Zeitschrift: L'Enseignement Mathématique

Band: 18 (1916)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR L'ARITHMÉTIQUE DES NOMBRES HYPERCOMPLEXES

Kapitel: I

Autor: DuPasquier, L.-G.

DOI: https://doi.org/10.5169/seals-16879

SUR L'ARITHMÉTIQUE DES NOMBRES HYPERCOMPLEXES

PAR

L.-G. DuPasquier (Neuchâtel).

Sommaire :

I

1. — En construisant une *théorie des nombres* ou *arithnomie*[1] dont les *éléments* sont non seulement les nombres entiers ordinaires, mais les nombres entiers dits imaginaires, ou complexes, de la forme $a_0 + a_1 i$, où a_0 et a_1 représentent des nombres réels quelconques, tandis que i est un symbole défini par l'équation

$$i^2 = -1 \ , \qquad \text{ce qui fait écrire} \qquad i = \sqrt{-1} \ ,$$

[1] Le néologisme d'arithnomie est proposé par M. A. Aubry à Dijon ; c'est une abréviation d'« arithmonomie » qui est synonyme d'« arithmologie », de « théorie des nombres », ou d'« arithmétique généralisée ». (En grec, « arithmos » = nombre ; « nomos » = loi ; d'où « arithmonomie » ; l'*arithnomie* signifie donc : la science des lois qui régissent les nombres.)

en créant cette arithmétique généralisée, dis-je, *Gauss* a fait œuvre de génie, car cette création hardie ouvrait à la théorie des nombres des horizons tout nouveaux et un champ de recherches d'une étendue insoupçonnée.

Cette arithmétique généralisée due à *Gauss* repose sur une définition qui semble se présenter d'elle-même à l'esprit et que voici :

Définition I: Soit $a = a_0 + a_1 i$ un nombre complexe, où a_0 et a_1 représentent deux nombres *réels* dits *coordonnées* du nombre complexe a. Nous appellerons a « un nombre complexe *entier* », si ses deux coordonnées, a_0 et a_1, sont des nombres *entiers ordinaires* positifs, nuls ou négatifs : nous appellerons a « un nombre complexe *non entier* », si l'une au moins de ses deux coordonnées est fractionnaire ou irrationnelle.

Par abréviation, nous dirons souvent, dans la suite, *entier complexe* au lieu de « nombre complexe entier ».

2. — L'arithmétique généralisée érigée par *Gauss* dans le domaine de ces nombres complexes et basée sur la définition I ci-dessus, présente des analogies frappantes avec l'arithmétique ordinaire. On y retrouve, entre autres, les nombres complexes entiers *irréductibles* jouant le même rôle que les nombres premiers dans l'arithmétique classique. Nous les appellerons souvent, pour abréger, *nombres premiers complexes*. On sait que ce sont : 1° les nombres premiers ordinaires de la forme $p = 4n + 3$, à savoir

$$3\,, \quad 7\,, \quad 11\,, \quad 19\,, \quad 23\,, \quad 31\,, \quad 43\,, \quad 47\,, \quad 59\,, \ldots$$

dont la *norme* est p^2; 2° le nombre $1 + i$ dont la norme est égale à 2 ; 3° les nombres complexes entiers $r + si$ dont la norme, $r^2 + s^2$, est un nombre premier ordinaire p de la forme $4n + 1$, par exemple :

$$1 + 2i\,, \quad 2 + i\,, \quad 2 + 3i\,, \quad 3 + 2i\,, \quad 1 + 4i\,, \quad 4 + i\,, \quad 2 + 5i\,, \quad 5 + 2i\,,$$
$$1 + 6i\,, \quad 1 - 6i\,, \quad 4 + 5i\,, \quad 5 + 4i\,, \quad \ldots$$

On retrouve ensuite, dans l'arithmétique généralisée de *Gauss*, la décomposition, toujours possible et toujours univoque, de tout entier complexe donné en ses facteurs premiers. On y retrouve encore *le plus grand commun diviseur* et le plus petit commun multiple de deux (ou, plus généralement, de n) entiers complexes donnés ; l'analogue de l'algorithme d'*Euclide* permettant de déterminer ce plus grand commun diviseur par un nombre fini d'opérations rationnelles. On y trouve aussi toute la théorie des *congruences ;* on y retrouve l'analogue du théorème de *Fermat*, l'analogue du théorème de *Wilson*, etc.

