V

dition et de la soustraction, tous les éléments de l'ensemble en question. Donc, $\{J\}$ n'est pas un domaine holoïde et ne saurait être envisagé comme composé exclusivement de nombres *entiers* (v. article 17).

V

51. — Bien que le corps de nombres $\{K\}$ ne contienne aucun domaine holoïde maximal, on peut néanmoins tenter d'y construire une arithmétique généralisée. Comme fondement de cette arithnomie, on essaiera la

Définition XI : un complexe rationnel

$$a = m_1 e_1 + \frac{m_2}{g} e_2 + m_3 e_3$$

est réputé *entier*, si m_1, m_2, m_3 représentent des nombres entiers ordinaires, pouvant prendre toutes les valeurs de $-\infty$ à $+\infty$, g étant un nombre entier non nul, arbitrairement choisi, mais fixe.

L'ensemble

$$[H] = \left[m_1 e_1 + \frac{m_2}{g} e_2 + m_3 e_3 \right]$$

est bien un domaine holoïde, et il renfermera exclusivement des complexes *entiers*, en vertu de la définition XI; tous les autres complexes du corps $\{K\}$, c'est-à-dire ceux ne faisant pas partie de [H], seront réputés *non entiers*.

Les « nombres entiers » dont nous allons faire la théorie constituent un domaine holoïde non maximal, de sorte qu'il faut s'attendre *a priori* à ce que cette arithnomie ne soit pas régulière, mais présente des singularités étonnantes, comparée à l'arithmétique classique.

52. — Pour abréger l'écriture, nous représenterons nos complexes entiers en écrivant uniquement les coordonnées. Nous figurerons ces complexes, sans écrire les unités relatives e_λ ni les signes +, en mettant simplement les coordonnées, séparées par des vigules, entre parenthèses; et ce seront ces parenthèses qui indiqueront symboliquement la

liaison censée exister entre les coordonnées, liaison qui fait que les 3 nombres constituent un seul et même tout. Ainsi, $a = a_1 e_1 + \frac{a_2}{g} e_2 + a_3 e_3$ s'écrira simplement $a = \left(a_1, \frac{a_2}{g}, a_3\right)$, où $g \neq 0$ est un nombre entier fixe. Le complexe a sera donc *entier*, si les trois nombres a_1, a_2 et a_3 le sont ; et a sera *non entier*, si l'un au moins de ces trois nombres a_λ est fractionnaire.

Tout nombre réel r pourra être envisagé comme un de ces complexes de la forme $r = (r, 0, r)$; en particulier, le nombre $1 = (1, 0, 1)$.

53. — *Définition de la divisibilité.* Un complexe entier $a = \left(a_1, \frac{a_2}{g}, a_3\right)$ est dit « divisible par le complexe entier $b = \left(b_1, \frac{b_2}{g}, b_3\right)$ », s'il existe un complexe *entier* $c = \left(c_1, \frac{c_2}{g}, c_3\right)$ satisfaisant à l'équation $a = b \,.\, c$. Nous dirons aussi que, dans ce cas, « b est un diviseur de a » et que « *a contient b* ». Si b est de norme nulle, l'équation $a = b \,.\, c$ n'a de solution en complexes entiers que si a est aussi de norme nulle. En particulier, b étant donné, l'égalité $0 = b \,.\, c$ est vérifiée par une infinité de complexes entiers $c = \mathrm{B}' \,.\, h$, où h est un complexe entier quelconque et B' le conjugué de b. De là vient le nom de « diviseur de zéro ».

54. — Le complexe entier ε est dit *une unité,* s'il entre comme diviseur dans tout complexe entier (v. article 10). Il existe dans le domaine [H] dont nous nous occupons une infinité d'unités, à savoir les complexes

$$\varepsilon = \left(\pm 1, \pm \frac{k}{g}, \pm 1\right)$$

k étant un nombre entier quelconque. Remarquons que $\left(1, \frac{k}{g}, 1\right) = \left(1, \frac{1}{g}, 1\right)^k$ pour toute valeur entière, positive, nulle ou négative, de k. En considérant comme unités *fondamentales* $\varepsilon_1 = (-1, 0, 1)$; $\varepsilon_2 = (1, 0, -1)$; $\varepsilon_3 = \left(1, \frac{1}{g}, 1\right)$, on peut mettre n'importe quelle unité ε sous forme d'un produit de ces 3 unités fondamentales : $\varepsilon = \varepsilon_1^n \,.\, \varepsilon_2^m \,.\, \varepsilon_3^k$, où n, m et k sont des entiers appropriés.

55. — Deux complexes entiers sont dits *associés*, s'ils ne diffèrent l'un de l'autre que par un facteur unité ε (v. article 10). A tout complexe entier a sont ainsi associés une infinité de complexes $a\varepsilon$, où ε représente une unité quelconque. On sait que dans toutes les recherches relatives à la divisibilité, des complexes associés sont équivalents et peuvent se remplacer l'un l'autre, comme c'est déjà le cas dans la théorie des nombres ordinaires. Dans le groupe formé par l'ensemble des complexes associés au même complexe entier a, donc associés entre eux, il suffira d'en choisir un, convenablement défini et qui remplacera tous les autres. On appelle ce représentant : un complexe *primaire* ; dans les théorèmes de divisibilité et de décomposition en facteurs, il suffit d'envisager les complexes primaires.

