SUR

L'ARITHNOMIE DES NOMBRES DE WEIERSTRASS GÉNÉRALISÉS

ET DE

QUELQUES SYSTÈMES DE POLYTETTARIONS COMPLEXES

THÈSE

PRÉSENTÉE A LA FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE NEUCHATEL
POUR OBTENIR LE GRADE DE DOCTEUR ÈS SCIENCES

PAR

BORIS SEITZ

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES

La présente publication est un extrait de la thèse ci-dessus.
Le manuscrit dans son intégrité est déposé à l'Université de Neuchâtel.

LAUSANNE
IMPRIMERIE LA CONCORDE
1926

La Faculté des Sciences de l'Université de Neuchâtel, sur le rapport de M. L.-G. Du Pasquier, autorise l'impression de la présente thèse, sans exprimer d'opinion sur les propositions qui y sont contenues.

Neuchâtel, juin 1926.

Le Doyen:
O. Fuhrmann.

A mon cher professeur

Monsieur L.-Gustave Du Pasquier,

Hommage d'affectueuse reconnaissance.

Boris Seitz.

L'idée du présent travail m'a été suggérée par

Monsieur le professeur L.-GUSTAVE DU PASQUIER.

Je tiens à lui exprimer ici ma vive gratitude pour les conseils qu'il a bien voulu me donner et pour l'intérêt qu'il m'a toujours témoigné au cours de mes travaux.

BORIS SEITZ.

SUR L'ARITHNOMIE DES NOMBRES DE WEIERSTRASS GÉNÉRALISÉS ET DE QUELQUES SYSTÈMES DE POLYTETTARIONS COMPLEXES

INTRODUCTION

Gauss, dans un passage célèbre d'un de ses travaux, a posé la question : *Pourquoi les relations entre les objets qui représentent une multiplicité à plus de deux dimensions ne peuvent-elles pas fournir de nouvelles espèces de quantités admissibles en arithmétique générale ?* Gauss n'a jamais publié ses recherches sur ce sujet. Weierstrass, reprenant la question posée par Gauss, la ramenait à cette autre : *une nouvelle extension de la notion de nombre est-elle possible ?* Il en donna la solution connue : *La nouvelle extension n'est possible qu'au prix de l'abandon d'une ou de plusieurs propriétés fondamentales des opérations de l'algèbre ordinaire.* En s'occupant de cette question, Weierstrass a recherché quels systèmes de nombres obéissent *le plus possible* aux lois de l'algèbre ordinaire. Dans un cours donné en 1863 à l'Univresité de Berlin, il a considéré des systèmes où une seule des lois classiques est abandonnée : un produit de deux facteurs peut s'annuler sans qu'aucun des facteurs ne soit nul. Ces systèmes, étudiés depuis lors par plusieurs auteurs, ont été retrouvés par M. le professeur L.-G. Du Pasquier comme cas particuliers d'un système très général de nombres hypercomplexes, qu'il appelle *polytettarions* ou m - tettarions. Dans ses recherches, M. Du Pasquier est arrivé à la conclusion que les polytettarions embrassent, comme cas particuliers, tous les systèmes possibles de nombres hypercomplexes à addition associative, commutative et à multiplication associative liée à l'addition par les lois distributives. En particulier, les nombres de Weierstrass ne sont autre chose que des m - tettarions diagonaux (ce terme sera défini plus bas).

M. Du Pasquier m'a proposé d'étudier l'arithnomie des nombres de Weierstrass généralisés, en supposant leurs coordonnées tirées du corps $K(\sqrt{a}, \sqrt{b})$, où a et b représentent deux entiers ordinaires positifs ou négatifs, puis de chercher à étendre au cas des polytettarions quelconques, à coordonnées tirées du même corps $K(\sqrt{a}, \sqrt{b})$, les résultats obtenus pour les nombres de Weierstrass. Dans le cas des nombres de Weierstrass, où la multiplication est commutative, les théorèmes classiques de la théorie des nombres algébriques se prêtent à la généralisation. En passant au cas des polytettarions quelconques, à coordonnées tirées du corps $K(\sqrt{a}, \sqrt{b})$, j'ai pu

malgré la non-commutativité de la multiplication, étendre les théorèmes principaux à une catégorie spéciale, celle des polytettarions complexes réduits (ce terme sera défini au ch. V). Quant aux polytettarions complexes non réduits, la non-commutativité de la multiplication semble empêcher d'y appliquer les méthodes classiques. Voici une esquisse de la marche suivie et des principaux résultats obtenus.

Le présent mémoire comprend deux parties ; la première (ch. I, II, III et IV) est consacrée aux nombres de Weierstrass, la seconde (ch. V) aux polytettarions réduits. Après avoir rappelé quelques définitions concernant les nombres de Weierstrass et le corps $K(\sqrt{a}, \sqrt{b})$, j'aborde le sujet de mon travail : l'étude du corps Ω_d des diagonaux complexes, c'est-à-dire des nombres de Weierstrass à coordonnées tirées du corps $K(\sqrt{a}, \sqrt{b})$. L'indice d, dans Ω_d, rappellera qu'il s'agit de nombres diagonaux. La théorie des idéaux permet d'édifier dans ce corps Ω_d une arithnomie semblable à celle des corps algébriques. En généralisant un théorème de Minkowski sur les formes linéaires, j'aboutis facilement au théorème de l'unicité de la décomposition des idéaux dans le corps Ω_d. Le deuxième chapitre est consacré à l'étude des congruences suivant un idéal. Je généralise les notions de *norme* et d'*indicateur* aux idéaux du corps Ω_d. Je démontre que les théorèmes fondamentaux de la théorie classique des congruences restent vrais dans le corps étudié, entre autres le théorème de Fermat avec ses conséquences. De même qu'un nombre premier naturel se décompose dans les corps algébriques, de même un nombre de Weierstrass rationnel premier se décompose dans le corps Ω_d des diagonaux complexes. C'est cette question que je traite dans le chapitre III. J'arrive au théorème suivant : pour décomposer dans le corps Ω_d un nombre diagonal rationnel premier, il suffit de décomposer ses coordonnées dans le corps $K(\sqrt{a}, \sqrt{b})$. Les résultats de ce chapitre me permettent de calculer le nombre des classes d'idéaux du corps Ω_d en fonction de celui du corps $K(\sqrt{a}, \sqrt{b})$. Dans le chapitre IV, j'étudie les unités du corps Ω_d. Dans la deuxième partie de mon travail, j'ai cherché à généraliser les résultats susmentionnés au cas du corps Ω des polytettarions réduits à gauche. Du reste, la théorie développée s'appliquerait intégralement au corps des polytettarions réduits à droite, si l'on modifiait d'une manière appropriée les définitions posées [1]. Dans le domaine des polytettarions réduits à gauche, il y a lieu de distinguer deux arithnomies, se développant parallèlement : une arithnomie à gauche, et une arithnomie à droite. Dans mon travail, je n'ai traité que l'arithnomie à droite. On pourrait ériger deux arithnomies analogues dans le domaine des polytettarions réduits à droite. Après plusieurs essais, j'ai vu qu'on pouvait beaucoup simplifier les démonstrations, sans changer les résultats, en modifiant 1° la définition de l'idéal et 2° celle du produit de deux idéaux. Je démontre que la définition modifiée de l'idéal est équivalente à celle de Dedekind, à condition toutefois de faire la distinction entre *idéaux à droite* et *idéaux à gauche*. Ceux que je définis sont des idéaux à droite (dans le corps des polytettarions réduits à gauche). On pourrait développer dans le même corps de nombres, une théorie analogue pour les idéaux à gauche. Dans le cours de mon travail, j'appelle idéaux, tout court, ceux que j'introduis, sans insister sur le fait que ce sont des idéaux à droite. Ma définition étant plus générale que celle posée

[1] L.-G. Du Pasquier. *Zahlentheorie der Tettarionen*. page 16.

par Dedekind, il fallait éviter une confusion possible avec l'idéal dans le sens classique. C'est pourquoi j'ajoute le qualificatif de *diagonal* pour distinguer le nouvel être mathématique : l'idéal diagonal. La définition nouvelle du produit de deux idéaux diffère de la définition ordinaire en ce que le produit de deux idéaux ne contient pas nécessairement tous les produits des nombres appartenant aux idéaux facteurs. Elle se justifie par un double fait : d'abord, elle coïncide avec la définition de Dedekind, dès que l'on passe du corps des polytettarions réduits à gauche au sous-corps des nombres diagonaux ; ensuite elle rend la multiplication des idéaux commutative, ce qui simplifie beaucoup la théorie de la décomposition en facteurs premiers et celle des congruences. J'appellerai *produit diagonal* ce nouveau genre de produits d'idéaux, afin d'éviter la confusion avec le produit idéal dans le sens classique. Les nouvelles définitions que je viens de mentionner me permettent de démontrer le théorème de la décomposition univoque des nombres diagonaux dans le corps Ω des polytettarions réduits, et par suite aussi la décomposition des polytettarions réduits complexes du même corps en un produit d'unités et de facteurs premiers du corps. Dans la théorie des congruences suivant un idéal, je montre quelles anomalies proviennent de la non-commutativité de la multiplication des tettarions et quels sont les théorèmes qui, malgré cette non-commutativité, subsistent dans le corps Ω. J'étudie enfin les unités de ce corps.

Dans mes recherches, je me suis basé principalement sur les travaux suivants :

L.-G. Du Pasquier, *Zahlentheorie der Tettarionen*, Vierteljahrsschrift. d. Naturf. Ges. in Zürich. Jahrgang 51. Zürich 1906.

L.-G. Du Pasquier, *Sur l'arithmétique des nombres hypercomplexes*. L'enseignement math. t. 18. Genève 1916.

L.-G. Du Pasquier, *Zur Theorie der Tettarionenideale*, Vierteljahrsch. der Naturf. Gesel. in Zürich. Jahrg. 52. Zürich 1907.

D. Hilbert, traduit de l'allemand par A. Lévy et Th. Got, *Théorie des corps de nombres algébriques*. Paris 1913.

J. Sommer, traduit de l'allemand par A. Lévy, *Introduction à la théorie des nombres algébriques*. Paris 1911.

E.-J. Amberg, *Ueber den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen*. Inaugur. Dissertation. Zürich 1897.

E. Cahen, *Théorie des nombres*. Tome II : Le second degré. Paris 1924.

Encyclopédie des sciences mathématiques pures et appliquées. Tome I, volume 1, fascicule 3. Paris et Leipzig 1908, et tome I, volume 2, fascicule 2. Paris et Leipzig 1910.

DEUXIÈME PARTIE

LE CORPS Ω DES POLYTETTARIONS COMPLEXES RÉDUITS A GAUCHE

§ 1. Définitions préliminaires.

1. Nous appellerons m — *tettarion* ou *polytettarion* un ensemble de m^2 nombres a_{rs}, rangés en un tableau carré de m lignes et m colonnes, soit [1] :

$$A \equiv \left\{ \begin{array}{l} a_{11},\ a_{12},\ a_{13},\ \ldots\ldots,\ a_{1m} \\ a_{21},\ a_{22},\ a_{23},\ \ldots\ldots,\ a_{2m} \\ a_{31},\ a_{32},\ a_{33},\ \ldots\ldots,\ a_{3m} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1},\ a_{m2},\ a_{m3},\ \ldots\ldots,\ a_{mm} \end{array} \right\} \equiv \left\{ a_{rs} \right\}. \qquad (1)$$

Un polytettarion dont toutes les coordonnées situées d'un même côté de la diagonale principale sont nulles, est dit *réduit*. Il est *réduit à gauche* ou *réduit à droite* suivant que les coordonnées nulles se trouvent à gauche ou à droite de la diagonale principale. Par exemple, le polytettarion

$$\left\{ \begin{array}{l} a_{11},\ a_{12},\ a_{13},\ \ldots\ldots,\ a_{1m} \\ 0\ ,\ a_{22},\ a_{23},\ \ldots\ldots,\ a_{2m} \\ 0\ ,\ 0\ ,\ a_{33},\ \ldots\ldots,\ a_{3m} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 0\ ,\ 0\ ,\ 0\ ,\ \ldots\ldots,\ a_{mm} \end{array} \right\}$$

est réduit à gauche.

Un polytettarion qui est à la fois réduit à gauche et réduit à droite est dit *polytettarion diagonal* ou *nombre diagonal*, par exemple

$$A \equiv \left\{ \begin{array}{l} a_{11},\ 0,\ \ldots\ldots,\ 0 \\ 0,\ a_{22},\ \ldots\ldots,\ 0 \\ \ldots\ldots\ldots\ldots \\ 0,\ 0,\ \ldots\ldots,\ a_{mm} \end{array} \right\} \equiv \left\{ a_{rr} \right\} \equiv \left\{ a_r \right\}.$$

[1] Le signe ≡ (doublement égal) signifie *égal par définition*.

Nous représenterons le polytettarion diagonal A symboliquement comme suit:

$$A \equiv \{ a_1, a_2, a_3, \ldots, a_m \} \equiv \{ a_r \}$$

En particulier si $a_1 = a_2 = \ldots = a_m$ le tettarion diagonal est dit *scalaire.*

Egalité. — Deux polytettarions sont dits *égaux*, si les coordonnées correspondantes le sont.

Addition. — La somme des deux polytettarions, $A = \{ a_{rs} \}$ et $B = \{ b_{rs} \}$, est le tettarion $C = \{ c_{rs} \}$ de coordonnées $c_{rs} \equiv a_{rs} + b_{rs}$. L'addition ainsi définie est commutative et associative. Elle a un module. C'est le tettarion dont toutes les coordonnées sont nulles. Il est appelé *polytettarion nul* ; on le représente par 0.

Soustraction. — La différence des deux tettarions, $A = \{ a_{rs} \}$ et $B = \{ b_{rs} \}$, est le tettarion $C = \{ c_{rs} \}$ de coordonnées $c_{rs} \equiv a_{rs} - b_{rs}$.

En additionnant k fois de suite un polytettarion $A = \{ a_{rs} \}$ à lui-même, on constate que les coordonnées de la somme ainsi obtenue sont $k.a_{rs}$. On est conduit à généraliser ce résultat au cas où k cesse d'être un nombre naturel et à poser la définition suivante :

Pour multiplier un tettarion $A = \{ a_{rs} \}$ par un nombre réel ou complexe quelconque k, il faut multiplier par k chacune des coordonnées de A.

Unités relatives. — On appelle *unité relative*, et on désigne par e_{rs}, un polytettarion dont 1) toutes les coordonnées, sauf une, sont nulles ; 2) la coordonnée non nulle est égale à 1 et se trouve à l'intersection de la $r^{ième}$ ligne et de la $s^{ième}$ colonne.

Multiplication. — La multiplication des tettarions entre eux se fait d'après la même règle que la composition des substitutions linéaires. Le tettarion $C = \{ c_{rs} \}$ est le produit de $A = \{ a_{rs} \}$ par $B = \{ b_{rs} \}$ et l'on écrira

$$A.B = C \quad \text{si} \quad c_{rs} \equiv \sum_{k}^{1 \ldots m} a_{rk} . b_{ks} .$$

La multiplication ainsi définie est associative et liée à l'addition par les deux lois de distributivité résumées par les formules :

$$A.(B + C) = A.B + A.C \quad \text{et} \quad (B + C).A = B.A + C.A$$

La multiplication des polytettarions n'est pas commutative en général. Si $A.B = B.A$, on dit que ces deux tettarions sont *permutables.* La multiplication possède un module : c'est le nombre diagonal $\{ 1, 1, \ldots, 1 \} = \sum_{r}^{1 \ldots m} e_{rr}$ appelé *polytettarion principal* et représenté par 1.