3. — En 1886, M. *Lipschitz* publiait le résultat de ses recherches sur la transformation, par des substitutions réelles, d'une somme de deux carrés en elle-même[1]. En partant d'un point de vue très original et tout à fait personnel, M. *Lipschitz* découvrait à nouveau le calcul des nombres complexes de la forme $a_0 + a_1 i$, où $i^2 = -1$. Il reconstruisait alors l'arithmétique généralisée ou arithnomie de ces nombres complexes, comme *Gauss* l'avait déjà fait avant lui, en prenant aussi comme éléments les nombres complexes *entiers* tels qu'ils résultent de la définition I ci-dessus. Quoique son point de départ soit tout autre que celui de *Gauss*, M. *Lipschitz* arrive au même résultat : à la même arithnomie, en se basant sur la même définition.

4. — Pour préparer la généralisation à d'autres systèmes de nombres complexes, nous introduirons dès maintenant un nouveau symbole e_0 en posant $e_0 = 1$; écrivant alors e_1 à la place de i, de sorte que

$$e_1^2 = -1 = -e_0 ,$$

on voit que les nombres complexes de *Gauss* peuvent s'écrire sous la forme

$$a = a_0 e_0 + a_1 e_1 = \sum_{\lambda}^{0;\,1} a_\lambda e_\lambda ,$$

où les e_λ sont des symboles dits « *unités relatives* du sys-

---

[1] *Untersuchungen über die Summen von Quadraten*. Bonn, 1886. Voir la traduction française publiée par *J. Molk* dans le « Journal de mathématiques pures et appliquées » fondé par *Liouville*, IV[e] série, tome 2[e] (année 1886), p. 373-439 : *Recherches sur la transformation, par des substitutions réelles, d'une somme de deux ou de trois carrés en elle-même.*

tème de nombres complexes », symboles obéissant, par définition, aux relations

$$e_0^2 = e_0 \ , \qquad e_1^2 = -\, e_0 \ , \qquad e_0 . e_1 = e_1 . e_0 = e_1 \tag{1}$$

Nous dirons que les nombres complexes de *Gauss* forment « un système de nombres complexes à 2 coordonnées indépendantes », ou « à 2 unités relatives », système entièrement défini par les conventions sur l'égalité, l'addition et par les relations (1) qui règlent la multiplication. On peut ranger celles-ci en un tableau de la manière suivante :

	e_0	e_1
e_0	e_0	e_1
e_1	e_1	$-\,e_0$

i et k représentant l'un des nombres 0 ou 1, le produit $e_i . e_k$ se trouve dans la ligne (horizontale) ayant à gauche e_i et dans la colonne (verticale) portant en haut e_k.

5. — Cherchant à étendre ses résultats à la transformation, par des substitutions réelles, d'une somme de *trois* carrés en elle-même, M. *Lipschitz*, partant du même point de vue original, retrouva le calcul des quaternions découvert avant lui, en 1843, par *W. R. Hamilton*.

Voici, à l'intention des lecteurs non versés dans la théorie des quaternions, les principes fondamentaux de ce calcul exposés dans un langage purement arithmétique.