Dans le domaine des nombres hypercomplexes dont nous nous occupons ici, on peut d'abord supposer non négatives les trois coordonnées d'un complexe primaire a, puisqu'au lieu de x, on peut au besoin considérer $-x$, ou $\varepsilon_1 x$, ou $\varepsilon_2 x$; a étant supposé de norme non nulle, envisageons son associé

$$a \cdot \varepsilon_3^k = \left(a_1, \frac{a_2}{g}, a_3\right) \cdot \left(1, \frac{k}{g}, 1\right) = \left(a_1, \frac{a_2 + k a_1}{g}, a_3\right) = \left(a_1, \frac{a_2'}{g}, a_3\right).$$

On voit que le nombre entier k peut être choisi de manière que $a_2' < a_1$ et qu'alors, a_2' est déterminé de façon univoque. Ceci conduit à la *définition* suivante : un complexe entier $a = \left(a_1, \frac{a_2}{g}, a_3\right)$ non diviseur de zéro est dit ***primaire,*** si ses coordonnées satisfont aux inégalités simultanées $0 < a_1$; $0 \leq a_2 < a_1$; $0 < a_3$.

Donc, si $x = \left(x_1, \frac{x_2}{g}, x_3\right)$ est un complexe entier primaire de norme non nulle, x_2 ne peut avoir que l'une des valeurs $0, 1, 2, 3, \ldots, x_1 - 1$. Parmi tous les complexes entiers associés entre eux se trouve toujours un, mais un seul, qui est *primaire*.

56. — Quant aux diviseurs de zéro à première coordonnée nulle, tous de la forme $\left(0, \frac{a_2}{g}, a_3\right)$, ils constituent un groupe particulier, un sous-système à deux coordonnées contenu

entièrement dans le système à trois coordonnées que nous envisageons. Leur étude devrait se faire à part, et comme ce n'est pas le but de ce travail, nous les excluons des recherches subséquentes.

Quant aux diviseurs de zéro dont la troisième coordonnée est nulle sans que la première le soit, tous de la forme $\left(y_1, \frac{y_2}{g}, 0\right)$, ils constituent également un sous-système particulier à deux unités relatives, demandant une étude spéciale. On peut y maintenir, pour le complexe *primaire*, la définition donnée ci-dessus (art. 55), avec cette seule différence que $a_3 = 0$. Nous les excluons aussi des recherches ultérieures dans ce travail.

57. — En analogie avec la théorie classique des nombres, nous définirons : un complexe entier $a = \left(a_1, \frac{a_2}{g}, a_3\right)$ qui n'est pas une unité ni un diviseur de zéro, est dit *irréductible*, ou *premier*, si dans toutes les décompositions possibles $a = b \,.\, c$ de a en deux facteurs, l'un de ces derniers est toujours une unité. Ces complexes entiers irréductibles joueront ici le rôle des nombres premiers de l'arithmétique ordinaire.

Dans le domaine que nous étudions, il existe trois catégories de complexes irréductibles, à savoir :

1° Les complexes de la forme $\alpha = (1, 0, p) = e_1 + pe_3$, où p est un nombre premier naturel. Leur norme $N(\alpha) = p$ est un nombre premier. Les complexes entiers, non primaires, de la forme $\left(1, \frac{a_2}{g}, p\right)$ leur sont associés et n'en diffèrent donc pas essentiellement.

2° Les complexes de la forme $\beta = (p, 0, 1) = pe_1 + e_3$, où p représente un nombre premier naturel. Leur norme $N(\beta) = p^2$ est le carré d'un nombre premier.

3° Les complexes de la forme $\gamma = \left(p^n, \frac{a_2}{g}, 1\right)$, où p est un nombre premier ordinaire, l'exposant n un nombre naturel quelconque et a_2 un nombre entier positif inférieur à p^n et non divisible par p,

$$0 < a_2 < p^n \qquad \text{et} \qquad a_2 \not\equiv 0 \pmod{p} \,.$$

Leur norme $N(\gamma) = p^{2n}$ est une puissance paire quelconque d'un nombre premier naturel p.

Si l'on voulait décomposer γ en facteurs, on devrait avoir :

$$\gamma = \left(p^k, \frac{x}{g}, 1\right) \cdot \left(p^m, \frac{y}{g}, 1\right) = \left(p^{k+m}, \frac{p^k y + p^m x}{g}, 1\right)$$

d'où résulterait : $k + m = n$, et

$$a_2 = p^m x + p^k y = p^m (x + y p^{k-m}) ,$$

en supposant $k \geqq m$. Si $m > 0$, la coordonnée a_2 serait divisible par p, contrairement à l'hypothèse. Cette contradiction ne peut être levée qu'en prenant $m = 0$; mais alors, l'un des deux facteurs est toujours une unité et, par conséquent, γ un complexe *irréductible*.