Il suit de là que le corps des tettarions à coordonnées réelles contient comme sous-groupe les nombres réels. Quand les coordonnées des tettarions sont elles-mêmes des nombres complexes tirés d'un corps algébrique K, comme nous le supposerons plus

bas, le corps formé par ces tettarions contiendra comme sous-groupe le corps K. Un nombre α de ce corps K peut en effet se mettre sous la forme d'un polytettarion scalaire

$$\alpha = \alpha \,.\, \sum e_{rr} = \sum \alpha \,.\, e_{rr} = \{\alpha, \alpha, \ldots, \alpha\}.$$

Tout nombre α du corps K, ainsi que tout nombre réel, est permutable avec un polytettarion quelconque.

2. On appelle *transposé* de A le polytettarion obtenu en changeant les lignes en colonnes. On appelle *adjoint* de A le tettarion obtenu en remplaçant chaque coordonnée de A par le mineur correspondant dans le déterminant des coordonnées de A. Le transposé de l'adjoint de A est dit son *conjugué complexe*. Nous le désignerons par $\overline{A}$. Tout tettarion est permutable avec son conjugué complexe.

Quand les coordonnées a_{rs} du tettarion A sont des nombres rationnels, le tettarion A n'a qu'un seul conjugué ; c'est précisément le conjugué complexe. Mais quand les coordonnées sont elles-mêmes tirées d'un corps algébrique K, comme nous le supposerons plus bas, il faut distinguer entre le conjugué complexe, défini ci-dessus et les *conjugués en K*. Ces derniers, que nous désignerons en affectant la lettre A d'accents, donc par A', A'', A''',...., sont des tettarions dont les coordonnées sont les conjugués en K des a_{rs}.

Proposition 1. Le produit du tettarion A par son conjugué complexe $\overline{A}$ est un nombre rationnel dans le corps des coordonnées. Sa valeur est égale à celle du déterminant des a_{rs}. Nous l'appellerons *la norme complexe de A* et la désignerons par $N(A)$, avec le N majuscule.

$$N(A) \equiv A \,.\, \overline{A} = \det(a_{rs}).$$

Quand les coordonnées de A sont elles-mêmes des nombres algébriques, il faut distinguer entre la norme complexe et la *norme en K*. Cette dernière, que nous désignerons par $n(A)$, avec le n minuscule, est égale au produit de A par ses conjugués en K :

$$n(A) = A \,.\, A' \,.\, A'' \ldots.$$

Proposition 2. La norme complexe d'un produit de deux tettarions est égale au produit des normes complexes des facteurs :

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

Cette proposition s'étend au cas où le produit se compose d'un nombre fini quelconque de facteurs.

3. **Division.** — La division est définie comme opération inverse de la multiplication. Etant donnés deux polytettarions, A et B, il y a lieu de distinguer entre le *quotient à gauche*, X, et le *quotient à droite*, Y, de A par B, suivant qu'on cherche X ou Y (en général différents entre eux) tels que

$$A = X \,.\, B \qquad\qquad A = B \,.\, Y.$$

Pour déterminer pratiquement les deux quotients, on procède comme suit :

Lorsque A n'est pas un diviseur de zéro, on appelle *réciproque de A*, et l'on écrit A^{-1}, le tettarion

$$A^{-1} \equiv \frac{\overline{A}}{N(A)}$$

Il satisfait à l'équation : $A^{-1}.A = A.A^{-1} = 1$.

En multipliant l'égalité $A = X.B$ à droite par B^{-1} et l'égalité $A = B.Y$ à gauche par B^{-1}, on obtient les deux quotients cherchés sous la forme

$$X = A.B^{-1} = \frac{A\,\overline{B}}{N(B)} \quad \text{et} \quad Y = B^{-1}.A = \frac{\overline{B}.A}{N(B)}.$$

On ne peut parler de *quotient*, tout court, sans ajouter *à gauche* ou *à droite*, que si A et $\overline{B}$ sont permutables. Dans ce cas seulement, le symbole $A : B$ a un sens.

Corollaires. Pour additionner, soustraire, multiplier ou diviser des tettarions diagonaux, il suffit d'effectuer les mêmes opérations sur les coordonnées correspondantes.

Les tettarions diagonaux ne sont autre chose que les *nombres de Weierstrass*, objet de la première partie de ce mémoire; ainsi se trouve justifié le nom de *nombres diagonaux*.

Les polytettarions forment un corps de nombres. Il en est de même des polytettarions réduits et des polytettarions diagonaux. Nous désignerons par Ω le corps des tettarions réduits à gauche et par Ω_d celui des tettarions diagonaux.

Définition. — Un polytettarion est dit *rationnel*, si ses coordonnées sont toutes des nombres rationnels ordinaires. Nous désignerons les tettarions rationnels par des lettres majuscules latines

$$A,\ B,\ C, \ldots\ldots,\ X,\ Y,\ Z$$

et les nombres rationnels ordinaires par des lettres latines minuscules :

$$a,\ b,\ c, \ldots\ldots,\ x,\ y,\ z.$$

Un tettarion sera dit *complexe*, si ses coordonnées sont des nombres pris dans un corps algébrique K.

4. Dans ce mémoire, nous entendrons par K le corps déduit de deux racines carrées, $\sqrt{a}$, et $\sqrt{b}$, où a et b représentent des nombres entiers ordinaires, positifs ou négatifs. Tout élément α de ce corps K peut se mettre sous la forme

$$\alpha = a'_0 + a'_1\sqrt{a} + a'_2\sqrt{b} + a'_3\sqrt{ab}$$

où les a'_r sont des nombres rationnels.

En désignant par r le p. gr. c. d. de a et de b, puis posant $t \equiv a : r$ et $\rho \equiv b : r$, on peut donner aux nombres de ce corps K la forme :

$$\alpha = a_0 + a_1\sqrt{t.r} + a_2\sqrt{r.\rho} + a_3\sqrt{\rho.t}$$

où les a_k sont rationnels.

On sait que ce corps admet les quatre substitutions :

$$S_1 = 1,\ S_2 = \left(\sqrt{t} : -\sqrt{t}\right),\ S_3 = \left(\sqrt{v} : -\sqrt{v}\right) \text{ et } S_4 = \left(\sqrt{r} : -\sqrt{r}\right).$$

Les corps provenant de ces substitutions sont dits *les corps conjugués de K*. Le corps K est *normal*, puisqu'il est identique à ses conjugués. Il contient trois sous-corps quadratiques. A chaque nombre α de K correspondent trois nombres que nous désignerons, comme on le fait généralement, par α', α'' et α''', appartenant respectivement aux trois corps conjugués de K. Ils se déduisent de α par les substitutions S_2, S_3 et S_4. Ils sont dits *conjugués* en K. Le produit d'un nombre du corps K par ses conjugués en K est un nombre rationnel dit *la norme de* α. On la désigne par $n(\alpha)$, avec le n minuscule. On démontre que les entiers du corps K possèdent *une base* ; on la représente par $[\omega_0 \equiv 1, \omega_1, \omega_2, \omega_3]$ ou quelquefois par $[\omega_1 \equiv 1, \omega_2, \omega_3, \omega_4]$. Cela revient à dire que tout nombre entier du corps K, par exemple α, peut se mettre sous la forme

$$\alpha = a_0 + a_1\omega_1 + a_2\omega_2 + a_3\omega_3,$$

où les a_k sont des nombres *entiers* ordinaires, positifs, nuls ou négatifs.

Nous avons emprunté les résultats ci-dessus, concernant le corps $K\left(\sqrt{a}, \sqrt{b}\right)$ au travail de M. E. Amberg cité dans l'introduction.

5. Dans ce chapitre, nous envisagerons les polytettarions complexes réduits à gauche dont les coordonnées sont tirées du corps K introduit ci-dessus.

Notation. Nous désignerons ces tettarions complexes par des lettres grecques majuscules :

$$\mathrm{A}, \mathrm{B}, \Gamma, \ldots\ldots, \Xi, \Theta,$$

et les nombres du corps K par des lettres grecques minuscules

$$\alpha, \beta, \gamma, \ldots\ldots, \xi, \eta.$$

Nos tettarions complexes réduits à gauche sont tous de la forme :

$$\mathrm{A} \equiv \left\{ \begin{array}{l} \alpha_{11}, \alpha_{12}, \alpha_{13}, \ldots\ldots, \alpha_{1m} \\ 0\ , \alpha_{22}, \alpha_{23}, \ldots\ldots, \alpha_{2m} \\ 0\ , 0\ , \alpha_{33}, \ldots\ldots, \alpha_{3m} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 0\ , 0\ , 0\ , \ldots\ldots, \alpha_{mm} \end{array} \right\}$$

où chacun des α_{rs} est lui-même de la forme

$$\alpha \equiv a_0 + a_1\sqrt{rt} + a_2\sqrt{vt} + a_3\sqrt{rv},$$

les a_k étant des nombres rationnels. Nous désignerons un tel tettarion complexe symboliquement par $\{\alpha_{rs}\}$, de sorte que :

$$\mathrm{A} \equiv \{\alpha_{rs}\}.$$

§ 2. La divisibilité et la théorie des idéaux dans le corps Ω.

1. L'objet de ce paragraphe est l'étude du corps Ω des polytettarions complexes réduits à gauche, c'est-à-dire ayant la forme indiquée au paragraphe précédent. Dans la suite, nous sous-entendrons le plus souvent les mots *à gauche* et dirons simplement *tettarions réduits*. Il va de soi qu'on pourrait faire une étude tout analogue des polytettarions réduits à droite.

Dans le domaine des tettarions, la multiplication n'étant pas commutative, il y a lieu de distinguer deux arithmétiques se développant parallèlement l'une à l'autre : *une arithmétique à gauche* et une *arithmétique à droite*. Dans notre travail, nous traiterons l'arithmétique à droite (des polytettarions réduits à gauche).

2. Pour abréger l'exposé :

1) Nous désignerons par E_k le polytettarion (réduit à gauche) dont toutes les coordonnées non diagonales sont nulles, sauf celles de la $k^{ième}$ ligne, lesquelles sont des nombres du corps K ; les coordonnées diagonales étant des 1. Par exemple :

$$E_2 \equiv \left\{ \begin{array}{l} 1,\ 0,\ 0,\ldots\ldots,\ 0 \\ 0,\ 1,\ \varepsilon_{23},\ldots\ldots,\ \varepsilon_{2m} \\ 0,\ 0,\ 1,\ldots\ldots,\ 1 \\ \ldots\ldots\ldots\ldots \\ 0,\ 0,\ 0,\ldots\ldots,\ 1 \end{array} \right\}$$

Remarque : $E_m = 1$.

2) Nous désignerons par H_k le nombre diagonal dont toutes les coordonnées sont des 1, sauf la $k^{ième}$ qui est un nombre, η, du corps K. Par exemple :

$$H_3 \equiv \{\, 1,\ 1,\ \eta,\ 1,\ldots\ldots,\ 1,\ldots\ldots,\ 1 \,\}$$

Dans la suite, la lettre H désignera exclusivement des nombres diagonaux de cette forme spéciale.

3. **Définitions.** — Un polytettarion complexe $A \equiv \{\, \alpha_{rs} \,\}$ est dit *entier*, si toutes ses coordonnées α_{rs} sont des entiers du corps K, c'est-à-dire des expressions de la forme :

$$\alpha_{rs} = c_0^{(rs)} + c_1^{(rs)}.\omega_1 + c_2^{(rs)}.\omega_2 + c_3^{(rs)}.\omega_3$$

où les $c_k^{(rs)}$ sont des entiers ordinaires, $[1, \omega_1, \omega_2, \omega_3]$ constituant une base du corps K.

Le polytettarion entier A est dit *divisible à droite* par le polytettarion entier B, s'il existe un polytettarion entier Γ vérifiant l'égalité :

$$A = \Gamma . B .$$

Dans ce cas, nous dirons aussi que A est *un multiple à droite* de B, ou simplement *un multiple de* B, en sous-entendant les mots *à droite* ; ou encore : que B est *contenu dans* A.

Un polytettarion entier E, contenu dans n'importe quel polytettarion entier, est dit un *polytettarion-unité*, ou simplement une *unité*. La condition nécessaire et suffisante pour que E soit une unité est que ses coordonnées diagonales soient des unités du corps K. (v. § 4, 2).

Un polytettarion complexe entier A est dit *premier* si, dans toutes les décompositions possibles de A en un produit de deux facteurs, l'un de ceux-ci est nécessairement un polytettarion unité.

4. Lemme. — *Pour qu'un nombre diagonal* $\mathrm{H}_k = \{1, 1, \ldots, 1, \eta, 1, \ldots, 1\}$ *divise à gauche un tettarion entier réduit à gauche* $\mathrm{A} = \{\alpha_{rs}\}$, *il faut et il suffit que les coordonnées de la* $k^{\text{ième}}$ *ligne de* A *soient des multiples de* η *dans le corps* K.

Pour fixer les idées, nous supposerons dans la démonstration $m = 5$, $k = 3$. Soit

$$\mathrm{A} = \begin{Bmatrix} \alpha_{11}, & \alpha_{12}, & \alpha_{13}, & \alpha_{14}, & \alpha_{15} \\ 0, & \alpha_{22}, & \alpha_{23}, & \alpha_{24}, & \alpha_{25} \\ 0, & 0, & \alpha_{33}, & \alpha_{34}, & \alpha_{35} \\ 0, & 0, & 0, & \alpha_{44}, & \alpha_{45} \\ 0, & 0, & 0, & 0, & \alpha_{55} \end{Bmatrix}$$

et $\mathrm{H}_3 = \{1, 1, \eta, 1, 1\}$, où tous les α_{rs} et η sont des nombres entiers du corps K. Pour que A soit un multiple à gauche de H_k, il faut et il suffit (§ 1, 3) que le produit suivant soit un tettarion entier :

$$\mathrm{H}_3^{-1}.\mathrm{A} = \frac{\overline{\mathrm{H}}_3.\mathrm{A}}{N(\mathrm{H}_3)} = \frac{\{\eta, \eta, 1, \eta, \eta\}.\mathrm{A}}{\eta}$$

$$= \frac{1}{\eta} \cdot \begin{Bmatrix} \alpha_{11}\eta, & \alpha_{12}\eta, & \alpha_{13}\eta, & \alpha_{14}\eta, & \alpha_{15}\eta \\ 0, & \alpha_{22}\eta, & \alpha_{23}\eta, & \alpha_{24}\eta, & \alpha_{25}\eta \\ 0, & 0, & \alpha_{33}, & \alpha_{34}, & \alpha_{35} \\ 0, & 0, & 0, & \alpha_{44}\eta, & \alpha_{45}\eta \\ 0, & 0, & 0, & 0, & \alpha_{55}\eta \end{Bmatrix}$$

Pour que ce produit soit un entier, il suffit que toutes les coordonnées α_{3s} ($s = 3, 4, 5$) soient des multiples de η dans le corps K, c'est-à-dire, dans le cas général, que

$$\alpha_{ks} \equiv 0 \pmod{\eta} \qquad s = k, k+1, \ldots, m.$$

Corollaire. Pour diviser à gauche un tettarion réduit A par un diagonal H_k défini ci-dessus, il suffit de diviser les coordonnées de la $k^{\text{ième}}$ ligne de A par η.

