Vmatrix} \pm 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{Vmatrix} = \mathcal{J}_0^{-1},$$

nous obtenons pour solution du problème

$$\mathrm{SI} = \mathrm{U}\mathcal{J}_0\mathrm{IV}.$$

Toute matrice orthogonale de norme m est donc de la forme

$$\mathrm{S} = \mathcal{J}_0 \mathrm{U}_g \mathrm{V}_d, \qquad \mathrm{N(U)\,N(V)} = m,$$

$\mathcal{J}_0$ étant pris avec $+1$ ou -1 suivant que le déterminant de S est positif ou négatif. *Cette représentation est unique*, au produit près des facteurs U et V par deux scalaires inverses l'un de l'autre.

3° Voici quelques propriétés des matrices orthogonales, conséquence immédiate de l'égalité de définition $\mathrm{S}\overline{\mathrm{S}} = m$.

La matrice conjuguée $\overline{\mathrm{S}}$ est orthogonale en même temps que S; la propriété orthogonale est donc vraie pour les colonnes comme pour les lignes. Ce sont là les propriétés bien connues du tableau des 9 cosinus, qui devient ici un tableau de 16 cosinus, après division par $\sqrt{m}$.

Le déterminant d'une matrice orthogonale égale au signe près le carré de la norme,

$$\text{déterminant S} = \pm m^2.$$

Le produit de matrices orthogonales est encore une matrice orthogonale dont la norme égale le produit des normes.

On peut aussi vérifier cette propriété et retrouver le signe du produit des déterminants en utilisant la formule du 2°. Il suffit

pour cela de permuter certaines matrices et d'appliquer l'égalité, suivant le cas,

$$\mathcal{J}_0 A_g \mathcal{J}_0 = A_g \quad \text{ou} \quad \overline{A}_d.$$

Remarque. — Toute matrice orthogonale S est un produit de matrices de quaternions. Il reste à savoir si ces dernières peuvent être effectivement calculées à partir de S. Si S possède des termes irrationnels, on cherchera à construire une suite de matrices orthogonales S_i à termes rationnels dont S soit la limite. En multipliant chaque S_i par le dénominateur commun de ses termes, on obtient une matrice à termes entiers ayant les mêmes facteurs U_g et V_d à un coefficient scalaire près. Nous donnons ci-après le calcul de la décomposition des matrices à termes entiers.

20. Matrices orthogonales à termes entiers. — Représentons une substitution (S) par l'égalité

$$y_0 + y_1 i + y_2 j + y_3 k = A_0 x_0 + A_1 x_1 + A_2 x_2 + A_3 x_3,$$

où les coefficients du second membre sont des quaternions. Pour que la matrice S de la substitution soit orthogonale de norme m et à termes entiers, il faut et il suffit que les quaternions A_α soient entiers, orthogonaux deux à deux et de norme commune m. Leurs p. g. c. d. mixtes (§ 6) ont une norme égale à m. Les quaternions sont donc nécessairement de la forme

$$A_\alpha = U J_\alpha V \qquad (\alpha = 0, 1, 2, 3);$$

les J_α, unités orthogonales deux à deux, sont, à l'ordre et au signe près, les quatre unités $1, i, j, k$.

On ne change pas le problème en remplaçant U par un associé à gauche et V par un associé à droite. De la sorte, on peut faire

$$J_0 = \pm 1, \qquad J_1, J_2, J_3 = i, j, k \text{ (à l'ordre près).}$$

Si nous désignons par $\mathcal{J}$ l'une quelconque des douze matrices obtenues à partir de $\mathcal{J}_0$ (paragraphe précédent) en permutant les trois dernières lignes, nous voyons que la colonne des J_α est de la forme $\mathcal{J}$I et que la substitution (S) vérifie la condition

$$SI = U\mathcal{J}IV.$$

Par conséquent : *Toute matrice orthogonale de norme m à termes entiers est de la forme*

$$S = \mathcal{J} U_g V_d, \qquad N(U)\,N(V) = m.$$

Elle est le produit permutable de deux matrices de quaternions entiers, l'une à gauche, l'autre à droite, à la multiplication près par une matrice $\mathcal{J}$ orthogonale de norme 1.

En particulier *toute matrice orthogonale de norme un nombre premier est le produit d'une matrice de quaternion par une matrice de norme* 1.

Si la matrice orthogonale est primitive de norme impaire, la décomposition est unique. En effet U est alors nécessairement primitif de norme impaire et les quatre UJ_α sont premiers à droite dans leur ensemble; V est donc l'unique p. g. c. d. à droite des quaternions A_α. Si la matrice admet un diviseur entier scalaire, ou si sa norme est paire, il peut y avoir échange de certains facteurs entre U et V et substitution d'une matrice $\mathcal{J}$ à une autre.