Remarquons qu'il existe un seul complexe premier *primaire* α de norme p, à savoir $(1, 0, p)$; il représente tous les complexes entiers $\left(1, \frac{x}{g}, p\right)$, car ils lui sont tous associés ; par contre, il existe p complexes premiers *primaires* β de même norme p^2, essentiellement différents entre eux, c'est-à-dire non associés, à savoir :

$$(p, 0, 1) ; \left(p, \frac{1}{g}, 1\right) ; \left(p, \frac{2}{g}, 1\right) ; \ldots ; \left(p, \frac{p-1}{g}, 1\right)$$

ils représentent tous les complexes $\left(p, \frac{x}{g}, 1\right)$ de même norme p^2.

Les nombres premiers naturels tels que p ne sont pas irréductibles dans ce domaine, puisque

$$p = (p, 0, p) = (1, 0, p) \cdot (p, 0, 1) .$$

58. — Pour décomposer en facteurs premiers un complexe entier donné quelconque, a, on a :

$$a = \left(a_1, \frac{a_2}{g}, a_3\right) = \left(a_1, \frac{a_2}{g}, 1\right) \cdot \left(1, 0, a_3\right) .$$

Il suffit donc de considérer deux catégories de complexes entiers : ceux de la forme $(1, 0, m) = e_1 + m e_3$ et ceux de la forme $\left(a_1, \frac{a_2}{g}, 1\right)$ dont la dernière coordonnée est 1.

Désignant par $p_1, p_2, \ldots, p_\nu$ les facteurs premiers de m, de sorte que $m = p_1 \cdot p_2 \cdot p_3 \ldots p_\nu$, on voit que

$$(1, 0, m) = (1, 0, p_1).(1, 0, p_2).(1, 0, p_3) \ldots (1, 0, p_\nu).$$

Il reste à considérer les complexes entiers de la forme $\left(a_1, \frac{a_2}{g}, 1\right)$. Si l'on pose $a_1 = r_1 \cdot r_2 \cdot \ldots r_\mu$, nous pourrons écrire la décomposition suivante :

$$\left(a_1, \frac{a_2}{g}, 1\right) = \left(r_1, \frac{x_1}{g}, 1\right).\left(r_2, \frac{x_2}{g}, 1\right) \ldots \left(r_\mu, \frac{x_\mu}{g}, 1\right)$$

où les r_λ sont des nombres premiers ou des puissances de nombres premiers. Les entiers $x_1, x_2, \ldots, x_\mu$ s'obtiennent sans difficulté, de proche en proche.

La décomposition en complexes premiers d'un complexe entier quelconque donné a *est donc toujours possible.*

59. — *Cette décomposition* d'un complexe entier donné en facteurs irréductibles *n'est pas nécessairement univoque.* Par exemple, le complexe entier $a = 625 e_1 + \frac{275}{g} e_2 + e_3$ peut se décomposer, et de plusieurs manières, soit en un produit de deux, soit en un produit de trois facteurs premiers :

$$\begin{aligned}
625 e_1 + \frac{275}{g} e_2 + e_3 &= \left(25 e_1 + \frac{2}{g} e_2 + e_3\right) \cdot \left(25 e_1 + \frac{9}{g} e_2 + e_3\right) \\
&= \left(25 e_1 + \frac{3}{g} e_2 + e_3\right) \cdot \left(25 e_1 + \frac{8}{g} e_2 + e_3\right) \\
&= \left(25 e_1 + \frac{4}{g} e_2 + e_3\right) \cdot \left(25 e_1 + \frac{7}{g} e_2 + e_3\right) \\
&= (5 e_1 + e_3)^2 \cdot \left(25 e_1 + \frac{11}{g} e_2 + e_3\right) \\
&= \left(5 e_1 + \frac{1}{g} e_2 + e_3\right)^2 \cdot \left(25 e_1 + \frac{1}{g} e_2 + e_3\right) \\
&= (5 e_1 + e_3) \cdot \left(5 e_1 + \frac{1}{g} e_2 + e_3\right) \cdot \left(25 e_1 + \frac{6}{g} e_2 + e_3\right) \\
&= (5 e_1 + e_3) \cdot \left(5 e_1 + \frac{2}{g} e_2 + e_3\right) \cdot \left(25 e_1 + \frac{1}{g} e_2 + e_3\right) \\
&= \text{etc.}
\end{aligned}$$

Toutes ces décompositions ne contiennent que des facteurs irréductibles et sont essentiellement différentes entre elles.

En général, p désignant un nombre premier naturel, la décomposition du complexe entier $p^2 e_1 + \frac{ap}{g} e_2 + e_3$ est plurivoque, dès que $a > 1$, puisqu'on a

$$\left(p^2, \frac{ap}{g}, 1\right) = (p, 0, 1) \cdot \left(p, \frac{a}{g}, 1\right) = \left(p, \frac{1}{g}, 1\right) \cdot \left(p, \frac{a-1}{g}, 1\right)$$
$$= \left(p, \frac{2}{g}, 1\right) \cdot \left(p, \frac{a-2}{g}, 1\right) = \ldots = \left(p, \frac{b}{g}, 1\right) \cdot \left(p, \frac{a-b}{g}, 1\right).$$

A plus forte raison, la décomposition de

$$p^{n+k} e_1 + \frac{mp^n}{g} e_2 + e_3$$

en facteurs irréductibles est-elle plurivoque, quand $m > 1$.