5. Lemme. — Entendons par $\mathrm{B}_\lambda \equiv \{\beta_{rs}\}$ un tettarion complexe jouissant des trois propriétés que voici : 1) il est réduit à gauche ; 2) ses coordonnées diagonales sont des 1, sauf $\beta_{\lambda\lambda}$, qui peut être quelconque ; 3) les coordonnées non diagonales sont toutes nulles, sauf celles de la $\lambda^{\text{ième}}$ ligne, qui sont quelconques (λ étant l'un des nombres 1, 2, 3,..., m arbitrairement choisi mais fixe). Par exemple pour $\lambda = 3$, $m = 5$, on aura :

$$B_3 = \left\{ \begin{array}{ccccc} 1, & 0, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0, & 0 \\ 0, & 0, & \beta_{33}, & \beta_{34}, & \beta_{35} \\ 0, & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 0, & 1 \end{array} \right\}$$

Entendons par $\Gamma_\lambda \equiv \{ \gamma_{rs} \}$ un tettarion complexe jouissant des propriétés suivantes : 1) il est réduit à gauche ; 2) ses coordonnées γ_{rs} sont quelconques pour $r < \lambda$; 3) ses coordonnées diagonales sont égales à 1 pour $r \geqq \lambda$; 4) pour $r \geqq \lambda$ ses coordonnées γ_{rs} sont nulles. Par exemple pour $\lambda = 3$, $m = 5$, on aura :

$$\Gamma_3 = \left\{ \begin{array}{ccccc} \gamma_{11}, & \gamma_{12}, & \gamma_{13}, & \gamma_{14}, & \gamma_{15} \\ 0, & \gamma_{22}, & \gamma_{23}, & \gamma_{24}, & \gamma_{25} \\ 0, & 0, & 1, & 0, & 0 \\ 0, & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 0, & 1 \end{array} \right\}$$

Dans ces conditions, le produit $B_\lambda \cdot \Gamma_\lambda$ *est un tettarion réduit dont les coordonnées des* $(\lambda - 1)$ *premières lignes sont celles de* Γ_λ, *les autres étant celles de* B_λ. Ainsi pour $\lambda = 3$, $m = 5$.

$$B_3 . \Gamma_3 = \left\{ \begin{array}{ccccc} \gamma_{11}, & \gamma_{12}, & \gamma_{13}, & \gamma_{14}, & \gamma_{15} \\ 0, & \gamma_{22}, & \gamma_{23}, & \gamma_{24}, & \gamma_{25} \\ 0, & 0, & \beta_{33}, & \beta_{34}, & \beta_{35} \\ 0, & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 0, & 1 \end{array} \right\}$$

On démontre ce lemme en appliquant la définition de la multiplication des tettarions (v. § 1, 1).

Corollaires.

1. $B_\lambda = E_\lambda . H_\lambda$ (v. § 2. 2)

où $\eta_\lambda = \beta_{\lambda\lambda}$ et $\varepsilon_r^\lambda = \beta_{\lambda_r}$

2. $\Gamma_2 = B_1$; $\Gamma_1 = B_0 = 1$

3. $\Gamma_\lambda = B_{\lambda-1} . \Gamma_{\lambda-1}$

4) Tout polytettarion complexe réduit à gauche est de la forme Γ_{m+1}.

6. Théorème. — *Tout polytettarion réduit à gauche,* $A = \{ \alpha_{rs} \}$, *se décompose en un produit de tettarions unités* E_λ *et de diagonaux* H_λ *définis au § 2. 2, pris dans un ordre déterminé. Les coordonnées non diagonales de la* $\lambda^{ième}$ *ligne de* E_λ *sont celles de la* $\lambda^{ième}$ *ligne de* A ; *la* $\lambda^{ième}$ *coordonnée de* H_λ *est* $\alpha_{\lambda\lambda}$. En formule

$$A = E_m \cdot H_m \cdot E_{m-1} \cdot H_{m-1} \ldots\ldots E_\lambda \cdot H_\lambda \ldots\ldots E_2 \cdot H_2 \cdot E_1 \cdot H_1 .$$

En effet, d'après le lemme précédent, pour $\lambda = m + 1$, on a

$$A = B_m \cdot \Gamma_m = E_m \cdot H_m \cdot \Gamma_m .$$

De même

$$\Gamma_m = B_{m-1} \cdot \Gamma_{m-1} = E_{m-1} \cdot H_{m-1} \cdot \Gamma_{m-1},$$

et ainsi de suite jusqu'à $\lambda = 2$

$$\Gamma_2 = B_1 \cdot \Gamma_1 = B_1 = E_1 \cdot H_1 .$$

D'où

$$A = E_m \cdot H_m \cdot E_{m-1} \cdot H_{m-1} \cdot \ldots \ldots E_1 \cdot H_1$$

ou (v. la remarque au § 2, 2)

$$A = H_m \cdot E_{m-1} \cdot H_{m-1} \cdot \ldots \ldots E_1 \cdot H_1 .$$

Exemple pour $m = 4$

$$\begin{Bmatrix} \alpha_{11}, & \alpha_{12}, & \alpha_{13}, & \alpha_{14} \\ 0, & \alpha_{22}, & \alpha_{23}, & \alpha_{24} \\ 0, & 0, & \alpha_{33}, & \alpha_{34} \\ 0, & 0, & 0, & \alpha_{44} \end{Bmatrix} = \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & \alpha_{44} \end{Bmatrix} \cdot \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & \alpha_{33}, & \alpha_{34} \\ 0, & 0, & 0, & 1 \end{Bmatrix}$$

$$A \quad = \quad B_4 \quad \cdot \quad B_3$$

$$\cdot \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & \alpha_{22}, & \alpha_{23}, & \alpha_{24} \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix} \cdot \begin{Bmatrix} \alpha_{11}, & \alpha_{12}, & \alpha_{13}, & \alpha_{14} \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix} = \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & \alpha_{44} \end{Bmatrix} \cdot \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & \alpha_{34} \\ 0, & 0, & 0, & 1 \end{Bmatrix}$$

$$\cdot \quad B_2 \quad \cdot \quad B_1 \quad = \quad H_4 \quad \cdot \quad E_3$$

$$\cdot \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & \alpha_{33}, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix} \cdot \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & \alpha_{23}, & \alpha_{24} \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix} \cdot \begin{Bmatrix} 1, & 0, & 0, & 0 \\ 0, & \alpha_{22}, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix} \cdot \begin{Bmatrix} 1, & \alpha_{12}, & \alpha_{13}, & \alpha_{14} \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix} \cdot \begin{Bmatrix} \alpha_{11}, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 1 \end{Bmatrix}$$

$$\cdot \quad H_3 \quad \cdot \quad E_2 \quad \cdot \quad H_2 \quad \cdot \quad E_1 \quad \cdot \quad H_1$$

Corollaire. — Les éléments indécomposables du corps Ω *sont des nombres diagonaux, abstraction faite des unités.*

7. Il résulte des théorèmes précédents que la décomposition en facteurs premiers des polytettarions complexes réduits à gauche dépend essentiellement de celle des nombres diagonaux. Comme cette dernière, pour être toujours univoque, doit se faire à l'aide des idéaux, il est nécessaire, pour la décomposition des polytettarions réduits à gauche, de recourir à une notion analogue, et d'introduire des idéaux de polytettarions.

Définitions. — Considérons m idéaux quelconques du corps K, par exemple $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$. Nous appellerons *idéal diagonal du corps* Ω l'ensemble suivant de polytettarions $A \equiv \{ \alpha_{rs} \}$:

1) Tous les A sont réduits à gauche ; 2) les coordonnées de la première ligne de A parcourent, indépendamment l'une de l'autre, tous les nombres de l'idéal $\mathfrak{a}_1$ dans le corps K et ne prennent pas d'autre valeur ; 3) les coordonnées de la deuxième

ligne de A parcourent, indépendamment l'une de l'autre, tous les nombres de l'idéal $\mathfrak{a}_2$ du corps K et ne prennent pas d'autre valeur ; et ainsi de suite ; finalement 4) les coordonnées de la $m^{ième}$ ligne de A parcourent tous les nombres de l'idéal $\mathfrak{a}_m$ du corps K et uniquement ceux-là.

Nous désignerons un tel ensemble symboliquement à l'aide d'un nombre diagonal dont les coordonnées sont elles-mêmes des idéaux, soit

$$\mathfrak{A} \equiv \mathrm{Id} \mid \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_m \mid \equiv \mathrm{Id} \mid \mathfrak{a}_r \mid$$

Exemple. — Id | (2), (3), (4) | dans le corps Ω des tritettarions est l'ensemble constitué par une infinité de tritettarions

$$\begin{Vmatrix} \alpha_{11}, & \alpha_{12}, & \alpha_{13} \\ 0, & \alpha_{22}, & \alpha_{23} \\ 0, & 0, & \alpha_{33} \end{Vmatrix}$$

où α_{11}, α_{12}, α_{13} parcourent, indépendamment l'un de l'autre, tous les nombres de l'idéal principal (2) du corps K, et ne parcourent que ces nombres-là ; α_{22} et α_{23} parcourent tous les nombres de l'idéal principal (3) et seulement ceux-là ; enfin α_{33} parcourt tous les nombres de l'idéal (4) dans le corps K.

Nous appellerons les idéaux $\mathfrak{a}_r$ du corps K, servant à former l'idéal diagonal $\mathfrak{A}$ du corps Ω, *les coordonnées de l'idéal* $\mathfrak{A}$.

Un idéal diagonal du corps Ω sera dit *scalaire*, si ses coordonnées sont toutes égales entre elles.

Un idéal diagonal $\mathfrak{A} \equiv \mathrm{Id} \mid \mathfrak{a}_r \mid$, où tous les $\mathfrak{a}_r$ sont des idéaux principaux du corps K, sera dit *un idéal diagonal principal du corps* Ω.

Un idéal diagonal contenant l'unité principale ou un des diviseurs de cette unité est dit *l'idéal unité*. Nous le désignerons par (1) ; il contient *tous* les nombres entiers du corps Ω et seulement ceux-là.

Nous appellerons *produit diagonal des deux idéaux diagonaux*, $\mathfrak{A} \equiv \mathrm{Id} \mid \mathfrak{a}_r \mid$ et $\mathfrak{B} \equiv \mathrm{Id} \mid \mathfrak{b}_r \mid$, du corps Ω l'idéal $\mathfrak{C} \equiv \mathrm{Id} \mid \mathfrak{c}_r \mid$ dont les coordonnées sont

$$\mathfrak{c}_r = \mathfrak{a}_r \cdot \mathfrak{b}_r \qquad (r = 1, 2, \ldots, m).$$

Ce produit $\mathfrak{C}$ contient tous les tettarions dont les coordonnées de la $r^{ième}$ ligne (pour $r = 1, 2, \ldots, m$) appartiennent à l'idéal $\mathfrak{a}_r \cdot \mathfrak{b}_r$ du corps K ; et $\mathfrak{C}$ ne contient que ces tettarions-là.

La définition nouvelle du produit de deux idéaux diffère de la définition ordinaire en ce que le produit diagonal de deux idéaux diagonaux ne contient pas nécessairement tous les produits des nombres appartenant aux idéaux facteurs. Mais cette définition se justifie par un double fait : d'abord, elle coïncide avec la définition de Dedekind, dès que l'on passe du corps des tettarions réduits à gauche au sous-corps des nombres diagonaux ; ensuite elle rend la multiplication des idéaux *commutative*, ce qui simplifie beaucoup la théorie de la décomposition en facteurs premiers, ainsi que celle des congruences.

Un idéal diagonal $\mathfrak{A}$ du corps Ω sera dit *diagonalement divisible* par un idéal

diagonal $\mathfrak{B}$ du même corps, lorsqu'on pourra trouver dans ce corps un idéal diagonal $\mathfrak{C}$ tel que :

$$\mathfrak{A} = \mathfrak{B} \cdot \mathfrak{C} .$$

$\mathfrak{C}$ sera dit *le quotient diagonal* de $\mathfrak{A}$ par $\mathfrak{B}$ ou *un diviseur diagonal* de $\mathfrak{A}$. On peut ici supprimer les termes *à gauche* et *à droite* et parler de quotient tout court, du moment que la multiplication des idéaux diagonaux est commutative. Le terme de *diagonal* permet d'éviter toute confusion avec le quotient dans le sens classique.

Conséquence. Pour diviser un idéal diagonal du corps Ω par un autre idéal diagonal, il suffit de diviser leurs coordonnées correspondantes.

Un idéal diagonal du corps Ω est dit *premier* si, dans toute décomposition possible de cet idéal en un produit diagonal de deux facteurs, l'un est toujours l'idéal unité.

Deux idéaux diagonaux sont dits *premiers entre eux*, s'ils n'ont aucun diviseur idéal diagonal commun, sauf l'idéal unité.

Si un nombre entier $A = | \alpha_{rs} |$ du corps Ω appartient à l'idéal diagonal $\mathfrak{A} = \mathrm{Id} | \mathfrak{a}_r |$ du même corps, nous dirons, par analogie avec la théorie classique des idéaux, que A est *congru à zéro mod.* $\mathfrak{A}$ et nous écrirons,

$$A \equiv 0 \ (\mathrm{mod.}\ \mathfrak{A}).$$

Nous dirons que *l'idéal* $\mathfrak{A}$ *divise le nombre* A.

Des définitions posées résultent les théorèmes suivants :

8. Théorème. — *Un entier* $A = | \alpha_{rs} |$ *du corps* Ω *est congru à zéro suivant un idéal diagonal* $\mathfrak{A} = \mathrm{Id} | \mathfrak{a}_r |$ *de ce corps, si les coordonnées* α_{rs} *de la* $r^{\text{ième}}$ *ligne (pour* $r = 1, 2, \ldots, m$ séparément) *sont des entiers du corps K appartenant à l'idéal* $\mathfrak{a}_r$ *du corps K.* En formule :

$$A \equiv 0 \ (\mathrm{mod.}\ \mathfrak{A}) \ \text{si} \ \alpha_{rs} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{a}_r) \quad s = r, r+1, \ldots, m \quad r = 1, 2, \ldots, m .$$

9. Théorème. — *La somme et la différence de deux entiers* $A = | \alpha_{rs} |$ *et* $B = | \beta_{rs} |$ *d'un idéal diagonal* $\mathfrak{A} = \mathrm{Id} | \mathfrak{a}_r |$ *du corps* Ω *appartiennent à l'idéal diagonal* $\mathfrak{A}$.

En effet, les congruences

$$A \equiv 0 \ (\mathrm{mod.}\ \mathfrak{A}) \quad \text{et} \quad B \equiv 0 \ (\mathrm{mod.}\ \mathfrak{A})$$

entraînent les suivantes

$$\alpha_{rs} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{a}_r) \quad \begin{pmatrix} r = 1, 2, \ldots, m \\ s = r, r+1, \ldots, m \end{pmatrix}$$

et

$$\beta_{rs} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{a}_r)$$

On sait par la théorie des corps algébriques (v. par exemple D. Hilbert) que dans ce cas

$$\alpha_{rs} \pm \beta_{rs} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{a}_r)$$

Or, cela entraîne, en vertu du théorème précédent,

$$A \pm B \equiv 0 \ (\mathrm{mod.}\ \mathfrak{A}).$$

10. Théorème. — *Le produit à droite,* $A.B$, *d'un entier* $A = |\ \alpha_{rs}\ |$ *de l'idéal diagonal* $\mathfrak{A} = \mathrm{Id}\ |\ \mathfrak{a}_r\ |$ *du corps* Ω *par un tettarion entier* $B = |\ \beta_{rs}\ |$ *du même corps, appartient au même idéal diagonal* $\mathfrak{A}$.