Toutes les matrices orthogonales à termes entiers forment un *ensemble multiplicatif* : elles contiennent tout produit de deux d'entre elles et la matrice scalaire 1. Cet ensemble constitue un semi-groupe : la multiplication y est unipare,

$$SS_1 = SS_2 \text{ entraîne } S_1 = S_2.$$

Les matrices orthogonales de norme 1 sont au nombre de 384. Elles s'écrivent

$$\pm \mathcal{J} J_g J'_d,$$

où J et J′ sont deux unités choisies entre 1, i, j, k. Les substitutions correspondantes se réduisent à des permutations et changements de signe des variables; ce sont les seules substitutions linéaires transformant tout quaternion entier en un quaternion entier de même norme.

21. Identité de Lagrange et quaternions. — Considérons deux nombres hypercomplexes d'ordre 4, dont les composantes sont entières

$$A = [x_0, x_1, x_2, x_3], \qquad B = [y_0, y_1, y_2, y_3].$$

Pour chacun d'eux, appelons encore *norme* la somme des carrés des composantes.

Nous définissons le *produit de* A *par* B comme étant un nombre hypercomplexe, dont les quatre composantes sont des fonctions entières bilinéaires des composantes de A et de B, et dont la norme est égale au produit des normes de A et de B

$$AB = \| x_0\, x_1\, x_2\, x_3 \| . S,$$

où S désigne une matrice d'ordre 4, nécessairement orthogonale, dont les termes sont des fonctions linéaires de y_0, y_1, y_2, y_3 à coefficients entiers.

La recherche de toutes les matrices S revient à écrire de toutes les manières possibles l'identité de Lagrange en nombres entiers.

Chaque ligne de la matrice est une substitution linéaire orthogonale à coefficients entiers des composantes de B : elle contient donc ces composantes à l'ordre et au signe près. Il en est de même de chaque colonne, puisque la matrice est orthogonale. Appelons y'_0, y'_1, y'_2, y'_3 la première ligne et faisons en sorte que la première colonne soit y'_0, $-y'_1$, $-y'_2$, $-y'_3$, en modifiant s'il y a lieu l'ordre et le signe des composantes de A, qui deviennent ainsi x'_0, x'_1, x'_2, x'_3. Considérons alors

$$A' = x'_0 + x'_1 i + x'_2 j + x'_3 k, \qquad B' = y'_0 + y'_1 i + y'_2 j + y'_3 k,$$

quaternions *isomorphes* de A et B (c'est-à-dire ayant les mêmes composantes à l'ordre et au signe près). Nous voyons que la matrice est nécessairement de la forme

$$S = B'_g \quad \text{ou} \quad B'_d.$$

Le produit AB a donc les mêmes composantes que l'un des produits de quaternions A'B' ou B'A'.

Parmi les divers systèmes de nombres hypercomplexes jouissant de la propriété de la norme, les quaternions possèdent l'associativité du produit; d'autres possèdent la presque-commutativité, tel le système défini par

$$AB = \| x_0\, x_1\, x_2\, x_3 \| . \overline{B}'_d,$$

où B' a les mêmes composantes que B, système qui vérifie

$$BA = AB\,\mathrm{I}.$$

22. Sur un problème d'Euler. — Il s'agit du problème étudié par Euler et mentionné par Legendre dans sa Théorie des nombres :

Trouver les tableaux carrés d'ordre 4 à termes entiers pour lesquels la somme des carrés des termes soit égale dans chacune des lignes, des colonnes ou des diagonales, et la somme des produits des termes deux à deux soit nulle à l'égard de deux lignes ou de deux colonnes quelconques.

Si nous laissons de côté la propriété des diagonales, qui sera examinée plus loin, nous reconnaissons les propriétés caractéristiques des matrices orthogonales. Les tableaux cherchés sont des matrices orthogonales d'ordre 4 à termes entiers de la forme

$$S = \mathfrak{I} U_g V_d.$$

Cherchons à caractériser U et V. Nous posons

$$U = x + yi + zj + tk, \qquad V = x' + y'i + z'j + t'k,$$

et nous appelons A_0, A_1, A_2, A_3 les quaternions qui correspondent aux colonnes du tableau.

Le couple U, V est un quelconque des p. g. c. d. mixtes des A_α; on peut supposer que V est le p. g. c. d. à droite. Les huit quaternions associés à U, à gauche, sont alors premiers entre eux à droite dans leur ensemble, ce qui entraîne que U est primitif et de norme impaire.