On sait que les *quaternions* sont des nombres hypercomplexes à 4 coordonnées indépendantes, tel par exemple

$$a = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 \ ,$$

où a_0, a_1, a_2, a_3 représentent quatre nombres réels dits *les coordonnées*[1] du quaternion a, et i_1, i_2, i_3, trois symboles

---

[1] Nous distinguons entre « coordonnées » et « composantes » d'un nombre complexe (ou hypercomplexe). Par *composantes* du quaternion a, nous entendons les produits $a_1 i_1$; $a_2 i_2$; $a_3 i_3$. Comparez la note suivante.

dits *les unités relatives*, obéissant aux relations suivantes :

$$\left.\begin{array}{c} i_1^2 = i_2^2 = i_3^2 = -1 \\ i_1.i_2 = -i_2.i_1 = i_3 \;,\quad i_2.i_3 = -i_3.i_2 = i_1 \;,\quad i_3.i_1 = -i_1.i_3 = i_2 \end{array}\right\} \quad (2)$$

Deux quaternions sont dits *égaux*, si les 4 coordonnées de l'un sont égales, respectivement, aux coordonnées correspondantes de l'autre.

Désignons par b le quaternion

$$b = b_0 + b_1 i_1 + b_2 i_2 + b_3 i_3 \;;$$

l'égalité entre quaternions $a = b$ est alors équivalente aux quatre égalités simultanées

$$a_\lambda = b_\lambda \qquad (\lambda = 0\,,\ 1\,,\ 2\,,\ 3)\ .$$

L'addition, la soustraction et la multiplication des *quaternions* se font d'après les règles ordinaires de l'algèbre, les symboles i_λ se composant conformément aux relations (2). La principale différence entre l'algèbre classique et celle des quaternions provient de ce que la multiplication des quaternions n'est pas commutative en général; en effet, $a.b \neq b.a$, comme on le voit en calculant directement ces deux produits, si a et b désignent, comme ci-dessus, deux quaternions quelconques. Donc, la valeur d'un produit de quaternions dépend, en général, de l'ordre de succession des facteurs de ce produit. Il s'ensuit que la division n'est en général pas univoque dans ce domaine ; il faut distinguer entre une « division à gauche » et une « division à droite », suivant que, les quaternions a et b étant donnés, on cherche le quaternion

$$y = y_0 + y_1 i_1 + y_2 i_2 + y_3 i_3 \qquad \text{tel que} \qquad a = y.b \ ,$$

ou le quaternion

$$x = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 \qquad \text{tel que} \qquad a = b.x \ .$$

6. — Par analogie avec la théorie des nombres complexes de *Gauss*, on pose les définitions suivantes :

Le quaternion a est dit *réel*, si ses trois dernières coordonnées, a_1, a_2, a_3, sont nulles.

A tout quaternion a correspond un quaternion

$$a' = a_0 - a_1 i_1 - a_2 i_2 - a_3 i_3$$

dit *conjugué de a*. Le produit d'un quaternion quelconque a et de son conjugué a' est toujours réel et s'appelle « *la norme* du quaternion a ». La norme de a, égale du reste à la norme de a', est donc définie par l'équation

$$\mathrm{N}(a) = a . a' = a' . a = a_0^2 + a_1^2 + a_2^2 + a_3^2 .$$

Ce nombre réel n'est nul *que* dans le cas où $a = 0$. Si $a \neq 0$, on entend par « l'*inverse* de a » le quaternion a^{-1} ainsi défini :

$$a^{-1} = \frac{1}{a} = \frac{a'}{\mathrm{N}(a)} ;$$

il satisfait aux relations $a . a^{-1} = a^{-1} . a = 1$.

On vérifie sans peine que le conjugué du produit de plusieurs quaternions donnés est égal au produit des conjugués des facteurs pris dans l'ordre renversé ; en formule :

$$(a . b)' = b' . a' .$$

Il s'ensuit le théorème fondamental que la norme d'un produit de quaternions est égale au produit des normes des facteurs :

$$\mathrm{N}(a . b) = \mathrm{N}(a) . \mathrm{N}(b) .$$

7. — Puisqu'en intervertissant l'ordre des facteurs, on change le produit, il existe en général deux quotients différents du quaternion donné a par le quaternion donné b où l'on suppose $b \neq 0$, à savoir :

1° le quaternion $b^{-1} . a$ qui est « le quotient *à droite* de a par b » ; c'est la solution x de l'équation $a = b . x$;

2° le quaternion $a . b^{-1}$ qui est « le quotient *à gauche* de a par b » ; c'est la solution y de l'équation $a = y . b$. On ne peut donc pas, en général, employer pour la division le signe ordinaire $a : b$ ou $\frac{a}{b}$. Sauf définition spéciale, ces signes n'ont de sens que si les deux quaternions a et b' sont *commutables,* c'est-à-dire si $a . b' = b' . a$, ce qui n'est pas le cas en général.