En effet, si :

$$A \equiv 0 \pmod{\mathfrak{A}},$$

on a

$$\alpha_{rs} \equiv \pmod{\mathfrak{a}_r}$$

pour $r = 1, 2, \ldots, m$ (v. § 2. 8). Formons le produit à droite de A par B ; il vient

$$A \cdot B = \left\{ \sum_k \alpha_{rk} \cdot \beta_{ks} \right\} \equiv \{ \gamma_{rs} \} ;$$

chacun des γ_{rs} ($r = 1, 2, \ldots, m$; $s = r + 1, r + 2, \ldots, m$) étant une combinaison linéaire de nombres de l'idéal $\mathfrak{a}_r$ avec des entiers du corps K, appartient encore à l'idéal $\mathfrak{a}_r$, donc

$$\gamma_{rs} \equiv 0 \pmod{\mathfrak{a}_r}.$$

Comme ceci reste vrai pour $r = 1, 2, \ldots, m$, il s'en suit que

$$A \cdot B \equiv 0 \pmod{\mathfrak{A}}.$$

11. La définition de l'idéal posée ci-dessus diffère de la définition classique introduite par Dedekind. Si nous avions introduit l'idéal tel qu'il est défini par Dedekind, il eût été nécessaire, vu la non-commutativité de la multiplication, de distinguer entre les *idéaux à droite* et les *idéaux à gauche*, suivant que l'ensemble des entiers constituant l'idéal contient les combinaisons linéaires à droite ou les combinaisons linéaires à gauche. Les deux théorèmes qu'on vient de démontrer prouvent que l'idéal que nous avons introduit est un idéal à droite si l'on adopte la définition de Dedekind. Réciproquement, tout idéal à droite dans le sens de Dedekind est un des idéaux introduits. En effet, et on le constate sans peine, l'ensemble des coordonnées d'une quelconque des m lignes des tettarions formant dans le corps Ω un idéal à droite dans le sens de Dedekind est à son tour un idéal du corps K : c'est là le fait qui caractérise l'idéal introduit.

Remarque. Dans la suite, nous sous-entendrons le plus souvent l'adjectif *diagonal* et dirons simplement *idéal du corps* Ω.

12. Théorème. — *Soit* $\mathfrak{A} \equiv \mathrm{Id}\ |\ \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m\ |$ *un idéal quelconque du corps* Ω. *Si cet idéal contient le tettarion* $A = |\ \alpha_{rs}\ |$, *il contient aussi le tettarion rationnel* $A \equiv |\ n(\alpha_{rs})\ |$ *dont les coordonnées,* $n(\alpha_{rs})$, *sont les normes en* K *des coordonnées de* A.

En effet, si $\mathfrak{A}$ contient A, on a, en vertu du théorème 8 de ce paragraphe, les congruences :

$$\alpha_{rs} \equiv 0 \pmod{\mathfrak{a}_r}.$$

D'autre part, on sait que si un idéal $\mathfrak{a}_r$ d'un corps algébrique K contient un entier α_{rs}, il contient aussi sa norme $n(\alpha_{rs})$. Il s'en suit

$$n(\alpha_{rs}) \equiv 0 \pmod{\mathfrak{a}_r}.$$

Dès lors, en vertu de la définition de l'idéal diagonal,

$$A \equiv 0 \ (\text{mod. } \mathfrak{A}).$$

13. Théorème. — *Tout idéal diagonal du corps* Ω *possède une base, c'est-à-dire que l'idéal contient un nombre fini d'entiers* A_k *tels que tout nombre de l'idéal puisse se mettre sous la forme :*

$$A_1 \cdot X_1 + A_2 \cdot X_2 + A_3 \cdot X_3 + \ldots\ldots,$$

les X_k *étant des polytettarions entiers rationnels réduits à gauche du corps* Ω.

Soit $\mathfrak{A} \equiv \text{Id} \mid \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m \mid$ un idéal quelconque du corps Ω ; les $\mathfrak{a}_r \equiv \text{Id}$ $(\alpha_1^{(r)}, \alpha_2^{(r)}, \alpha_3^{(r)}, \alpha_4^{(r)})$ sont, pour $r = 1, 2, \ldots, m$, des idéaux du corps K, idéaux dont les bases sont respectivement

$$(\alpha_1^{(r)}, \alpha_2^{(r)}, \alpha_3^{(r)}, \alpha_4^{(r)}) \,.$$

Si $B = \mid \beta_{rs} \mid$ est un tettarion complexe de l'idéal $\mathfrak{A}$, on a (v. théorème 8 de ce paragraphe)

$$\beta_{rs} \equiv 0 \ (\text{mod. } \mathfrak{a}_r)$$

et dès lors, puisque les β_{rs} appartiennent à l'idéal $\mathfrak{a}_r$ du corps K,

$$\beta_{rs} = \sum_k^{1..4} \alpha_k^{(r)} x_k^{(rs)}$$

où $x_1^{(rs)}, x_2^{(rs)}, x_3^{(rs)}, x_4^{(rs)}$ sont des nombres rationnels. Il s'en suit :

$$B \equiv \mid \beta_{rs} \mid = \left| \sum_k \alpha_k^{(r)} . x_k^{(rs)} \right| = \left| \begin{array}{cccc} \sum_{k=1}^{k=4} \alpha_k^{(1)} x_k^{(11)}, & \sum_{k=1}^{k=4} \alpha_k^{(1)} x_k^{(12)}, & \ldots\ldots, & \sum_{k=1}^{k=4} \alpha_k^{(1)} x_k^{(1m)} \\ 0 \quad , & \sum_{k=1}^{k=4} \alpha_k^{(2)} x_k^{(22)}, & \ldots\ldots, & \sum_{k=1}^{k=4} \alpha_k^{(2)} x_k^{(2m)} \\ \ldots & \ldots & \ldots & \ldots \\ 0 \quad , & 0 & ,\ldots\ldots, & \sum_{k=1}^{k=4} \alpha_k^{(m)} x_k^{(mm)} \end{array} \right|$$

ou bien, en vertu de la définition de l'addition des polytettarions (§ 1. 1)

$$= \sum_{k=1}^{k=4} \left| \begin{array}{cccc} \alpha_k^{(1)} x_k^{(11)}, & \alpha_k^{(1)} x_k^{(12)}, & \ldots\ldots, & \alpha_k^{(1)} x_k^{(1m)} \\ 0 \quad , & \alpha_k^{(2)} x_k^{(22)}, & \ldots\ldots, & \alpha_k^{(2)} x_k^{(2m)} \\ \ldots & \ldots & \ldots & \ldots \\ 0 \quad , & 0 & ,\ldots\ldots, & \alpha_k^{(m)} x_k^{(mm)} \end{array} \right|$$

ou (v. § 2. 4)

$$= \sum_{k=1}^{k=4} \begin{Vmatrix} \alpha_k^{(1)}, & 0, \ldots, & 0 \\ 0, & \alpha_k^{(2)}, \ldots, & 0 \\ \cdots & \cdots & \cdots \\ 0, & 0, \ldots, & \alpha_k^{(m)} \end{Vmatrix} \cdot \begin{Vmatrix} x_k^{(11)}, & x_k^{(12)}, \ldots, & x_k^{(1m)} \\ 0, & x_k^{(22)}, \ldots, & x_k^{(2m)} \\ \cdots & \cdots & \cdots \\ 0, & 0, \ldots, & x_k^{(mm)} \end{Vmatrix}$$

ou, sous forme plus concise,

$$= \sum_{k=1}^{k=4} \left\{ \alpha_k^{(1)}, \alpha_k^{(2)}, \ldots, \alpha_k^{(m)} \right\} \cdot \left\{ x_k^{(rs)} \right\}.$$

On constate : 1° que $\left\{ \alpha_k^{(1)}, \alpha_k^{(2)}, \ldots, \alpha_k^{(m)} \right\}$ est un nombre diagonal (pour $k = 1, 2, 3, 4$) ; nous le désignerons par A_k ; 2° que les tettarions $\left| x_k^{(rs)} \right|$ sont des polytettarions *rationnels* réduits à gauche ; nous les désignerons par X_k. Il s'en suit

$$B = \sum_{k=1}^{k=4} A_k \cdot X_k .$$

Corollaire. Ce théorème donne un moyen pratique de trouver une base de l'idéal $\mathfrak{A} = \mathrm{Id} \mid \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m \mid$. En effet, si les bases des idéaux $\mathfrak{a}_r$ du corps K sont

$$\left(\alpha_1^{(r)}, \alpha_2^{(r)}, \alpha_3^{(r)}, \alpha_4^{(r)}\right),$$

l'une des bases de l'idéal $\mathfrak{A}$ sera formée par les quatre nombres diagonaux suivants :

$$A_1 \equiv \left\{ \alpha_1^{(1)}, \alpha_1^{(2)}, \ldots, \alpha_1^{(r)}, \ldots, \alpha_1^{(m)} \right\}$$

$$A_2 \equiv \left\{ \alpha_2^{(1)}, \alpha_2^{(2)}, \ldots, \alpha_2^{(r)}, \ldots, \alpha_2^{(m)} \right\}$$

$$A_3 \equiv \left\{ \alpha_3^{(1)}, \alpha_3^{(2)}, \ldots, \alpha_3^{(r)}, \ldots, \alpha_3^{(m)} \right\}$$

$$A_4 \equiv \left\{ \alpha_4^{(1)}, \alpha_4^{(2)}, \ldots, \alpha_4^{(r)}, \ldots, \alpha_4^{(m)} \right\}$$

14. Théorème. — *Si* $\mathfrak{B} \equiv \mathrm{Id} \mid \mathfrak{b}_r \mid$ *est un diviseur diagonal de l'idéal* $\mathfrak{A} \equiv \mathrm{Id} \mid \mathfrak{a}_r \mid$ *du corps* Ω, *tout entier* $\Gamma \equiv \mid \gamma_{rs} \mid$ *de* $\mathfrak{A}$ *appartient à* $\mathfrak{B}$, *c'est-à-dire se trouve parmi les éléments de* $\mathfrak{B}$; en formule :

$$\text{si} \quad \Gamma \equiv 0 \ (\mathrm{mod.}\ \mathfrak{A}) \quad \text{et} \quad \mathfrak{A} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{B}),$$
$$\text{on a} \quad \Gamma \equiv 0 \ (\mathrm{mod.}\ \mathfrak{B}).$$

En effet, la congruence $\Gamma \equiv 0$ (mod. $\mathfrak{A}$) entraîne, en vertu du théorème 8 de ce paragraphe, les suivantes :

$$\gamma_{rs} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{a}_r) \quad \begin{pmatrix} r = 1, 2, \ldots, m \\ s = r, r+1, \ldots, m \end{pmatrix};$$

$$\text{la congruence} \quad \mathfrak{A} \equiv 0 \ (\mathrm{mod.}\ \mathfrak{B}) \quad \text{entraîne}$$
$$\mathfrak{a}_r \equiv 0 \ (\mathrm{mod.}\ \mathfrak{b}_r).$$

On sait d'autre part (théorie des corps algébriques) que, si dans le corps K un idéal $\mathfrak{a}_r$ est divisible par un idéal $\mathfrak{b}_r$, tous les nombres de $\mathfrak{a}_r$ appartiennent à $\mathfrak{b}_r$ donc :

$$\gamma_{rs} \equiv 0 \pmod{\mathfrak{b}_r}.$$

Il s'en suit

$$\Gamma \equiv 0 \pmod{\mathfrak{B}}. \qquad \text{c. q. f. d.}$$

15. Théorème. — *Si* $\mathfrak{A} \equiv \mathrm{Id} \{ \mathfrak{a}_r \}$ *est un idéal du corps* Ω, *il existe toujours dans ce corps un idéal* $\mathfrak{B}$, *tel que le produit diagonal*

$$\mathfrak{A}.\mathfrak{B}$$

soit un idéal principal.

Démonstration. On sait qu'à tout idéal $\mathfrak{a}_r$ du corps K on peut faire correspondre dans le même corps un idéal $\mathfrak{a}_r^{-1}$, dit réciproque du premier, tel que leur produit $\mathfrak{a}_r.\mathfrak{a}_r^{-1}$ donne un idéal principal, soit (α_r). Dès lors, l'idéal

$$\mathfrak{B} \equiv \mathrm{Id} \left\{ \mathfrak{a}_r^{-1} \right\}$$

du corps Ω satisfait au théorème. En effet le produit

$$\mathfrak{A}.\mathfrak{B} = \mathrm{Id} \left\{ \mathfrak{a}_r \right\}. \ \mathrm{Id} \left\{ \mathfrak{a}_r^{-1} \right\} = \mathrm{Id} \left\{ \mathfrak{a}_r.\mathfrak{a}_r^{-1} \right\} = \mathrm{Id} \left\{ \alpha_r \right\}$$

cst un idéal principal.

Nous appellerons l'idéal $\left\{ \mathfrak{a}_r^{-1} \right\}$ *l'idéal réciproque* de l'idéal $\mathfrak{A}$ dans le corps Ω et nous le désignerons par

$$\mathfrak{A}^{-1}.$$

16. Théorème. — *Un polytettarion réduit entier complexe* $\Gamma = \{ \gamma_{rs} \}$ *du corps* Ω *ne peut être contenu que dans un nombre fini d'idéaux distincts du corps* Ω.

En effet, soit $\mathfrak{A} = \mathrm{Id} \{ \mathfrak{a}_r \}$ un idéal quelconque du corps Ω et supposons que $\mathfrak{A}$ contienne le tettarion rationnel $C \equiv \{ n (\gamma_{rs}) \}$ dont les coordonnées sont les normes en K des coordonnées correspondantes de Γ. On sait, par la théorie des corps algébriques, que chaque nombre entier du corps K, donc aussi chacun des $n (\gamma_{rs})$, n'appartient qu'à un nombre fini d'idéaux $\mathfrak{a}_r$ de ce corps K. Il en résulte que le nombre des idéaux $\mathfrak{A} \equiv \mathrm{Id} \{ \mathfrak{a}_r \}$, qui contiennent C, est fini. D'autre part, si un idéal contient Γ, il contient aussi $C = \{ n (\gamma_{rs}) \}$ (v. théorème 12 de ce paragraphe). Dès lors, dans le corps Ω, le nombre des idéaux contenant Γ est, au plus, égal à celui des idéaux contenant C ; par conséquent ce nombre est limité.

17. Théorème. — *Un idéal du corps* Ω *ne peut avoir qu'un nombre fini de diviseurs idéaux diagonaux* (dans le sens du § 2. 7).

Démonstration. Soit $\mathfrak{A}$ un idéal du corps Ω, $\mathfrak{B}$ un de ses diviseurs idéaux diagonaux, Γ un nombre de $\mathfrak{A}$ et C le tettarion rationnel dont parle le théorème précédent. C appartient à l'idéal $\mathfrak{B}$ (théorème 14 de ce paragraphe). Dès lors, en vertu du théorème précédent, il n'y a qu'un nombre fini d'idéaux $\mathfrak{B}$ qui contiennent C, donc aussi un nombre fini d'idéaux diviseurs diagonaux de $\mathfrak{A}$.

c. q. f. d.