Remplacer U par un de ses associés à gauche, ou remplacer V par un de ses associés à droite, revient à changer l'ordre et le signe des colonnes du tableau. On peut alors prendre pour x et pour x' les composantes ayant dans chaque quaternion la plus grande valeur absolue.

Si nous remplaçons U par un associé à droite (ou V par un associé à gauche), les quaternions A_α sont remplacés par des associés à droite (ou à gauche); les lignes du tableau permutent ou changent de signe. Si donc on ne tient compte ni du signe ni de l'ordre des lignes, on peut supposer que U contient au plus une seule composante négative, la première par exemple, et de même pour V. En effet

$$iUi = -x - yi + zj + tk,$$
$$jUj = -x + yi - zj + tk, \quad kUk = -x + yi + zj - tk.$$

Le changement de signe simultané de x et x', ou encore le remplacement de U et V par leurs conjugués, revient à une symétrie du tableau par rapport à la diagonale principale. Cette symétrie admise, on peut supposer qu'aucune composante de U n'est négative.

Enfin l'échange simultané de y avec z, de y' avec z' (ou y avec i, et y' avec t') revient à la même symétrie suivie d'une permutation de deux lignes ou de deux colonnes.

En conclusion, si l'on ne tient compte ni de l'ordre ni du signe des lignes ou des colonnes, ni de l'échange global des lignes et des colonnes, le tableau peut s'écrire

$$S = U_g V_d,$$

U étant un quaternion primitif de norme impaire dont les composantes vérifient

$$x \geqq y \geqq z \geqq t \geqq 0,$$

le quaternion V ayant ses trois dernières composantes positives ou nulles et au plus égales à la valeur absolue de la première composante.

23. **Exemples numériques.** — 1° Parmi les solutions du problème précédent se trouve le cas banal des matrices de quaternions, dont les termes sont égaux deux à deux. A l'opposé de ce cas, et d'après l'exemple même donné par Euler, recherchons des tableaux où les *seize termes soient tous différents en valeur absolue*.

Pour cela il ne faut pas que deux composantes de U forment une proportion (en valeur absolue) avec les deux composantes de mêmes rangs ou de rangs associés de V. C'est ainsi, par exemple, que tout tableau de norme $391 = 17.23$ possède au moins deux termes égaux ou opposés.

Il suffit de prendre, pour obtenir une famille de solutions,

$$U = 1 + i + j, \qquad x' \geqq y' \geqq z' \geqq t' \geqq 0,$$

ce qui correspond à la norme minimum de U, et de soumettre les composantes de V à un ensemble de conditions simples. On trouve

ainsi les deux tableaux

$$\begin{vmatrix} 17 & 7 & 4 & 0 \\ 6 & -14 & -1 & -11 \\ 5 & -3 & -16 & 8 \\ 2 & -10 & 9 & 13 \end{vmatrix}, \qquad \begin{vmatrix} 20 & 9 & 4 & 1 \\ 8 & -11 & -12 & -13 \\ 5 & -10 & -7 & 18 \\ 3 & -14 & 17 & -2 \end{vmatrix}.$$

Le premier est le tableau à termes tous différents qui a la norme minimum 354, et celui dont le plus haut terme 17 est minimum. Le second tableau, de norme 498, est un des plus simples qui contienne seize valeurs absolues toutes différentes et positives.

2° L'exemple donné par Euler possède une *propriété supplémentaire relative aux diagonales* : la somme des carrés des termes est la même pour les diagonales et pour les lignes, c'est-à-dire égale à la norme du tableau.

Cette propriété se traduit par les égalités

$$\begin{aligned} 4(x^2x'^2+y^2y'^2+z^2z'^2+t^2t'^2) &= 4(x^2t'^2+y^2z'^2+z^2y'^2+t^2x'^2) \\ &= (x^2+y^2+z^2+t^2)(x'^2+y'^2+z'^2+t'^2) \end{aligned}$$

dont l'étude n'est pas simple. Toutefois elles sont impossibles pour une norme impaire.