60. — On sait qu'une constatation analogue faite dans un autre domaine (dans un système de nombres complexes à deux coordonnées indépendantes, appartenant à un corps dérivé d'une racine de l'unité) a amené le mathématicien *E. E. Kummer* à créer ses *nombres idéaux*. Voyant que la décomposition d'un complexe entier en facteurs premiers était plurivoque, il imagina, pour faire disparaître cette anomalie, de considérer ces facteurs premiers eux-mêmes non plus comme irréductibles, mais comme décomposables encore en d'autres éléments ; or, comme ces derniers, les éléments vraiment irréductibles, ne se trouvent en réalité pas dans le système qu'il envisageait, *Kummer* les a créés de toutes pièces, par la pensée, en posant des définitions appropriées. A ces entités logiques créées par pure convention et pour des besoins de simplification, *Kummer* appliqua le nom de *nombres ;* et pour les distinguer des nombres ou complexes réels dont était composé effectivement le système qu'il étudiait, *Kummer* les appela « nombres *idéaux* » (le mot de « nombres imaginaires » ayant déjà une signification fort différente). De cette façon, *Kummer* a considérablement élargi le domaine de nombres qu'il étudiait, en lui *adjoignant* une infinité d'éléments nouveaux dits « nombres idéaux », parmi

lesquels se trouvent les nombres vraiment irréductibles, c'est-à-dire indécomposables. *Kummer* a, naturellement, posé d'une façon très judicieuse les conventions auxquelles étaient censés obéir ses « nombres idéaux », de sorte qu'il réussit à démontrer que, dans ce domaine agrandi, on peut ériger une arithnomie régulière, semblable en tous points à celle construite par *Gauss* dans le système des nombres $a + bi$.

Des rapprochements suggestifs ont été faits entre les nombres idéaux de cette arithnomie et certains radicaux ou éléments chimiques dont l'existence a été postulée par la théorie bien avant d'être confirmée par l'expérience; tout comme ces radicaux de la chimie, les facteurs idéaux de *Kummer* n'apparaissent jamais à l'état isolé, mais figurent « à l'état de combinaison » dans les complexes entiers (v. « Journal f. d. reine u. angew. Mathematik » fondé par *Crelle*, vol. 35, p. 360).

61. — Les théorèmes de décomposition valables dans le domaine des quaternions entiers et des tettarions entiers (v. article 23) pourraient peut-être faire apparaître sous un jour nouveau cette pluralité de possibilités dans la décomposition en facteurs premiers. Soit un tettarion entier c dont la norme $\mathrm{N}(c)$ comprenne quatre facteurs premiers dont deux égaux entre eux, et posons :

$$\mathrm{N}(c) = p_1 \cdot p_2 \cdot p_1 \cdot p_3$$

Ayant arrêté cet ordre de succession des facteurs p_λ, on peut décomposer le tettarion donné c supposé primitif (c'est-à-dire tel que le plus grand commun diviseur de ses coordonnées soit 1) en un produit de quatre tettarions premiers primaires :

$$c = \pi_1 . \pi_2 . \pi_3 . \pi_4$$

où

$$\mathrm{N}(\pi_1) = p_1 \; ; \qquad \mathrm{N}(\pi_2) = p_2 \; ; \qquad \mathrm{N}(\pi_3) = p_1 \; ; \qquad \mathrm{N}(\pi_4) = p_3 \; ,$$

et cette décomposition est unique. Si l'on fixe un autre ordre de succession, qu'on pose par exemple

$$\mathrm{N}(c) = p_2 \cdot p_1 \cdot p_3 \cdot p_1 \; ,$$

on aura une autre décomposition du tettarion donné c en un produit de quatre tettarions premiers primaires :

$$c = \rho_1 \cdot \rho_2 \cdot \rho_3 \cdot \rho_4$$

où

$$\mathrm{N}(\rho_1) = p_2 ; \ \mathrm{N}(\rho_2) = p_1 ; \ \mathrm{N}(\rho_3) = p_3 ; \ \mathrm{N}(\rho_4) = p_1 ,$$

et cette décomposition sera de nouveau unique, c'est-à-dire déterminée sans ambigüité.

Les tettarions premiers ρ_λ seront différents, en général, des tettarions premiers π_λ ; ainsi $\rho_1 \neq \pi_2$, quoique $\mathrm{N}(\rho_1) = \mathrm{N}(\pi_2) = p_2$; de même $\pi_1 \neq \rho_4$, quoique $\mathrm{N}(\pi_1) = \mathrm{N}(\rho_4) = p_1$; etc.