18. Théorème. — *Soient* $\mathfrak{A}$, $\mathfrak{B}$ et $\mathfrak{C}$, *trois idéaux du corps* Ω ; *si*

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

on a

$$\mathfrak{B} = \mathfrak{C}.$$

Démonstration. Soit $\mathfrak{D}$ l'idéal réciproque de $\mathfrak{A}$. Il résulte de l'hypothèse

$$\mathfrak{D} \,.\, \mathfrak{A} \,.\, \mathfrak{B} = \mathfrak{D} \,.\, \mathfrak{A} \,.\, \mathfrak{C} \quad \text{c'est-à-dire} \quad \mathfrak{B}\,(\Gamma) = \mathfrak{C}\,(\Gamma)$$

où (Γ) est l'idéal principal égal au produit diagonal $\mathfrak{D} \,.\, \mathfrak{A}$. En divisant l'égalité précédente par Γ, qui est un facteur numérique, on obtient

$$\mathfrak{B} = \mathfrak{C}. \qquad \text{c. q. f. d.}$$

19. Théorème. — *Si tous les nombres d'un idéal* $\mathfrak{A} \equiv \mathrm{Id} \mid \mathfrak{a}_r \mid$ *du corps* Ω *sont congrus à zéro suivant un idéal* $\mathfrak{B} = \mathrm{Id} \mid \mathfrak{b}_r \mid$ *du même corps, l'idéal* $\mathfrak{A}$ *est diagonalement divisible par* $\mathfrak{B}$.

En effet, soit $\mathrm{A} = \mid \alpha_{rs} \mid$ un tettarion complexe quelconque de l'idéal $\mathfrak{A}$ du corps Ω. La congruence

$$\mathrm{A} \equiv 0 \ (\text{mod. } \mathfrak{B})$$

entraîne les suivantes (théorème 8 de ce paragraphe)

$$\alpha_{rs} \equiv 0 \ (\text{mod. } \mathfrak{b}_r).$$

Dans la théorie générale des corps algébriques, on déduit de là que

$$\mathfrak{a}_r \equiv 0 \ (\text{mod. } \mathfrak{b}_r)$$

et par suite, en vertu de la définition de la division des idéaux du corps Ω (v. 7 de ce paragraphe), que

$$\mathfrak{A} \equiv 0 \ (\text{mod. } \mathfrak{B}).$$

Corollaire. — Le plus grand commun diviseur diagonal $\mathfrak{D}$ de deux idéaux diagonaux $\mathfrak{A}$ et $\mathfrak{B}$ du corps Ω est un idéal diagonal qui contient tous les nombres de $\mathfrak{A}$ et tous ceux de $\mathfrak{B}$.

En effet, tout diviseur diagonal commun à $\mathfrak{A}$ et à $\mathfrak{B}$ doit contenir, en vertu du théorème précédent, à la fois tous les nombres de $\mathfrak{A}$ et tous ceux de $\mathfrak{B}$. Par hypothèse, $\mathfrak{D}$ contient ces nombres-là. Comme, d'autre part, tout autre idéal contenant, outre tous les nombres de $\mathfrak{D}$, encore d'autres ne résultant pas de combinaisons linéaires des précédents divise $\mathfrak{D}$, on peut dire que $\mathfrak{D}$ est le plus grand commun diviseur de $\mathfrak{A}$ et de $\mathfrak{B}$; nous le désignerons par

$$\mathfrak{D} \equiv (\mathfrak{A} \mid \mathfrak{B}).$$

20. Théorème. — *Le plus grand commun diviseur diagonal des idéaux* $\mathfrak{A} = \mathrm{Id} \mid \mathfrak{a}_r \mid$ *et* $\mathfrak{B} = \mathrm{Id} \mid \mathfrak{b}_r \mid$ *du corps* Ω *est un idéal* $\mathfrak{D} = \mathrm{Id} \mid \mathfrak{b}_r \mid$ *dont les coordonnées* $\mathfrak{b}_r$ *sont, dans le corps K, les pl. gr. c. d. des coordonnées correspondantes* $\mathfrak{a}_r$ *et* $\mathfrak{b}_r$ *des idéaux* $\mathfrak{A}$ *et* $\mathfrak{B}$.

$$\mathfrak{D} \equiv (\mathfrak{A} \mid \mathfrak{B}) = \mathrm{Id} \mid (\mathfrak{a}_1 \mid \mathfrak{b}_1), (\mathfrak{a}_2 \mid \mathfrak{b}_2), \ldots, (\mathfrak{a}_m \mid \mathfrak{b}_m) \mid \equiv \mathrm{Id} \mid \mathfrak{b}_r \mid.$$

En effet : en vertu du corollaire précédent, l'idéal $\mathfrak{D}$ contient tous les nombres des idéaux $\mathfrak{A}$ et $\mathfrak{B}$. Il en résulte, en vertu de la définition de l'idéal posée au 7 de ce paragraphe, que les $r^{ièmes}$ coordonnées de $\mathfrak{D}$ forment, pour $r = 1, 2, \ldots, m$, un idéal $\mathfrak{d}_r$ du corps K, idéal qui contient à la fois tous les nombres de $\mathfrak{a}_r$ et tous ceux de $\mathfrak{b}_r$. Cet idéal est le pl. gr. c. d. des idéaux $\mathfrak{a}_r$ et $\mathfrak{b}_r$ du corps K (v. la théorie des corps algébriques).

21. Théorème. — *Lorsque le produit diagonal de deux idéaux* $\mathfrak{A} = \mathrm{Id} \mid \mathfrak{a}_r \mid$ *et* $\mathfrak{B} = \mathrm{Id} \mid \mathfrak{b}_r \mid$ *du corps* Ω *est divisible diagonalement par un idéal premier* $\mathfrak{P} = \mathrm{Id} \mid \mathfrak{p}_r \mid$ *du même corps, l'un au moins des idéaux* $\mathfrak{A}$ *ou* $\mathfrak{B}$ *est divisible diagonalement par* $\mathfrak{P}$.

En effet : si le produit $\mathfrak{A} \cdot \mathfrak{B}$ est divisible diagonalement par $\mathfrak{P}$, le produit $\mathfrak{a}_r \cdot \mathfrak{b}_r$ des idéaux du corps K doit être divisible par $\mathfrak{p}_r$ (v. 7 de ce paragraphe). En vertu de la théorie générale des corps algébriques, il en résulte que :

$$\begin{array}{ll} \text{ou bien} & \mathfrak{a}_r \equiv 0 \pmod{\mathfrak{p}_r} \\ \text{ou bien} & \mathfrak{b}_r \equiv 0 \pmod{\mathfrak{p}_r}. \end{array}$$

Dès lors, on a aussi l'alternative :

$$\begin{array}{ll} \text{ou} & \mathfrak{A} \equiv 0 \pmod{\mathfrak{P}} \\ \text{ou} & \mathfrak{B} \equiv 0 \pmod{\mathfrak{P}} \end{array}$$ c. q. f. d.

22. Théorème. — *Tout idéal du corps* Ω *peut être décomposé en un produit diagonal d'un nombre fini d'idéaux premiers et il ne peut l'être que d'une seule manière, abstraction faite de l'ordre de succession des facteurs.*

23. Les considérations précédentes nous montrent que la théorie des idéaux diagonaux dans le corps Ω obéit aux mêmes lois que celle des idéaux du corps Ω_d des nombres diagonaux complexes (nombres de Weierstrass). Quoique étant des ensembles plus larges que les idéaux du corps des nombres diagonaux, les idéaux diagonaux ont les mêmes bases. Par suite, la décomposition des nombres diagonaux rationnels, ainsi que la détermination des idéaux diagonaux premiers du corps Ω sont tout analogues aux théories correspondantes du corps des nombres diagonaux. Les nombres de classes sont les mêmes.

Les résultats obtenus dans ce paragraphe tranchent les questions concernant la décomposition multiplicative dans le corps Ω. En effet, les théorèmes 15 et 22 nous donnent la décomposition des nombres diagonaux en idéaux diagonaux premiers du corps Ω. Cette décomposition s'effectue d'après les lois de la décomposition des nombres diagonaux dans le corps Ω_d. Les idéaux premiers en Ω_d sont premiers en Ω. D'autre part, le théorème 6 permet de décomposer les polytettarions réduits à gauche. Chaque polytettarion se présente comme produit d'unités et de nombres diagonaux, pris dans un ordre déterminé, et la décomposition des polytettarions se ramène ainsi à la décomposition des nombres diagonaux dans le même corps.

§ 3. Les congruences suivant un idéal diagonal dans le corps Ω.

1. L'objet de ce chapitre est l'étude des congruences dans le corps Ω des polytettarions complexes réduits à gauche.

Il résulte des définitions posées au § 2. 7 :

1) que tout entier Γ est congru à lui-même suivant n'importe quel idéal ;

2) que $A \equiv B \pmod{\mathfrak{A}}$ entraîne $B \equiv A \pmod{\mathfrak{A}}$;

3) que deux entiers congrus à un troisième suivant le même idéal $\mathfrak{A}$ sont congrus entre deux modulo $\mathfrak{A}$.

On peut dès lors répartir les entiers du corps Ω en classes, telles que tous les nombres d'une classe soient congrus à un même entier modulo $\mathfrak{A}$. Tout entier du corps Ω appartient à une classe et à une seule modulo $\mathfrak{A}$, et tout nombre d'une classe détermine cette classe mod. $\mathfrak{A}$. Si l'on prend un nombre dans chacune de ces classes, on obtient un *système complet de restes* suivant le module $\mathfrak{A}$.

Définitions. — Nous appellerons *norme de l'idéal diagonal* $\mathfrak{A}$, et nous désignerons par $n(\mathfrak{A})$, le nombre des entiers de ce système complet de restes mod. $\mathfrak{A}$.

2. Théorème. — *Si* $A \equiv B$ *et* $\Gamma \equiv \Delta \pmod{\mathfrak{A}}$,
on a $A \pm \Gamma \equiv B \pm \Delta \pmod{\mathfrak{A}}$.

3. Théorème. — *Il est permis de multiplier à droite par un polytettarion quelconque du corps* Ω *les deux membres d'une congruence suivant un idéal quelconque de ce corps.* En formule : Si

$$A \equiv B \pmod{\mathfrak{A}}, \text{ on a } A \cdot M \equiv B \cdot M \pmod{\mathfrak{A}}.$$

En effet : si $A \equiv B \pmod{\mathfrak{A}}$ leur différence, $A - B$, est contenue dans l'idéal $\mathfrak{A}$ et par suite aussi le produit

$$(A - B) \cdot M \quad \text{(v. § 2. 10)}.$$

Il s'en suit

$$(A - B) \cdot M \equiv 0 \pmod{\mathfrak{A}}$$

c'est-à-dire,

$$AM \equiv BM \pmod{\mathfrak{A}}.$$

4. Théorème. — *Une congruence suivant un idéal scalaire du corps* Ω *subsiste si l'on multiplie à gauche ses deux membres par un polytettarion quelconque du corps.* En formule :

$$\text{Si } A \equiv B \pmod{\mathfrak{A}} \text{ et } \mathfrak{A} = \mathrm{Id} \mid a_1, a_2, \ldots, a_m \mid \text{ où}$$
$$a_1 = a_2 = a_3 \ldots = a_m \equiv a, \text{ on a}$$
$$M \cdot A \equiv M \cdot B \pmod{\mathfrak{A}}.$$

Démonstration. Soit

$$A = \mid \alpha_{rs} \mid, \; B = \mid \beta_{rs} \mid \text{ et } M = \mid \mu_{rs} \mid.$$

Le produit M · A est égal à $\mid \gamma_{rs} \mid$ avec $\gamma_{rs} = \sum_k \mu_{rk} \cdot \alpha_{ks} \ldots$ (1)

Le produit M · B est égal à $\mid \delta_{rs} \mid$ avec $\delta_{rs} = \sum_k \mu_{rk} \cdot \beta_{ks}$.

D'autre part, la congruence

$$A \equiv B \pmod{\mathfrak{A}}$$

entraîne les suivantes

$$\alpha_{rs} \equiv \beta_{rs} \pmod{\mathfrak{a}} \quad r = 1, 2, \ldots, m,$$

par suite les coordonnées correspondantes des $r^{ièmes}$ lignes des produits (1) sont congrues entre elles mod. $\mathfrak{a}$, car

$$\sum_k \mu_{rk}\alpha_{ks} \equiv \sum_k \mu_{rk}\beta_{ks} \pmod{\mathfrak{a}}$$

c'est-à-dire

$$\gamma_{rs} \equiv \delta_{rs} \pmod{\mathfrak{a}}.$$

Il en résulte que les polytettarions $|\gamma_{rs}|$ et $|\delta_{rs}|$ sont congrus entre eux mod. $\mathfrak{A}$, c'est-à-dire

$$M \cdot A \equiv M \cdot B \pmod{\mathfrak{A}}.$$

Remarque. Le théorème cesse d'être vrai pour un idéal quelconque du corps, car dans ce cas

$$\sum_k \mu_{rk} \cdot \alpha_{ks} \text{ n'est pas congrue à } \sum_k \mu_{rk} \cdot \beta_{ks} \pmod{\mathfrak{a}_r}.$$

5. Théorème. — *Une congruence suivant un idéal quelconque du corps Ω subsiste si l'on multiplie à gauche ses deux membres par un nombre diagonal du corps.*

En effet : soit $A \equiv B \pmod{\mathfrak{A}}$ où $A \equiv |\alpha_{rs}|$ et $B \equiv |\beta_{rs}|$ sont deux polytettarions réduits à gauche et $\mathfrak{A} \equiv \mathrm{Id}\,|\mathfrak{a}_r|$; soit enfin $M \equiv |\mu_1, \mu_2, \ldots, \mu_m|$ un nombre diagonal du corps.

Le produit $M \cdot A$ est égal à $|\gamma_{rs}| \equiv |\mu_r \cdot \alpha_{rs}|$.
Le produit $M \cdot B$ est égal à $|\delta_{rs}| \equiv |\mu_r \cdot \beta_{rs}|$.

La congruence

$$A \equiv B \pmod{\mathfrak{A}}$$

entraîne les suivantes

$$\alpha_{rs} \equiv \beta_{rs} \pmod{\mathfrak{a}_r}$$

et par suite

$$\mu_r \cdot \alpha_{rs} \equiv \mu_r \cdot \beta_{rs} \pmod{\mathfrak{a}_r}$$

c'est-à-dire

$$\gamma_{rs} \equiv \delta_{rs} \pmod{\mathfrak{a}_r}.$$

Il en résulte

$$M \cdot A \equiv M \cdot B \pmod{\mathfrak{A}}.$$

6. Théorème. — *Il est permis de multiplier à droite, et de multiplier à gauche, membre à membre, deux congruences suivant un idéal scalaire du corps.* En formule :

si $\quad A \equiv B \pmod{\mathfrak{A}} \quad$ et $\quad \Gamma \equiv \Delta \pmod{\mathfrak{A}}$,

on a $\quad A \cdot \Gamma \equiv B \cdot \Delta \pmod{\mathfrak{A}} \quad$ et $\quad \Gamma \cdot A \equiv \Delta \cdot B \pmod{\mathfrak{A}}$

si $\mathfrak{A}$ est un idéal scalaire du corps.