Dans le domaine des quaternions, il y a donc lieu de distinguer deux arithmétiques se développant parallèlement l'une à l'autre, mais différentes l'une de l'autre : une « arithmétique à gauche » et une « arithmétique à droite ». Elles se pénètrent du reste souvent l'une l'autre, engendrant des analogies et des contrastes frappants avec l'arithmétique classique.

8. — Pour nous conformer aux notations générales utiles plus tard, nous introduirons de nouveau les symboles e_λ dits *unités relatives,* en posant

$$e_0 = 1 \ , \qquad e_1 = i_1 \ , \qquad e_2 = i_2 \ , \qquad e_3 = i_3 \ .$$

Tout quaternion x s'écrit alors

$$x = x_0 e_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 = \sum_{\lambda}^{0..3} x_\lambda e_\lambda \ .$$

Nous dirons que les quaternions forment « un système de nombres hypercomplexes à 4 coordonnées indépendantes », ou « à 4 *unités relatives* », système qui sera défini par les conventions se rapportant à l'égalité, à l'addition et par les relations suivantes qui règlent la multiplication :

$$\left.\begin{array}{c} e_0^2 = e_0 \ ; \quad e_1^2 = e_2^2 = e_3^2 = -\, e_0 \\ e_1 . e_2 = -\, e_2 . e_1 = e_3 \ ; \quad e_2 . e_3 = -\, e_3 . e_2 = e_1 \ ; \quad e_3 . e_1 = -\, e_1 . e_3 = e_2 \end{array}\right\} \quad (3)$$

Ces relations se trouvent condensées dans le tableau suivant :

	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	$-e_0$	e_3	$-e_2$
e_2	e_2	$-e_3$	$-e_0$	e_1
e_3	e_3	e_2	$-e_1$	$-e_0$

Représentant par i et par k l'un des nombres 0, 1, 2, 3, on trouvera la valeur du produit $e_i . e_k$ à l'intersection de la ligne (horizontale) portant à gauche e_i et de la colonne (verticale) portant en haut e_k.

Définition II: Un quaternion

$$a = \sum_{\lambda}^{0..3} a_\lambda e_\lambda$$

est dit *rationnel*, si chacune de ses 4 coordonnées a_λ est un nombre rationnel quelconque, entier ou fractionnaire.

L'ensemble de tous les quaternions rationnels forme alors un « *corps* de quaternions » ou « domaine de rationalité »; c'est-à-dire que les quaternions rationnels se reproduisent par addition, soustraction, multiplication et division; en d'autres termes encore : la somme, la différence, les produits et les quotients de deux quaternions rationnels sont toujours de nouveau des quaternions rationnels.

C'est exclusivement de quaternions rationnels que nous parlerons dans la suite.

9. — Après cette digression sur les quaternions, revenons au mémoire de M. *Lipschitz* cité plus haut.

Ayant retrouvé, par une voie toute personnelle, le calcul des quaternions, M. *Lipschitz* érige une nouvelle arithmétique généralisée dont les éléments sont *les quaternions entiers.* Cette arithnomie des quaternions, érigée par M. *Lipschitz,* repose sur une définition qui se présente d'elle-même à l'esprit et qui semble une extension naturelle de la définition I ci-dessus, donnée déjà par *Gauss* pour les nombres complexes ordinaires.