A chaque décomposition de $\mathrm{N}(c)$ en facteurs premiers, ou plutôt à chaque ordre de succession que l'on fixe, arbitrairement du reste, pour ces facteurs premiers p_λ (il y a douze permutations possibles dans cet exemple particulier) correspond une décomposition unique et bien déterminée de c en tettarions premiers primaires, mais ces diverses décompositions de c (au nombre de douze dans l'exemple particulier) ne contiennent pas les mêmes facteurs premiers. Si le produit final est néanmoins toujours le même, c'est-à-dire si

$$\pi_1 \cdot \pi_2 \cdot \pi_3 \cdot \pi_4 = \rho_1 \cdot \rho_2 \cdot \rho_3 \cdot \rho_4 = \sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdot \sigma_4 = \ldots = c$$

c'est parce qu'un produit dépend non seulement de ses facteurs, mais aussi de leur ordre de succession.

Ce théorème reste vrai pour les tritettarions (nous l'avons démontré dans un autre mémoire) ; en d'autres termes : ce théorème reste vrai si c est un complexe à neuf coordonnées (v. article 29) représentable par

$$c = \left\{ \begin{array}{ccc} c_{11} , & c_{12} , & c_{13} \\ c_{21} , & c_{22} , & c_{23} \\ c_{31} , & c_{32} , & c_{33} \end{array} \right\}$$

Or, le système de complexes à trois coordonnées que nous venons d'étudier est un cas particulier des tritettarions (v. article 44). Donc, le théorème de décomposition en fac-

teurs premiers énoncé ci-dessus doit rester applicable, semble-t-il, quelles que soient les coordonnées c_{ik}, pourvu que $N(c) \neq 0$. Or, en prenant en particulier

$$c_{11} = c_{22} = a_1 \ , \quad c_{12} = a_2 \ , \quad c_{33} = a_3 \ , \quad c_{13} = c_{31} = c_{23} = c_{32} = c_{21} = 0 \ ,$$

on obtient précisément le complexe entier $a = \left(a_1 \, . \, \frac{a_2}{1}, \, a_3\right)$ appartenant au domaine que nous étudions depuis l'article 51, en faisant $g = 1$; on doit donc toujours avoir plusieurs possibilités de décomposition :

$$c = a = \pi_1 . \pi_2 . \pi_3 . \pi_4 = \rho_1 . \rho_2 . \rho_3 . \rho_4 = \sigma_1 . \sigma_2 . \sigma_3 . \sigma_4 = \dots \ .$$

Mais maintenant, la multiplication est commutative ; le produit $\pi_1 . \pi_2 . \pi_3 . \pi_4$ qui est égal à c ne dépend plus de l'ordre de succession des facteurs, ni le produit $\rho_1 . \rho_2 . \rho_3 . \rho_4$, ni les autres produits analogues. Il en résulte du même coup que la décomposition de c en facteurs premiers n'est plus univoque, puisqu'en général, les ρ_λ sont différents des π_λ, différents aussi des σ_λ, etc.

62. — De plus, ces réflexions semblent indiquer que la multiplicité de décomposition tient à la commutativité de la multiplication et provient d'elle, tandis que l'unicité de décomposition tient à la non-commutativité de la multiplication. Ces considérations nous ont amené à rechercher si, dans *tous* les systèmes de nombres hypercomplexes, la décomposition d'un complexe entier donné en facteurs premiers est plurivoque ou unique, selon que la multiplication, dans le système en question, est commutative, ou ne l'est pas.

Quelques faits paraissent militer en faveur de cette thèse : c'est d'abord un théorème fondamental qui repose sur l'importante notion de *système simple* introduite par MM. *E. Cartan* et *Th. Molien ;* ce théorème dit que tous les systèmes « simples » de nombres hypercomplexes à multiplication associative, où l'égalité et l'addition de deux complexes sont définis par l'égalité et l'addition de leurs coordonnées correspondantes, constituent des sous-systèmes, donc des cas particuliers, de certains systèmes de tettarions. C'est ensuite le fait qu'un système de polytettarions à ρ^2 coordonnées

entre lesquelles existent n relations n'est autre chose, en réalité, qu'un système de nombres hypercomplexes à $(\mu^2 - n)$ unités relatives. Il semble même que les polytettarions ou μ-tettarions ($\mu = 2, 3, 4, 5, \ldots$) contiennent, comme cas particuliers, tous les systèmes possibles de nombres hypercomplexes à multiplication associative, c'est-à-dire où la relation $(a.b).c = a.(b.c)$ est toujours satisfaite; il semble, dis-je, qu'il suffise d'établir des liaisons appropriées entre les coordonnées d'un système de μ-tettarions pour obtenir, à l'écriture près, tel système qu'on voudra de nombres hypercomplexes à multiplication associative. Par exemple, les nombres complexes de *Gauss* sont un cas particulier des duotettarions; les quaternions sont un sous-système particulier des tetratettarions, et ainsi de suite. Des propositions ci-dessus ressort en tout cas l'importance très grande des tettarions dans la théorie générale des systèmes de nombres hypercomplexes.