En effet, si $A \equiv B \pmod{\mathfrak{A}}$, on a (§ 3. 3 et 4)

$$A \cdot \Gamma \equiv B \cdot \Gamma \quad \text{et} \quad \Gamma \cdot A \equiv \Gamma \cdot B \pmod{\mathfrak{A}}.$$

De même, si $\Gamma \equiv \Delta \pmod{\mathfrak{A}}$, on a

$$B \cdot \Gamma \equiv B \cdot \Delta \pmod{\mathfrak{A}} \quad \text{et} \quad \Gamma \cdot B \equiv \Delta \cdot B \pmod{\mathfrak{A}}$$

en vertu des mêmes théorèmes. Il en résulte :

$$A \cdot \Gamma \equiv B \cdot \Gamma \equiv B \cdot \Delta \pmod{\mathfrak{A}} \quad \text{ou} \quad A \cdot \Gamma \equiv B \cdot \Delta \pmod{\mathfrak{A}}$$

et $$\Gamma \cdot A \equiv \Gamma \cdot B \equiv \Delta \cdot B \pmod{\mathfrak{A}} \quad \text{ou} \quad \Gamma \cdot A \equiv \Delta \cdot B \pmod{\mathfrak{A}}.$$ c. q. f d.

Remarque. Le théorème cesse d'être vrai si l'on prend comme module un idéal quelconque du corps Ω, en vertu de la remarque faite au théorème 4.

7. Théorème. — *La congruence* $A \equiv B$ *entre deux tettarions* $A = |\alpha_{rs}|$ *et* $B = |\beta_{rs}|$ *suivant un idéal scalaire* $\mathfrak{A}$ *du corps* Ω *entraîne les congruences*

$$\overline{A} \equiv \overline{B} \pmod{\mathfrak{A}} \quad \text{et} \quad N(A) \equiv N(B) \pmod{\mathfrak{A}}$$

ou $\overline{A}$ *et* $\overline{B}$ *sont les conjugués complexes de* A *et de* B (v. § 1. 2), et $N(A)$ et $N(B)$ *les normes complexes de* A *et de* B.

Démonstration. Soit $\mathfrak{A} = \mathrm{Id}\,|\,a, a, \ldots, a\,|$. La congruence $A \equiv B \pmod{\mathfrak{A}}$ entraîne les suivantes :

$$\alpha_{rs} \equiv \beta_{rs} \pmod{a} \quad \begin{pmatrix} r = 1, 2, \ldots, m \\ s = r, r+1, \ldots, m \end{pmatrix}.$$

Par suite les coordonnées du polytettarion $(\overline{A}—\overline{B})$, qui sont les mineurs du déterminant des coordonnées de $(A — B)$, sont aussi congrues à zéro mod. a, l'idéal $\mathfrak{A}$ étant un idéal scalaire. Il en résulte

$$\overline{A} \equiv \overline{B} \pmod{\mathfrak{A}}.$$

En vertu du théorème 6 de ce paragraphe, on peut multiplier à gauche ou à droite, membre à membre, les congruences

$$A \equiv B \pmod{\mathfrak{A}} \quad \text{et} \quad \overline{A} \equiv \overline{B} \pmod{\mathfrak{A}};$$

il vient $$N(A) \equiv N(B) \pmod{\mathfrak{A}}.$$

Remarque. Le théorème cesse d'être vrai pour un idéal quelconque du corps Ω comme module, en vertu de la remarque faite au théorème 6 de ce paragraphe.

8. Théorème. — *Il est permis de diviser à droite par un même polytettarion* M *du corps* Ω, *les deux membres d'une congruence suivant un idéal quelconque* $\mathfrak{A}$ *de ce corps, à condition que l'idéal principal Id* $(N(M))$, *où* $N(M)$ *est la norme complexe de* M, *soit premier avec* $\mathfrak{A}$.

En effet, la division à droite par un tettarion M est équivalente à la multiplication à droite par $\overline{M}/N(M)$, c'est-à-dire à la multiplication à droite par $\overline{M}$ (ce qui est toujours permis en vertu de § 3. 3), suivie d'une division par un nombre $N(M)$ du corps K. Cette division n'est permise que si l'idéal principal $(N(M))$ est premier avec le module.

9. Théorème. — *Il est permis de diviser à gauche, par un même tettarion* M *du corps* Ω, *les deux membres d'une congruence suivant un idéal scalaire* $\mathfrak{A}$ *du même corps,*

à condition que l'idéal principal Id $(N(\mathbf{M}))$, *où* $N(\mathbf{M})$ *est la norme complexe de* $\mathbf{M}$, *soit premier avec* $\mathfrak{A}$.

En effet : la division à gauche par un tettarion $\mathbf{M}$ est équivalente à la multiplication à gauche par $\overline{\mathbf{M}}/N(\mathbf{M})$, c'est-à-dire à la multiplication à gauche par $\overline{\mathbf{M}}$ (ce qui n'est permis que si le module est un idéal scalaire — théorème 4 de ce paragraphe), suivie de la division par un nombre $N(\mathbf{M})$ du corps K. Cette dernière n'est permise que si l'idéal principal $(N(\mathbf{M}))$ est premier avec le module.

Remarque. Le théorème cesse d'être vrai si le module est un idéal quelconque, en vertu de la remarque faite au théorème 4 de ce paragraphe.

10. Théorème. — *Si les tettarions réduits* Γ_r *forment un système complet de restes suivant un idéal* $\mathfrak{A}$ *du corps* Ω, *les produits* $\Gamma_r \cdot \mathbf{A}$, *où* $\mathbf{A}$ *est un polytettarion entier du corps* Ω, *en forment aussi un à condition que l'idéal principal Id* $(N(\mathbf{A}))$ *soit premier avec* $\mathfrak{A}$.

Démonstration. Comme le nombre des $\Gamma_r \cdot \mathbf{A}$ est le même que celui des Γ_r, il suffit de montrer que ces produits sont incongrus entre eux modulo $\mathfrak{A}$. Si

$$\Gamma_k \cdot \mathbf{A} \equiv \Gamma_s \cdot \mathbf{A} \pmod{\mathfrak{A}},$$

il s'en suivrait

$$(\Gamma_k - \Gamma_s) \cdot \mathbf{A} \equiv 0 \pmod{\mathfrak{A}}.$$

L'idéal principal $(N(\mathbf{A}))$ étant premier avec $\mathfrak{A}$, on pourrait diviser à droite par $\mathbf{A}$ et l'on obtiendrait

$$\Gamma_k \equiv \Gamma_s \pmod{\mathfrak{A}},$$

ce qui serait contraire à l'hypothèse.

11. Théorème. — *Si les polytettarions* Γ_r *forment un système complet de restes suivant un idéal scalaire,* $\mathfrak{A}$, *du corps* Ω, *les produits* $\mathbf{A} \cdot \Gamma_r$, *où* $\mathbf{A}$ *est un polytettarion entier du corps* Ω, *en forment aussi un, à condition que l'idéal principal Id* $(N(\mathbf{A}))$ *soit premier avec* $\mathfrak{A}$.

Remarque. Ce théorème cesse d'être vrai si le module est un idéal quelconque, en vertu de la remarque faite au théorème 9 de ce paragraphe.

12. Théorème. — La norme $n(\mathfrak{A})$ d'un idéal

$$\mathfrak{A} \equiv \mathrm{Id} \mid \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_r, \ldots, \mathfrak{a}_m \mid$$

du corps Ω est égale au produit

$$[n(\mathfrak{a}_1)]^m [n(\mathfrak{a}_2)]^{m-1} \ldots [n(\mathfrak{a}_r)]^{m-r+1} \ldots [n(\mathfrak{a}_m)]$$

où $n(\mathfrak{a}_r)$ est la norme de l'idéal $\mathfrak{a}_r$ dans le corps K.

Démonstration. Pour que deux entiers $\mathbf{A} = \mid \alpha_{rs} \mid$ et $\mathbf{B} = \mid \beta_{rs} \mid$ du corps Ω soient incongrus entre eux suivant un idéal $\mathfrak{A}$ du corps Ω, il faut et il suffit que, pour chaque indice $r = 1, 2, \ldots, m$, les coordonnées correspondantes α_{rs} et β_{rs} le soient suivant la coordonnée correspondante $\mathfrak{a}_r$ de cet idéal $\mathfrak{A}$ (v. § 2, théorème 8). Dès lors, on obtiendra tous les éléments d'un système de restes modulo $\mathfrak{A}$ en faisant parcourir aux coordonnées γ_{rs} du tettarion $\Gamma = \mid \gamma_{rs} \mid$ tous les éléments d'un système complet de restes mo-

dulo $\mathfrak{a}_r$ dans le corps K, et cela pour chaque indice $r = 1, 2, \ldots, m$ séparément. Il en résulte que la $r^{ième}$ ligne, ayant $m - r + 1$ coordonnées non nulles, nous donne

$$[n(\mathfrak{a}_r)]^{m-r+1}$$

combinaisons ; r doit prendre toutes les valeurs entières de 1 à m ; on obtient ainsi

$$[n(\mathfrak{a}_1)]^{m}[n(\mathfrak{a}_2)]^{m-1}\ldots[n(\mathfrak{a}_r)]^{m-r+1}\ldots\ldots[n(\mathfrak{a}_m)]$$

combinaisons possibles et par suite autant de restes incongrus entre eux modulo $\mathfrak{A}$. Il reste à montrer que tout tettarion du corps Ω est congru à l'un de ces restes, et à un seul. Si c'est le cas, l'ensemble de ces restes formera un système complet de restes modulo $\mathfrak{A}$, et leur nombre sera égal à la norme, $n(\mathfrak{A})$, de l'idéal $\mathfrak{A}$ (v. la définition de la norme § 3. 1). Soit $\mathbf{M} = \mid \mu_{rs} \mid$ un entier quelconque du corps Ω. Il sera congru à l'un des restes $\Gamma = \mid \gamma_{rs} \mid$ suivant l'idéal $\mathfrak{A}$, si les congruences suivantes

$$\mu_{rs} \equiv \gamma_{rs} \pmod{\mathfrak{a}_r} \quad \begin{pmatrix} r = 1, 2, \ldots, m \\ s = r, r+1, \ldots, m \end{pmatrix}$$

sont satisfaites (§ 2 théorème 8). Nous savons par la théorie générale des corps algébriques que chacun des γ_{rs} est univoquement déterminé pour chaque système complet de restes modulo $\mathfrak{a}_r$.

Corollaire. Si $\mathfrak{A} = Id \mid \mathfrak{a}, \mathfrak{a}, \ldots, \mathfrak{a} \mid$ *est un idéal scalaire,*

$$n(\mathfrak{A}) = [n(\mathfrak{a})]^{\frac{m(m+1)}{2}} = [Nn(\mathfrak{a})]^{\frac{m+1}{2}}.$$

Il suffit de faire dans la formule du théorème précédent

$$\mathfrak{a}_1 = \mathfrak{a}_2 = \ldots = \mathfrak{a}_r \ldots = \mathfrak{a}_m.$$

Il vient alors

$$n(\mathfrak{A}) = n(\mathfrak{a})^m n(\mathfrak{a})^{m-1} \ldots n(\mathfrak{a}) = [n(\mathfrak{a})]^{\frac{m(m+1)}{2}}.$$

D'autre part

$$[n(\mathfrak{a})]^m = Nn(\mathfrak{a})$$

d'où

$$n(\mathfrak{A}) = [Nn(\mathfrak{a})]^{\frac{m+1}{2}}$$

13. Théorème. — *La norme d'un produit diagonal de deux idéaux* $\mathfrak{A} = \mathrm{Id} \mid \mathfrak{a}_r \mid$ $\mathfrak{B} = \mathrm{Id} \mid \mathfrak{b}_r \mid$ *du corps* Ω *est égale au produit des normes des facteurs.*

$$n(\mathfrak{A} \cdot \mathfrak{B}) = n(\mathfrak{A}) \cdot n(\mathfrak{B}).$$

En effet

$$n(\mathfrak{A}\mathfrak{B}) = \prod_{r=1}^{m} [n(\mathfrak{a}_r \cdot \mathfrak{b}_r)]^{m-r+1} = \prod_{r=1}^{m} [n(\mathfrak{a}_r) \cdot n(\mathfrak{b}_r)]^{m-r+1}$$

$$= \prod_{r=1}^{m} [n(\mathfrak{a}_r)]^{m-r+1} \cdot [n(\mathfrak{b}_r)]^{m-r+1} = \prod_{r=1}^{m} [n(\mathfrak{a}_r)]^{m-r+1} \cdot \prod_{r=1}^{m} [n(\mathfrak{b}_r)]^{m-r+1}$$

$$= n(\mathfrak{A}) \cdot n(\mathfrak{B}).$$

14. **Définition.** — Envisageons un système complet de restes suivant un idéal $\mathfrak{A}$ du corps Ω. Le nombre de ceux d'entre eux dont les normes complexes, considérées comme des idéaux principaux, sont premières avec $\mathfrak{A}$ s'appellera *l'indicateur d'Euler*, ou *indicateur* tout court de l'idéal $\mathfrak{A}$ du corps Ω. Nous désignerons par $\Phi(\mathfrak{A})$ l'indicateur ainsi défini de l'idéal $\mathfrak{A}$.

15. Théorème. — *Si* $\mathfrak{A}$ *est un idéal du corps* Ω *de la forme particulière*

$$\mathrm{Id} \mid 1, 1, \ldots, 1, \mathfrak{a}_r, 1, \ldots, 1 \mid,$$

on a

$$\Phi(\mathfrak{A}) = \varphi(\mathfrak{a}_r) \cdot [n(\mathfrak{a}_r)]^{m-r}$$

où $\varphi(\mathfrak{a}_r)$ *désigne l'indicateur d'Euler de l'idéal* $\mathfrak{a}_r$ *et* $n(\mathfrak{a}_r)$ *sa norme dans le corps* K.

En effet : les éléments $\Gamma = \mid \gamma_{rs} \mid$ d'un système complet de restes mod. $\mathfrak{A}$ sont, dans notre cas, de la forme

$$\Gamma = \left\{ \begin{array}{l} 1, 1, \ldots, 1, \ldots, 1 \\ 0, 1, \ldots, 1, \ldots, 1 \\ \ldots\ldots\ldots\ldots\ldots \\ 0, 0, \ldots, \gamma_{rr}, \ldots, \gamma_{rm} \\ \ldots\ldots\ldots\ldots\ldots \\ 0, 0, \ldots, 0, \ldots, 1 \end{array} \right\}$$

c'est-à-dire des tettarions dont toutes les coordonnées non nulles sont des 1, sauf celles de la $r^{ième}$ ligne, lesquelles sont

$$\gamma_{rr}, \ \gamma_{r,r+1}, \ldots, \gamma_{r,m}.$$

Chacun des γ_{rs} peut parcourir les $n(\mathfrak{a}_r)$ éléments d'un système complet de restes mod. $\mathfrak{a}_r$ dans le corps K. La norme complexe d'un Γ est égale à γ_{rr}. Envisagée comme idéal principal, elle sera première avec $\mathfrak{A}$, si γ_{rr} est premier avec $\mathfrak{a}_r$. On obtiendra dès lors les restes mod. $\mathfrak{A}$, dont la norme complexe est première avec $\mathfrak{A}$, en faisant parcourir dans le corps K 1) à γ_{rr} les $\varphi(\mathfrak{a}_r)$ éléments d'un système complet de restes mod. $\mathfrak{a}_r$ et premiers avec $\mathfrak{a}_r$ et 2) à chacun des γ_{rs} $(s = r+1, \ldots, m)$ les $n(\mathfrak{a}_r)$ éléments d'un système complet de restes mod. $\mathfrak{a}_r$. Il en résultera

$$\varphi(\mathfrak{a}_r) \cdot [n(\mathfrak{a}_r)]^{m-r}$$

combinaisons possibles et autant de restes incongrus mod. $\mathfrak{A}$, restes dont la norme complexe, envisagée comme idéal principal, sera première avec $\mathfrak{A}$.