Nous appellerons *lipschitzienne* cette définition du quaternion entier, par opposition à la définition *hurwitzienne* que nous introduirons plus bas et que nous démontrerons être préférable. Voici la définition « lipschitzienne » du quaternion entier :

Définition III: Un quaternion rationnel $a = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3$ est dit *entier*, si ses coordonnées a_λ (où $\lambda = 0, 1, 2, 3$) sont toutes quatre des nombres entiers ordinaires, positifs, nuls ou négatifs.

Le quaternion rationnel a sera dit *non entier*, si l'une au moins de ses quatre coordonnées est un nombre fractionnaire.

10. — L'arithnomie des quaternions telle que l'a érigée M. *Lipschitz* présente des exceptions étonnantes aux règles générales ; on dirait presque des anomalies. Nous allons en citer deux exemples. A cet effet, il est nécessaire de poser encore quelques définitions.

Le quaternion entier a est dit « *divisible à droite* [resp. *à gauche*] par le quaternion entier b », s'il existe un quaternion *entier* c vérifiant l'égalité $a = c.b$ [resp. $a = b.c$]. Dans ce cas, on dit aussi que « b est *un diviseur à droite* [resp. *à gauche*] de a », ou encore : que « b est contenu, ou entre dans a, comme diviseur à droite [resp. à gauche] ». D'après cela, le quaternion entier et non nul b sera un diviseur à droite de a, si $a.b^{-1}$ est un quaternion entier.

Pour que le quaternion entier ε soit contenu comme diviseur à droite dans n'importe quel quaternion entier, il faut que ε^{-1} soit entier ; alors ε est aussi contenu comme diviseur à gauche dans tout quaternion entier. Un tel quaternion ε est dit « une *unité* ». *La condition nécessaire et suffisante pour que ε soit une unité est que* $\mathrm{N}(\varepsilon) = 1$. Il existe, dans le domaine des quaternions entiers au sens de M. *Lipschitz*, 8 unités qui sont ± 1, $\pm i_1$, $\pm i_2$, $\pm i_3$.

Deux quaternions entiers sont dits *associés à droite* (resp. *à gauche*), s'ils ne diffèrent l'un de l'autre que par un facteur unité à droite (resp. à gauche) ; ainsi, a désignant un quaternion entier, $\pm a$, $\pm a.i_1$, $\pm a.i_2$, $\pm a.i_3$ sont « associés à droite », et $\pm a$, $\pm i_1.a$, $\pm i_2.a$, $\pm i_3.a$ sont « associés à gauche ». Dans les recherches sur la divisibilité, des quaternions associés sont équivalents, c'est-à-dire qu'ils peuvent se remplacer l'un l'autre (comme c'est le cas dans la théorie classique des nombres et dans l'arithnomie des « complexes entiers » de *Gauss*).

On définit le quaternion *primaire* de façon à ce qu'il soit toujours déterminé univoquement dans le groupe des 8 quaternions associés entre eux ; dans les théorèmes de divisibilité, on peut alors se borner à la considération des quaternions primaires.

Enfin, un quaternion entier a est *primitif* (ou *proprement dit*), si ses 4 coordonnées a_λ n'ont pas d'autre commun diviseur que 1 ; dans le cas contraire, a est un quaternion non primitif (ou improprement dit) ; exemple : $9 + 3i_1 + 6i_2 + ni_3$ est *primitif* dès que sa dernière coordonnée, n, n'est pas divisible par 3, mais non primitif, si n est multiple de 3.

11. — Malgré la non-commutativité de la multiplication, on réussit à définir le quaternion entier *irréductible*, ou *quaternion premier*, l'analogue du nombre premier de l'arithmétique classique. *Pour qu'un quaternion entier* p *soit premier, il faut et il suffit que sa norme* N(p) *soit un nombre premier ordinaire.* Il existe en tout $p + 1$ quaternions premiers, tous de même norme p, essentiellement différents entre eux, c'est-à-dire non associés, par exemple tous primaires. M. *Lipschitz* démontre ensuite qu'on peut toujours mettre un quaternion entier primitif donné, c, sous forme d'un produit de quaternions premiers, en imposant à ces quaternions de se suivre, de droite à gauche, dans un ordre tel que leurs normes suivent un ordre fixé arbitrairement pour les facteurs premiers de la norme du quaternion donné c. Une fois qu'on a fixé cet ordre, chacun des quaternions premiers qui figurent dans le produit est déterminé, de proche en proche, sans ambiguïté, à condition toutefois que $N(c)$ soit un nombre impair ou le double d'un nombre impair.