63. — Revenons au domaine [H] formé par l'ensemble des complexes *entiers* $x = x_1 e_1 + \frac{x_2}{g} e_2 + x_3 e_3 = \left(x_1, \frac{x_2}{g}, x_3\right)$, où les x_λ sont des nombres entiers variant de $-\infty$ à $+\infty$, et g un nombre entier fixe (v. **51**). Que devient, dans ce domaine [H], la théorie du plus grand commun diviseur ? Voici ce que l'on peut démontrer sans grande difficulté : deux complexes entiers donnés, $a = \left(a_1, \frac{a_2}{g}, a_3\right)$ et $b = \left(b_1, \frac{b_2}{g}, b_3\right)$, possèdent « en général » un plus grand commun diviseur, unique et bien déterminé si l'on ne considère que les entiers primaires (v. **55**) ; de plus, il existe un procédé analogue à l'algorithme d'Euclide permettant de déterminer ce plus grand commun diviseur par un nombre fini d'opérations rationnelles.

Mais ce théorème « général » présente ici (comme dans le cas des quaternions entiers *lipschitziens*, v. articles 9 et 12), des exceptions déconcertantes. Elles sont même si nombreuses qu'on peut se demander si le théorème énoncé ci-dessus n'est pas plutôt un théorème exceptionnel (nous le qualifions de « général », parce que son analogue est vrai, sans exception, dans l'arithmétique classique). D'abord, dans certains cas, l'algorithme d'Euclide ne conduit pas au

but : à mi-chemin, il cesse d'être applicable ; cela arrive, par exemple, lorsque a_1 et a_3, coordonnées extrêmes de a, sont des multiples de $\mathrm{N}(b)$ et qu'en même temps a_2 n'est pas divisible par $\mathrm{N}(b)$. Ensuite et surtout, un *plus grand* commun diviseur au sens habituel de ce terme n'existe pas toujours. En fait de démonstration, donnons un exemple numérique facilement généralisable.

Les complexes entiers

$$a = \left(25e_1 + \frac{20}{g}e_2 + e_3\right) \qquad \text{et} \qquad b = \left(25e_1 + \frac{15}{g}e_2 + e_3\right)$$

ont même norme : $\mathrm{N}(a) = \mathrm{N}(b) = 625$, sans cependant être associés. Les égalités

$$\begin{aligned} a &= \left(5e_1 + \frac{2}{g}e_2 + e_3\right)^2 \\ &= \left(5e_1 + \frac{1}{g}e_2 + e_3\right)\cdot\left(5e_1 + \frac{3}{g}e_2 + e_3\right) \\ &= (5e_1 + e_3)\cdot\left(5e_1 + \frac{4}{g}e_2 + e_3\right) ; \\ b &= (5e_1 + e_3)\cdot\left(5e_1 + \frac{3}{g}e_2 + e_3\right) \\ &= \left(5e_1 + \frac{1}{g}e_2 + e_3\right)\cdot\left(5e_1 + \frac{2}{g}e_2 + e_3\right) \end{aligned}$$

montrent que ces complexes a et b possèdent quatre communs diviseurs, tous quatre entiers et non associés, donc essentiellement différents entre eux, à savoir :

$$d_0 = 5e_1 + e_3 \qquad ; \qquad d_2 = 5e_1 + \frac{2}{g}e_2 + e_3$$

$$d_1 = 5e_1 + \frac{1}{g}e_2 + e_3 \; ; \qquad d_3 = 5e_1 + \frac{3}{g}e_2 + e_3 \; .$$

Si a et b possédaient un *plus grand commun* diviseur d, on devrait avoir : d'une part $\begin{cases} a = f.d \\ b = h.d \end{cases}$ où f et h seraient certains complexes entiers, d'autre part

$$d = d_0.\delta_0 = d_1.\delta_1 = d_2.\delta_2 = \delta_3.d_3 \; ,$$

les δ_λ représentant certains complexes entiers, puisque *le plus grand commun* diviseur d, devant contenir comme facteurs tous les autres communs diviseurs, devrait être divisible par d_0, d_1, d_2 et d_3. Comme $N(a) = N(d).N(f) = 625$, il n'y a que les 5 possibilités suivantes : $N(d) = 1$, ou $= 5$, ou $= 25$, ou $= 125$, ou $= 625$. Mais $N(d) = 625$ est exclu, car il s'ensuivrait que a et b seraient associés, ce qui n'est pas le cas. Les égalités

$$N(d) = N(d_0).N(\delta_0) = N(d_1).N(\delta_1) = N(d_2).N(\delta_2) = N(d_3).N(\delta_3)$$

excluent les hypothèses $N(d) = 1$ et $N(d) = 5$, puisque $N(d_0) = N(d_1) = N(d_2) = N(d_3) = 25$; si $N(d) = 25$, il s'ensuivrait que, les δ_λ étant des unités, d_0, d_1, d_2 et d_3 seraient associés, ce qui n'est pas le cas. Il ne reste ainsi plus à examiner que la dernière hypothèse, savoir : $N(d) = 125$; il s'ensuivrait $N(f) = 5$; donc f, étant un complexe entier, serait nécessairement de la forme $f = (1, \frac{x}{g}, 5)$. De l'égalité $a = f.d$, on tirerait, en écrivant $d = \left(d_1', \frac{d_2'}{g}, d_3'\right)$:

$$\left(25, \frac{20}{g}, 1\right) = \left(1, \frac{x}{g}, 5\right).\left(d_1', \frac{d_2'}{g}, d_3'\right), \qquad \text{d'où} \qquad 1 = 5.d_3'$$

ce qui est impossible en nombres entiers. Donc enfin, l'hypothèse d'un *plus grand* commun diviseur d de a et b conduit nécessairement à une contradiction. Et voilà deux complexes entiers a et b ayant quatre diviseurs communs bien différents entre eux, mais ne possédant, néanmoins, aucun *plus grand* commun diviseur, au sens qu'a ce terme dans l'arithmétique ordinaire.