16. Théorème. — *Si* $\mathfrak{A} = \mathrm{Id} \mid \mathfrak{a}, \mathfrak{a}, \ldots, \mathfrak{a} \mid$ *est un idéal scalaire du corps* Ω, *on a*

$$\Phi(\mathfrak{A}) = [\varphi(\mathfrak{a})]^m \cdot [n(\mathfrak{a})]^{\frac{m(m-1)}{2}}$$

ce qui peut s'écrire

$$\Phi(\mathfrak{A}) = [N\varphi[(\mathfrak{a})]] \, [N n(\mathfrak{a})]^{\frac{m-1}{2}}.$$

Démonstration. Les éléments d'un système complet de restes mod. $\mathfrak{A}$ sont, dans notre cas, des polytettarions $\Gamma = \mid \gamma_{rs} \mid$ dont chacune des coordonnées γ_{rs} peut prendre chacune des $n(\mathfrak{a})$ valeurs d'un système complet de restes mod. $\mathfrak{a}$ dans le corps K. La

norme complexe, $N(\Gamma)$, d'un de ces restes Γ est égale au produit des coordonnées diagonales γ_{rr}. Envisagée comme idéal principal, cette norme sera première avec $\mathfrak{A}$, si chacune des coordonnées γ_{rr} est première avec $\mathfrak{a}$. On sait qu'il existe $\varphi(\mathfrak{a})$ restes incongrus mod. $\mathfrak{a}$ et premiers avec $\mathfrak{a}$. Dès lors nous obtiendrons tous ceux des éléments d'un système complet de restes mod. $\mathfrak{A}$, dont la norme complexe est première avec $\mathfrak{A}$, en faisant parcourir à chacune des coordonnées γ_{rr} les $\varphi(\mathfrak{a})$ valeurs sus-mentionnées et à chacune des autres coordonnées γ_{rs} $(s \neq r)$ les $n(\mathfrak{a})$ éléments d'un système complet de restes mod. $\mathfrak{a}$. Il en résulte

$$[\varphi(\mathfrak{a})]^m \cdot \prod_{r=1}^{m} [n(\mathfrak{a})]^{m-r}$$

combinaisons possibles. Il vient dès lors :

$$\Phi(\mathfrak{A}) = [\varphi(\mathfrak{a})]^m \cdot \prod_{r=1}^{m} [n(\mathfrak{a})]^{m-r} = [\varphi(\mathfrak{a})]^m \cdot [n(\mathfrak{a})]^{\sum_{r=1}^{m} (m-r)}$$

$$= [\varphi(\mathfrak{a})]^m \cdot [n(\mathfrak{a})]^{\frac{m(m-1)}{2}} = [N\varphi(\mathfrak{a})] \cdot [Nn(\mathfrak{a})]^{\frac{m-1}{2}}.$$

17. **Théorème de Fermat pour un idéal scalaire.** — $\mathfrak{A} = Id \mid \mathfrak{a}, \mathfrak{a}, \ldots, \mathfrak{a} \mid$ *étant un idéal scalaire du corps* Ω *et* A *un polytettarion réduit à gauche dont la norme complexe,* $N(\mathrm{A})$, *envisagée comme un idéal principal, est première avec* $\mathfrak{A}$, *on a la congruence*

$$[N(\mathrm{A})]^{\Phi(\mathfrak{A})} \equiv 1 \pmod{\mathfrak{A}}.$$

Démonstration. Désignons par $\mathrm{B}_1, \mathrm{B}_2, \ldots, \mathrm{B}_t$ les $t \equiv \Phi(\mathfrak{A})$ éléments d'un système complet de restes (mod. $\mathfrak{A}$) dont la norme complexe, envisagée comme un idéal principal, est première avec $\mathfrak{A}$; choisissons les Λ_r tels que

$$\mathrm{A} \cdot \mathrm{B}_r \equiv \Lambda_r \pmod{\mathfrak{A}}. \tag{1}$$

Je dis que les Λ_r forment encore un système complet de restes mod. $\mathfrak{A}$; car si l'on avait

$$\Lambda_k \equiv \Lambda_s \pmod{\mathfrak{A}},$$

il s'en suivrait, en vertu de (1),

$$\mathrm{A} \cdot \mathrm{B}_k \equiv \mathrm{A} \cdot \mathrm{B}_s \pmod{\mathfrak{A}}$$

et par suite (§ 3, théorème 9)

$$\mathrm{B}_k \equiv \mathrm{B}_s \pmod{\mathfrak{A}},$$

contrairement à l'hypothèse.

En plus, les normes complexes des Λ_r sont premières avec $\mathfrak{A}$. Passons des congruences (1) aux suivantes (§ 3, théorème 7)

$$N(\mathrm{A} \cdot \mathrm{B}_r) \equiv N(\Lambda_r) \pmod{\mathfrak{A}} \tag{2}$$

et supposons que $N(\Lambda_r)$, envisagée comme idéal principal, ne soit pas première avec $\mathfrak{A}$; soit $\mathfrak{P}$ leur plus grand facteur idéal diagonal commun de sorte que

$$\mathrm{Id}\ N(\Lambda_r) = \mathfrak{P} \cdot \mathfrak{B} \quad \text{et} \quad \mathfrak{A} = \mathfrak{P} \cdot \mathfrak{C}.$$

Dès lors la congruence

$$\mathrm{Id}\ N(\Lambda_r) \equiv 0 \pmod{\mathfrak{P}}$$

entraînerait la suivante

$$N(\mathrm{A} \cdot \mathrm{B}_r) \equiv 0 \pmod{\mathfrak{P}}$$

et

$$N(\mathrm{A}) \cdot N(\mathrm{B}_r) \equiv 0 \pmod{\mathfrak{P}}$$

ou (§ 3, théorème 9)

$$N(\mathrm{B}_r) \equiv 0 \pmod{\mathfrak{P}},$$

contrairement à l'hypothèse faite sur les normes complexes des B_r. Les considérations précédentes permettent de regarder les Λ_r comme constituant un système complet de restes (mod. $\mathfrak{A}$). Dès lors les Λ_r ne sont autre chose que les B_r pris dans un certain ordre de succession. Multiplions les congruences (2) membre à membre ; il vient

$$\prod_{r=1}^{t} N(\mathrm{AB}_r) \equiv \prod_{r=1}^{t} N(\Lambda_r) \pmod{\mathfrak{A}}$$

d'où, en simplifiant (§ 3, théorème 9),

$$[N(\mathrm{A})]^t \equiv 1 \pmod{\mathfrak{A}}$$

ou

$$[N(\mathrm{A})]^{\Phi(\mathfrak{A})} \equiv 1 \pmod{\mathfrak{A}}$$

Corollaire. N (A) et l'idéal scalaire $\mathfrak{A} = \mathrm{Id} \mid a, a, \ldots, a \mid$ étant des éléments du corps K on a, en vertu de la théorie générale des corps algébriques, la congruence

$$[N(\mathrm{A})]^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{A}}$$

où φ ($\mathfrak{a}$) désigne l'indicateur de l'idéal $\mathfrak{a}$ dans le corps K.

18. **Théorème de Fermat pour un idéal quelconque du corps Ω.** — *Soit* $\mathfrak{A} = Id \mid \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m \mid$ *un idéal quelconque du corps* Ω, *et* $\mathrm{A} = \mid \alpha_{rs} \mid$ *un polytettarion complexe dont les coordonnées diagonales* α_{rr} ($r = 1, 2, \ldots, m$), *envisagées comme idéaux principaux, soient toutes premières avec* $\mathfrak{A}$; *on a la congruence :*

$$[N(\mathrm{A})]^{\varphi(\mathfrak{a}_1) \cdot \varphi(\mathfrak{a}_2) \cdot \ldots \varphi(\mathfrak{a}_r) \cdot \ldots \varphi(\mathfrak{a}_m)} \equiv 1 \pmod{\mathfrak{A}}$$

où φ ($\mathfrak{a}_r$) *désigne l'indicateur de l'idéal* $\mathfrak{a}_r$ *dans le corps* K.

En effet : les idéaux principaux (α_{11}), $(\alpha_{22}), \ldots, (\alpha_{mm})$ sont, par hypothèse, premiers avec l'idéal $\mathfrak{A}$ et par suite avec chacune de ses coordonnées $\mathfrak{a}_r$ ($r = 1, 2, \ldots, m$). Il en résulte, en vertu de la théorie générale des corps algébriques, les congruences :

$$\alpha_{11}^{\varphi(\mathfrak{a}_r)} \equiv 1 \pmod{\mathfrak{a}_r}$$

$$\alpha_{22}^{\varphi(\mathfrak{a}_r)} \equiv 1 \pmod{\mathfrak{a}_r}$$

$$\ldots\ldots\ldots\ldots$$

$$\alpha_{mm}^{\varphi(\mathfrak{a}_r)} \equiv 1 \pmod{\mathfrak{a}_r}$$

et cela pour chaque valeur de $r = 1, 2, \ldots, m$. En multipliant membre à membre ces dernières congruences, il vient :

$$\alpha_{11}^{\varphi(a_r)} \cdot \alpha_{22}^{\varphi(a_r)} \ldots \alpha_{mm}^{\varphi(a_r)} \equiv 1 \pmod{a_r}$$

c'est-à-dire

$$[\alpha_{11} \cdot \alpha_{22} \cdot \ldots \cdot \alpha_{mm}]^{\varphi(a_r)} \equiv 1 \pmod{a_r}$$

ou, puisque $\alpha_{11} \cdot \alpha_{22} \cdot \ldots \alpha_{mm} = N(A)$,

$$[N(A)]^{\varphi(a_r)} \equiv 1 \pmod{a_r}$$

et cela pour $r = 1, 2, \ldots, m$. Par suite

$$[N(A)]^{\varphi(a_1) \cdot \varphi(a_2) \cdot \ldots \cdot \varphi(a_m)} \equiv 1 \pmod{a_r}.$$

En vertu du théorème 8 du paragraphe 2, on a dès lors la congruence

$$[N(A)]^{\varphi(a_1) \cdot \varphi(a_2) \cdot \ldots \cdot \varphi(a_m)} \equiv 1 \pmod{\mathfrak{A}}.$$

Corollaire 1. — En désignant par $\Phi_m(\mathfrak{A})$ *le plus petit commun multiple des m indicateurs* $\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_m)$, *on a la congruence*

$$[N(A)]^{\Phi_m(\mathfrak{A})} \equiv \pmod{\mathfrak{A}}.$$

Corollaire 2. — Si $\mathfrak{A}$ *est un idéal du corps* Ω, *de la forme Id* $\{1, 1, \ldots, 1, a_r, 1, \ldots, 1\}$ *et* A *un tettarion réduit à gauche dont la norme complexe, envisagée comme idéal principal, est première avec* $\mathfrak{A}$, *on a la congruence*

$$[N(A)]^{\varphi(a_r)} \equiv 1 \pmod{\mathfrak{A}},$$

$\varphi(a_r)$ *désignant l'indicateur de* a_r *dans le corps K.* En effet : dans ce cas $\Phi_m(\mathfrak{A})$ est égal à $\varphi(a_r)$.

19. **Congruences linéaires à une inconnue suivant un idéal du corps Ω.** — Nous appellerons *congruence linéaire à gauche à une inconnue* une congruence de la forme

$$\Xi \cdot A \equiv B \pmod{\mathfrak{A}} \qquad (1)$$

où $\mathfrak{A}$ est un idéal du corps Ω, A et B étant des entiers donnés, tandis que Ξ représente une inconnue. Cherchons les conditions nécessaires pour qu'une pareille congruence admette des solutions entières Ξ.

Soit A un tettarion complexe entier du corps Ω dont la norme complexe, $N(A)$, envisagée comme idéal principal, soit première avec $\mathfrak{A}$. Nous savons que dans ce cas, si l'on remplace Ξ successivement par tous les entiers Γ_s d'un système complet de restes modulo $\mathfrak{A}$, on obtient des tettarions entiers réduits à gauche

$$\Gamma_s A \qquad s = 1, 2, \ldots, n(\mathfrak{A})$$

qui forment à leur tour un système complet de restes modulo $\mathfrak{A}$ (v. § 3. 10). Dès lors, le nombre B est congru suivant $\mathfrak{A}$ à l'un de ces entiers et à un seul. Si

$$\Gamma \cdot A \equiv B \pmod{\mathfrak{A}}$$

Γ est une solution de la congruence (1) et c'est la seule comprise dans le système complet de restes considéré. Dans ces hypothèses, tout tettarion de la forme

$$\Gamma + \sum_s \Delta_s Y_s ,$$

où les Δ_s forment une base de l'idéal $\mathfrak{A}$ et où les Y_s sont des tettarions rationnels entiers, est également solution de la congruence (1). La congruence (1) admet ainsi une infinité de solutions.

Le théorème de Fermat permet de trouver une solution particulière de la congruence (1). En effet, par hypothèse, la norme complexe, $N(A)$, envisagée comme idéal principal, est première avec $\mathfrak{A}$. Si $\mathfrak{A}$ est un idéal scalaire du corps Ω, on a

$$[N(A)]^{\Phi(\mathfrak{A})} \equiv 1 \pmod{\mathfrak{A}}.$$

En multipliant à droite la congruence (1) par

$$\overline{A} \cdot [N(A)]^{\Phi(\mathfrak{A})-1}$$

où $\overline{A}$ désigne le conjugué complexe de A, on obtient

$$\Xi \cdot A \cdot \overline{A} [N(A)]^{\Phi(\mathfrak{A})-1} \equiv B \cdot \overline{A} \cdot [N(A)]^{\Phi(\mathfrak{A})-1} \pmod{\mathfrak{A}}$$

ou bien

$$\Xi \equiv B \cdot \overline{A} \cdot [N(A)]^{\Phi(\mathfrak{A})-1} \pmod{\mathfrak{A}}$$

d'où une solution particulière de la congruence (1)

$$\Gamma = B \cdot \overline{A} \cdot [N(A)]^{\Phi(\mathfrak{A})-1} .$$

La solution générale de la congruence (1) est dès lors donnée par la formule

$$\Gamma + \sum_s \Delta_s \cdot Y_s$$

les Δ_s et les Y_s ayant la signification indiquée ci-dessus. En tenant compte du corollaire du théorème de Fermat (§ 3. 17), on obtient une solution particulière plus simple

$$\Gamma = B \cdot \overline{A} \cdot [N(A)]^{\varphi(a)-1} .$$

Si $\mathfrak{A} = \mathrm{Id} \mid a_r \mid$ est un idéal quelconque du corps Ω, un raisonnement analogue au précédent donne une solution particulière de la congruence (1), dans le cas où chacune des coordonnées diagonales de A est première avec $\mathfrak{A}$, sous la forme suivante

$$\Gamma = B \cdot \overline{A} \, [N(A)]^{\Phi_m(\mathfrak{A})-1} .$$

La solution générale de la congruence (1) est alors donnée par la formule

$$\Gamma + \sum_s \Delta_s \cdot Y_s .$$

20. La congruence

$$A \cdot \Xi \equiv B \pmod{\mathfrak{A}}$$

sera dite *congruence linéaire à droite à une inconnue.* Les raisonnements ci-dessus, relatifs aux congruences linéaires à gauche, sont encore valables pour les congruences linéaires à droite, mais seulement dans le cas où l'idéal $\mathfrak{A}$ est un idéal scalaire du corps (v. remarque du théorème 11 de ce paragraphe). Une solution particulière d'une telle congruence est donnée par le théorème de Fermat sous la forme

$$\Gamma = [N(\mathrm{A})]^{\Phi(\mathfrak{A})-1} \cdot \overline{\mathrm{A}} \cdot \mathrm{B}$$

à condition toutefois que la norme complexe, N (A), envisagée comme idéal principal soit première avec $\mathfrak{A}$.