Nous tournons la difficulté en permutant circulairement les trois dernières colonnes du tableau. La condition devient

$$\begin{aligned} (xy+zt)(x'y'-z't') &= (xz+yt)(x'z'-y't') \\ &\quad +(xt+yz)(x't'-y'z') = 0. \end{aligned}$$

Une famille de solutions à un paramètre s'écrit

$$U = -9+5i+zj, \qquad V = 6+2i+3j+4k,$$

la norme de U n'étant plus supposée impaire. La première valeur $z = 2$ correspondant à des termes tous différents donne le tableau ci-après (au signe près des lignes) de norme 7150, un des plus simples du genre. Pour $z = 5$ nous retrouvons l'exemple choisi par Euler, de norme 8515.

$$\begin{vmatrix} 70 & 47 & 4 & 5 \\ 20 & -19 & -58 & -55 \\ 35 & -56 & -17 & 50 \\ 25 & -38 & 59 & -40 \end{vmatrix}, \qquad \begin{vmatrix} 79 & 41 & 8 & 23 \\ 32 & -37 & 49 & 61 \\ 17 & -68 & 12 & 59 \\ 31 & -29 & -77 & -28 \end{vmatrix}.$$

24. Tableaux de cosinus directeurs rationnels. — 1° Considérons un tableau de neuf cosinus directeurs. Ajoutons-lui une ligne de zéros, une colonne de zéros, à l'intersection desquelles nous plaçons le nombre 1. Nous obtenons une matrice orthogonale S d'ordre 4.

Le problème est ramené à l'étude d'une matrice orthogonale d'ordre 4, de norme 1, à termes rationnels, l'un d'eux valant 1. Supposons que le terme 1 appartienne à la première ligne et à la première colonne. La matrice est de la forme

$$S = \frac{1}{n} \mathcal{J} U_g V_d,$$

n désignant le dénominateur commun de ses termes, U et V étant des quaternions entiers. Le produit $\pm UV$, égal au premier terme de la colonne nSI (§ 20), se réduit à un scalaire puisque la première ligne de S comprend seulement 1, 0, 0, 0. Les quaternions U et V sont donc conjugués, à un coefficient scalaire près. Par conséquent *la matrice* S *est de la forme*

$$S = \frac{1}{u} \mathcal{J} U_g \overline{U}_d, \qquad N(U) = u,$$

où l'on peut supposer U primitif de norme impaire. En particulier les tableaux de cosinus exprimables exactement en décimales correspondent à une norme u valant 5^h, puissance de 5.

Si l'on fait abstraction de l'ordre et du signe des lignes ou des colonnes, on peut écrire

$$S = \frac{1}{u} U_g \overline{U}_d, \qquad U = x + yi + zj + tk, \qquad x \geqq y \geqq z \geqq t \geqq 0.$$

2° Recherchons les tableaux dont les cosinus sont différents en valeur absolue. Le changement de signe ou l'échange des composantes de U modifient seulement l'ordre ou le signe des cosinus. Nous supposons donc ces composantes positives et distinctes

$$x > y > z > t > 0.$$

Il faut alors et il suffit que $xy - zt$ soit différent de $xz + yt$ et de $xt + yz$.

On obtient ainsi le *tableau des cosinus rationnels distincts de dénominateur commun minimum*, dénominateur valant 57

$$\frac{1}{57}\begin{vmatrix} 52 & 23 & 4 \\ 17 & -44 & 32 \\ 16 & -28 & -47 \end{vmatrix}.$$

Parmi les tableaux exprimables exactement en décimales, celui qui dérive de $u = 5$ correspond à une solution impropre, la matrice orthogonale ne portant que sur quatre termes. Pour les tableaux à deux décimales, dérivant de $u = 25$, il y a une seule solution propre possédant d'ailleurs plusieurs termes égaux ou opposés. Avec trois décimales, $u = 125$, plusieurs tableaux existent dont un seul comporte des termes tous différents : c'est le *tableau le plus simple qui contienne neuf cosinus tous différents exprimés exactement en décimales.* Avec quatre décimales on pourrait écrire une dizaine de tableaux à cosinus tous distincts et non nuls.

$$\begin{vmatrix} 0,8 & 0,48 & 0,36 \\ 0,6 & -0,64 & -0,48 \\ 0,0 & -0,60 & 0,80 \end{vmatrix} \quad \begin{vmatrix} 0,8 & 0,576 & 0,168 \\ 0,6 & -0,768 & -0,224 \\ 0,0 & -0,280 & 0,960 \end{vmatrix}.$$

3° Supposons les neuf cosinus réduits au plus petit dénominateur commun; le tableau contient alors six numérateurs pairs et trois impairs. Cette remarque suffit à prouver que la somme des carrés des cosinus ne peut valoir 1 dans chaque diagonale, quel que soit l'ordre choisi pour les lignes ou les colonnes.

Il n'y a donc pas de tableau de cosinus rationnels possédant la propriété des diagonales.

(Manuscrit reçu le 10 août 1943.)