Dès lors, il n'est plus vrai qu'un complexe *premier* qui divise un produit de deux facteurs divise nécessairement l'un de ces facteurs. Par exemple, les égalités ci-dessus prouvent que le complexe entier $5e_1 + \frac{4}{g}e_2 + e_3$ qui est irréductible dans ce domaine et qui ne divise ni d_1, ni d_3, divise cependant le produit $d_1.d_3 = a$. Enfin, quoique les complexes entiers $d_2 = 5e_1 + \frac{2}{g}e_2 + e_3$ et $d_3 = 5e_1 + \frac{3}{g}e_2 + e_3$,

tous deux irréductibles dans ce domaine, soient *premiers entre eux* (c'est-à-dire admettent comme plus grand commun diviseur 1), leurs cinquièmes puissances,

$$d_2^5 = 3\,125e_1 + \frac{6\,250}{g}e_2 + e_3 \qquad \text{et} \qquad d_3^5 = 3\,125e_1 + \frac{9\,375}{g}e_2 + e_3\ ,$$

ne le sont point et admettent le diviseur commun $3\,125e_1 + e_3$.

Ainsi se trouve confirmée la présomption émise à la fin de l'article 51, à savoir que l'arithnomie du corps de nombres $\{K\}$ basée sur la définition XI ne serait probablement pas « régulière », parce que la dite définition du complexe *entier* engendre un domaine holoïde [H] non maximal.

64. — Toutes les déductions précédentes restent valables, si l'on remplace $\frac{1}{g}$ par un nombre rationnel γ non nul, du reste arbitraire. Faisons remarquer que plus le nombre entier g contient de diviseurs, plus le domaine holoïde [H] correspondant enveloppera de complexes rationnels. On peut donc agrandir indéfiniment le contenu du domaine [H], ou, pour employer une image empruntée à la physique, y « comprimer » des complexes rationnels de plus en plus nombreux. Si l'on choisit, au contraire, pour γ un nombre entier m, on pourra diminuer indéfiniment l'ensemble des complexes rationnels faisant partie de [H], en prenant pour m un nombre de plus en plus grand ; on a donc la possibilité (pour employer la même image que tout à l'heure) de « faire le vide » de plus en plus complètement dans l'ensemble [H]. Mais, qu'on augmente ou qu'on diminue le contenu de cet ensemble, l'arithnomie dont nous avons esquissé ci-dessus la partie élémentaire ne changera pas essentiellement, le domaine holoïde non maximal [H] restera toujours non maximal.

Pour faire disparaître les singularités dont nous avons signalé quelques-unes, il faut avoir recours à des procédés plus profonds.

65. — En principe, deux voies bien différentes s'offrent au mathématicien. *La première* consiste à maintenir les mêmes définitions : de la divisibilité, du commun diviseur, du nombre premier, etc., mais à *élargir l'ensemble* [H] que l'on étudie. On peut y arriver de deux façons : 1° en définis-

sant différemment le nombre hypercomplexe rationnel « entier » dans le corps de tous les complexes rationnels ; cette manière de faire est due à M. *A. Hurwitz* qui l'appliqua pour la première fois au système des quaternions ; 2° en créant, par des définitions judicieuses, des entités logiques soumises à des lois appropriées, entités que l'on appellera, par extension, des « nombres » et que l'on adjoindra à [H] ; cette manière de procéder est due à *Kummer* (v. article 60).

La deuxième voie consiste à suivre une marche en quelque sorte inverse de la précédente : on maintient tel quel le domaine [H] que l'on étudie, on ne l'élargit point, mais on *change les définitions* de la divisibilité, du commun diviseur, du « nombre premier », etc. Le changement le plus radical provient de ce que, dans les nouvelles définitions, l'on n'envisage guère un nombre ou un complexe isolément, mais plutôt *des ensembles* composés d'une infinité de complexes, et que l'on opère avec ces ensembles de complexes au lieu d'opérer avec des complexes isolés. Cette voie fut ouverte par *J.-W. Richard Dedekind*. — *R. Dedekind* désigne par des lettres gothiques minuscules : $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, $\mathfrak{e}$... ces ensembles particuliers auxquels il donna le nom d'*idéaux*, nom critiquable peut-être, mais qui a acquis droit de cité dans la théorie moderne des nombres. L'idée géniale du célèbre mathématicien revient à ceci : prendre comme sujet direct d'étude, au lieu de l'entier considéré a, l'ensemble de ses multiples $g.a$; cet ensemble forme « *l'idéal principal* de l'entier a ». A ces idéaux principaux, *Dedekind* a joint des idéaux secondaires ; ce sont de nouvelles familles de nombres déduites des précédentes par voie d'addition. La définition générale d'un idéal peut s'énoncer ainsi :