Ainsi, la décomposition du quaternion entier primitif donné c est univoque dès que, ayant décomposé sa norme $N(c)$ en ses facteurs premiers, par exemple $N(c) = p.r.s \ldots$, on a arrêté l'ordre de succession de ces facteurs premiers $p, r, s \ldots$ qui peuvent naturellement être égaux ou inégaux entre eux.

Mais il y a une curieuse exception : c'est quand la norme du quaternion donné c est divisible par 4 ; dans ce cas, la décomposition de c, quand bien même on a arrêté l'ordre de succession des facteurs premiers $p, r, s, \ldots$, n'est plus univoque, mais possible de 24 manières différentes ! On peut bien dire que c'est là une anomalie.

12. — On en trouve aussi dans la théorie du plus grand commun diviseur. Deux quaternions entiers donnés, a et b, ont un plus grand commun diviseur différent d'une unité quand leurs normes, N(a) et N(b), ne sont pas deux nombres premiers entre eux. Mais ici encore, il y a de curieuses exceptions, des anomalies étonnantes qui paraissent tout à fait inexplicables, déconcertantes même.

En prenant, par exemple, $a = 2$, $b = 1 + i_1 + i_2 + i_3$, on a $\mathrm{N}(a) = \mathrm{N}(b) = 4$ et l'on s'attend à ce que a et b possèdent « un plus grand commun diviseur à droite », disons δ, de façon à ce qu'on ait simultanément

$$2 = p.\delta \; ; \quad 1 + i_1 + i_2 + i_3 = p_1.\delta \, ,$$

où p et p_1 désigneraient certains quaternions entiers. (Pour donner un exemple concret, nous prenons « l'arithnomie à droite ».) Les égalités

$$2 = (1 - i_1).(1 + i_1) = (1 - i_2).(1 + i_2) = (1 - i_3).(1 + i_3)$$
$$1 + i_1 + i_2 + i_3 = (1 + i_3).(1 + i_1) = (1 + i_1).(1 + i_2) = (1 + i_2).(1 + i_3)$$

montrent bien que les deux quaternions en question possèdent trois « communs diviseurs à droite », à savoir :

$$\delta_1 = 1 + i_1 \, , \qquad \delta_2 = 1 + i_2 \, , \qquad \delta_3 = 1 + i_3 \, .$$

Raison de plus, semble-t-il, pour qu'il existe « *un plus grand* commun diviseur à droite », δ, lequel devrait être un commun multiple des trois diviseurs δ_1, δ_2, δ_3, en sorte qu'on ait $\delta = d_1.\delta_1 = d_2.\delta_2 = d_3.\delta_3$, où d_1, d_2, d_3 désigneraient certains quaternions entiers. Or, il n'en est rien.

On démontre très facilement, en prenant les normes, que les trois dernières équations sont en contradiction avec $2 = p\,\delta$, $1 + i_1 + i_2 + i_3 = p_1.\delta$. Voilà donc deux quaternions entiers a et b de même norme, possédant trois communs diviseurs différents (ces diviseurs sont même tous trois des quaternions *premiers*), mais n'ayant, malgré cela, pas de *plus grand* commun diviseur, au sens habituel de ce terme. On peut bien dire, de nouveau, que c'est là une anomalie.

La raison profonde de ces anomalies a été trouvée et indiquée pour la première fois par M. *A. Hurwitz* à Zurich. Elle tient à la définition même du quaternion « entier », comme nous allons le montrer.