Définition XII : Un *idéal* $\mathfrak{a}$ est un ensemble formé d'une infinité de nombres entiers ordinaires ou de nombres hypercomplexes *entiers*, dits *les éléments* de l'idéal $\mathfrak{a}$, ensemble jouissant des deux propriétés suivantes : 1° les éléments de l'idéal se reproduisent par addition et soustraction ; 2° si x est un élément quelconque de l'idéal $\mathfrak{a}$, le produit $g.x$, où g représente un complexe entier quelconque, est aussi contenu dans cet idéal $\mathfrak{a}$.

En vertu de cette définition, un idéal a contenant les deux éléments a et b différents entre eux, contient nécessairement aussi $a+b$, $a-b$, $g.a$, $g.b$, où g est un complexe entier quelconque pouvant lui-même faire partie, ou non, de l'idéal en question. On démontre alors que tout idéal possède une base finie (v. articles 16 et 17).

On définit ce qu'il faut entendre par le produit et par le quotient de deux idéaux a et b, ce qu'est un idéal « premier », un idéal « composé », un diviseur d'idéal, le plus grand commun diviseur de deux idéaux, et ainsi de suite.

Ceci montre que l'arithnomie du domaine [H] que l'on veut étudier devient un calcul avec des idéaux, au lieu d'être un calcul avec des nombres ordinaires ou avec des complexes entiers. Mais ces *idéaux* au sens de *Dedekind* (et contrairement aux « nombres *idéaux* » de *Kummer*) ne sont plus des abstractions; ce sont des ensembles tout aussi réels, tout aussi effectifs, que les nombres hypercomplexes eux-mêmes dont ils sont constitués. Tel est le principe de la méthode de *Dedekind*, permettant d'étudier le domaine holoïde [H] sans modifier ce domaine.

La méthode employée par *E. E. Kummer* est tout autre. Elle modifie très profondément le domaine holoïde [H] à étudier, puisqu'elle lui adjoint une infinité de « nombres idéaux » qui, au fond, ne s'y trouvent pas du tout. Ces nombres idéaux rappellent un peu les *points imaginaires* et les *droites imaginaires* des géomètres quand ils disent, par exemple, que deux circonférences dont l'une est entièrement intérieure à l'autre se coupent, néanmoins, en deux (voire même en quatre) points *imaginaires* et que ces mêmes circonférences ont quatre tangentes communes, mais *imaginaires*. Les *nombres idéaux* de la méthode de *Kummer*, comme les *figures imaginaires* de la géométrie, touchent à ce qu'on pourrait appeler la « métamathématique » (par analogie à « métaphysique ») et restent impénétrables à beaucoup d'esprits. La méthode de *Kummer* est du reste d'une application moins facile que la théorie des idéaux, car on ne voit pas toujours du premier coup d'œil quelles sont les définitions qu'il faut poser pour créer de façon appropriée les « nombres idéaux ».

Les deux voies, si différentes en principe, celle de *E. E. Kummer* et celle de *R. Dedekind,* peuvent conduire au même résultat : faire tomber les singularités que présente l'arithnomie de certains domaines holoïdes.

66. — Résumons en disant: la définition *lipschitzienne* du nombre hypercomplexe *entier* a l'avantage d'être toujours applicable et toujours univoque (v. définition V) ; mais elle est en quelque sorte superficielle, en ce sens qu'en l'adoptant, on ne tient compte que de la nature des coordonnées, sans aucun égard aux règles qui définissent le système envisagé de nombres hypercomplexes. Malgré l'avantage d'être toujours applicable et univoque, elle doit être rejetée comme pouvant conduire à des arithnomies non régulières.

La manière *hurwitzienne* de définir le nombre hypercomplexe *entier* est plus profonde (v. définition IX, art. 24), en ce sens qu'en l'adoptant, on tient compte non seulement de la nature des coordonnées, mais des propriétés intrinsèques du système envisagé de nombres hypercomplexes, puisqu'on doit rechercher un domaine holoïde *maximal* et qu'il n'est pas possible de le déterminer sans se servir des règles qui définissent le système en question. Aussi la définition *hurwitzienne* conduit-elle à des arithnomies régulières là où la définition *lipschitzienne* reste en défaut.

Par contre, la définition *hurwitzienne* a l'inconvénient de ne pas être toujours univoque, et surtout celui de ne pas pouvoir s'appliquer à tous les cas, puisqu'il existe des corps de nombres sans domaine holoïde maximal. Pour étudier ces systèmes de nombres, on se sert avec avantage de la *méthode des idéaux.* Elle consiste à modifier les définitions de façon à ne plus avoir, dans la théorie de la divisibilité, à calculer avec des nombres entiers isolés, mais avec des idéaux. Cette méthode permet d'écarter les obstacles qui pendant longtemps ont obstrué l'entrée d'une immense région : l'arithnomie des nombres complexes généraux.

Neuchâtel, octobre 1915.