21. *Exemple.* Considérons le corps des duotettarions ($m = 2$) dont les coordonnées sont tirées du corps K ($i = \sqrt{-1}, \sqrt{13}$). Soit la congruence

$$\Xi \cdot \begin{Bmatrix} \dfrac{1+\sqrt{13}}{2}, & \dfrac{1+i+\sqrt{13}+i\sqrt{13}}{2} \\ 0, & \dfrac{1-\sqrt{13}}{2} \end{Bmatrix} \equiv \begin{Bmatrix} 5, & 3 \\ 0, & i \end{Bmatrix}$$

mod. $\mathfrak{A} = \{ \mathrm{Id}\,(2), \mathrm{Id}\,(1+i) \}$.

Les coordonnées diagonales : $\dfrac{1+\sqrt{13}}{2}$ et $\dfrac{1-\sqrt{13}}{2}$, sont premières avec $\mathfrak{A}$. La solution est donnée par la formule

$$\Gamma \equiv \begin{Bmatrix} 5, & 3 \\ 0, & i \end{Bmatrix} \cdot \overline{\begin{Bmatrix} \dfrac{1+\sqrt{13}}{2}, & \dfrac{1+i+\sqrt{13}+i\sqrt{13}}{2} \\ 0, & \dfrac{1-\sqrt{13}}{2} \end{Bmatrix}} \cdot \left[\frac{1+\sqrt{13}}{2} \cdot \frac{1-\sqrt{13}}{2} \right]^{\Phi_m(\mathfrak{A})-1} \quad (\mathrm{mod.}\ \mathfrak{A}).$$

$\Phi_m(\mathfrak{A})$ est le plus petit commun multiple de

$$\varphi(2) \quad \text{et} \quad \varphi(1+i);$$

$\varphi(1+i)$ est l'indicateur d'Euler de l'idéal principal $(1+i)$ du corps K. Nous savons par la théorie des corps algébriques qu'il est égal à

$$n(1+i) - 1$$

où $n(1+i)$ désigne la norme de l'idéal $(1+i)$ dans le corps K. Or

$$n(1+i) = (1+i)(1-i)(1+i)(1-i) = 4.$$

Il s'ensuit

$$\varphi(1+i) = 4 - 1 = 3.$$

De même

$$\varphi(2) = n(2) \cdot \left[1 - \frac{1}{n(1+i)} \right]^2.$$

Comme

$$n(2) = (1+i)^2 = 4^2 = 16,$$

il vient

$$\varphi(2) = 16 \cdot \frac{9}{16} = 9.$$

Il en résulte

$$\Phi_m(\mathfrak{A}) = 9.$$

Dès lors

$$\Gamma \equiv \begin{Bmatrix} 5, & 3 \\ 0, & i \end{Bmatrix} \cdot \begin{Bmatrix} \dfrac{1-\sqrt{13}}{2}, & -\dfrac{(1+\sqrt{13})(1+i)}{2} \\ 0, & \dfrac{1+\sqrt{13}}{2} \end{Bmatrix} \cdot (-3)^8 \pmod{\mathfrak{A}}$$

$$\equiv \begin{Bmatrix} \dfrac{32805(1-\sqrt{13})}{2}, & -\dfrac{6561(2+5i)(1+\sqrt{13})}{2} \\ 0, & \dfrac{6561\,i(1+\sqrt{13})}{2} \end{Bmatrix} \pmod{\mathfrak{A}}$$

En rejetant les multiples de 2 (qui est un nombre de l'idéal $\mathfrak{A}$), on obtient finalement

$$\Gamma \equiv \begin{Bmatrix} \dfrac{-(1-\sqrt{13})}{2}, & -\dfrac{i(1+\sqrt{13})}{2} \\ 0, & \dfrac{i(1+\sqrt{13})}{2} \end{Bmatrix} \pmod{\mathfrak{A}}$$

Vérification.

$$\begin{Bmatrix} \dfrac{-(1-\sqrt{13})}{2}, & -\dfrac{i(1+\sqrt{13})}{2} \\ 0, & \dfrac{i(1+\sqrt{13})}{2} \end{Bmatrix} \cdot \begin{Bmatrix} \dfrac{1+\sqrt{13}}{2}, & \dfrac{(1+i)(1+\sqrt{13})}{2} \\ 0, & \dfrac{1-\sqrt{13}}{2} \end{Bmatrix}$$

$$= \begin{Bmatrix} 3, & 3(1+2i) \\ 0, & -3i \end{Bmatrix}$$

Donc, on doit avoir

$$\begin{Bmatrix} 3, & 3(1+2i) \\ 0, & -3i \end{Bmatrix} \equiv \begin{Bmatrix} 5, & 3 \\ 0, & i \end{Bmatrix} \pmod{\{\mathrm{Id}(2)).\ \mathrm{Id}(1+i)\}},$$

ce qui est le cas, puisque

$$3 - 5 = -2 \equiv 0 \pmod{2}$$
$$3(1+2i) - 3 = 6i \equiv 0 \pmod{2}$$
$$-3i - i = -4i \equiv 0 \pmod{(1+i)} \text{ (v. § 2. 8).}$$

§ 4. Les unités du corps Ω.

1. **Définition.** — Nous appellerons *tettarion unité* ou simplement *unité du corps* Ω tout entier E de ce corps dont le réciproque,

$$E^{-1} \equiv \frac{\overline{E}}{N(E)}$$

est encore un entier du même corps.

Il résulte de cette définition que la norme complexe, N (E), d'une unité E du corps Ω est une unité du corps K et réciproquement : si la norme complexe d'un entier du corps Ω est une unité du corps K, cet entier est une unité du corps Ω.

2. Théorème. — *Toute unité du corps* Ω *est un tettarion réduit dont les coordonnées diagonales sont des unités du corps* K.

En effet, si E est une unité du corps Ω, sa norme complexe, $N(E)$, est égale à une unité ε du corps K. Or, la norme complexe d'un tettarion réduit est égale au produit de ses coordonnées diagonales. Ce produit doit être égal à ε. Il s'ensuit que les coordonnées diagonales d'une unité de Ω sont des unités du corps K, les coordonnées non diagonales pouvant être des entiers quelconques du corps K. Dans le cas général, E est donc de la forme

$$E = \left\{ \begin{array}{cccc} \varepsilon_1, & \alpha_{12}, & \alpha_{13}, \ldots\ldots, & \alpha_{1m} \\ 0, & \varepsilon_2, & \alpha_{23}, \ldots\ldots, & \alpha_{2m} \\ 0, & 0, & \varepsilon_3, \ldots\ldots, & \alpha_{3m} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0, & 0, & 0, \ldots\ldots, & \varepsilon_m \end{array} \right\} \quad \ldots\ldots\ldots \quad (1)$$

où les ε_k (pour $k = 1, 2, \ldots, m$) désignent des unités du corps K, les α_{ks} étant des entiers quelconques du corps K.

3. Théorème. — *Toute unité* E *du corps* Ω *est un produit à droite d'un nombre diagonal unité par une unité du corps* Ω *dont les coordonnées diagonales sont des 1.*

Démonstration. Soit E une unité du corps Ω ; elle est de la forme (1). Dès lors (v. corol. du § 2. 4)

$$E = \left\{ \begin{array}{cccc} \varepsilon_1, & 0, & 0, \ldots\ldots, & 0 \\ 0, & \varepsilon_2, & 0, \ldots\ldots, & 0 \\ 0, & 0, & \varepsilon_3, \ldots\ldots, & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0, & 0, & 0, \ldots\ldots, & \varepsilon_m \end{array} \right\} \cdot \left\{ \begin{array}{cccc} 1, & \frac{\alpha_{12}}{\varepsilon_1}, & \frac{\alpha_{13}}{\varepsilon_1}, \ldots\ldots, & \frac{\alpha_{1m}}{\varepsilon_1} \\ 0, & 1, & \frac{\alpha_{23}}{\varepsilon_2}, \ldots\ldots, & \frac{\alpha_{2m}}{\varepsilon_2} \\ 0, & 0, & 1, \ldots\ldots, & \frac{\alpha_{3m}}{\varepsilon_3} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0, & 0, & 0, \ldots\ldots, & 1 \end{array} \right\}$$

Or, les ε_r étant des unités du corps K, les nombres

$$\frac{\alpha_{rs}}{\varepsilon_r}$$

sont des entiers du même corps ; désignons les par β_{rs}

$$\frac{\alpha_{rs}}{\varepsilon_r} \equiv \beta_{rs} .$$

Il vient

$$\mathrm{E} = \left| \varepsilon_1, \varepsilon_2, \ldots\ldots, \varepsilon_m \right| . \left\{ \begin{array}{cccc} 1, & \beta_{12}, & \beta_{13}, \ldots\ldots, & \beta_{1m} \\ 0, & 1, & \beta_{23}, \ldots\ldots, & \beta_{2m} \\ 0, & 0, & 1, \ldots\ldots, & \beta_{3m} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0, & 0, & 0, \ldots\ldots, & 1 \end{array} \right\} .$$

En posant pour abréger

$$\left\} \varepsilon_r \right\{ \equiv \left\} \varepsilon_1, \varepsilon_2, \ldots\ldots, \varepsilon_m \right\{$$

et

$$\mathrm{E}' \equiv \left\{ \begin{array}{cccc} 1, & \beta_{12}, & \beta_{13}, \ldots\ldots, & \beta_{1m} \\ 0, & 1, & \beta_{23}, \ldots\ldots, & \beta_{2m} \\ 0, & 0, & 1, \ldots\ldots, & \beta_{3m} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0, & 0, & 0, \ldots\ldots, & 1 \end{array} \right\} \quad \ldots\ldots\ldots \quad (2)$$

on obtient

$$\mathrm{E} = \left| \varepsilon_r \right| . \mathrm{E}' .$$

4. **Définition.** — Désignons par E_r une unité du corps Ω définie comme suit : 1) Les coordonnées diagonales de E_r sont toutes égales à 1 ; 2) en même temps, les coordonnées non diagonales de E_r sont nulles sauf celles de la $r^{ième}$ ligne, lesquelles peuvent être des entiers quelconques du corps K. Par exemple :

$$\mathrm{E}_3 = \left\{ \begin{array}{ccccc} 1, & 0, & 0, & 0, \ldots\ldots, & 0 \\ 0, & 1, & 0, & 0, \ldots\ldots, & 0 \\ 0, & 0, & 1, & \beta_{34}, \ldots\ldots, & \beta_{3m} \\ 0, & 0, & 0, & 1, \ldots\ldots, & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0, & 0, & 0, & 0, \ldots\ldots, & 1 \end{array} \right\} \quad \ldots\ldots\ldots \quad (3)$$

5. Théorème. — *Dans le corps* Ω, *toute unité de la forme* (2) *est un produit d'unités de la forme spéciale* E_r, *prises dans un ordre de succession déterminé*, savoir

$$\mathrm{E}' = \mathrm{E}_{m-1} . \mathrm{E}_{m-2} \ldots . \mathrm{E}_r \ldots . \mathrm{E}_2 . \mathrm{E}_1 .$$

Ce théorème est une conséquence du théorème 6, paragraphe 2.

6. **Définition.** — Soient e_{rs} *les unités relatives* du corps Ω définies au § 1. 1 et $[\omega_1, \omega_2, \omega_3, \omega_4]$ une base du corps K définie au § 1. 4. Posons

$$E_{rs}^{(k)} \equiv 1 + \omega_k \cdot e_{rs} \qquad \begin{matrix} r = 1,2,\ldots, m \\ s = r, r+1,\ldots, m \\ k = 1, 2, 3, 4. \end{matrix}$$

Cette unité est de la forme

$$E_{rs}^{(k)} = \begin{matrix} \\ \left\{ \begin{matrix} 1, & 0, & 0,\ldots, & 0,\ldots, & 0,\ldots, & 0 \\ 0, & 1, & 0,\ldots, & 0,\ldots, & 0,\ldots, & 0 \\ 0, & 0, & 1,\ldots, & 0,\ldots, & 0,\ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & 0,\ldots, & 1,\ldots, & \omega_k,\ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & 0,\ldots, & 0,\ldots, & 1,\ldots & 0, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & 0,\ldots, & 0,\ldots, & 0,\ldots & 1, \end{matrix} \right. \end{matrix} \begin{matrix} 1 \\ 2 \\ 3 \\ . \\ r \\ . \\ s \\ . \\ m \end{matrix}$$

7. Théorème.

$$\left[E_{rs}^{(k)}\right]^a = 1 + a \cdot \omega_k \cdot e_{rs}.$$

Ce théorème se démontre directement par le calcul.

8. Théorème. — *Toute unité du corps* Ω *de la forme* E_u *définie au* 4 *de ce paragraphe est un produit de puissances des* $E_{rs}^{(k)}$.

Pour abréger l'écriture nous supprimerons les zéros et les 1 superflus et n'écrirons que les coordonnées de la $u^{ième}$ ligne de E_u ; nous utiliserons les crochets [] afin d'éviter la confusion avec les nombres diagonaux. Ainsi, l'unité

$$E_3 \equiv \left\{ \begin{matrix} 1, & 0, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0, & 0 \\ 0, & 0, & 1, & \beta_{34}, & \beta_{35} \\ 0, & 0, & 0, & 1, & 0 \\ 0, & 0, & 0, & 0, & 1 \end{matrix} \right\} \text{sera représentée par } [1, \beta_{34}, \beta_{35}].$$

Dans le cas général

$$E_u = [1, \beta_{u,\,u+1}, \beta_{u,\,u+2}, \beta_{u,\,u+3},\ldots\ldots, \beta_{u,\,m}].$$

Les β_{rs} sont des entiers quelconques du corps K ; ils sont tous de la forme

$$\beta_{rs} = c_1^{(rs)} \cdot \omega_1 + c_2^{(rs)} \cdot \omega_2 + c_3^{(rs)} \cdot \omega_3 + c_4^{(rs)} \cdot \omega_4.$$

Pour rendre la démonstration plus claire, nous supposerons $m = 8$ (le corps des octotettarions complexes) et $u = 4$. Dès lors

$$E_4 = [1, \beta_{45}, \beta_{46}, \beta_{47}, \beta_{48}].$$

On constate par le calcul que, d'une part,

$$E_4 = [1, \beta_{45}, 0, 0, 0].[1, 0, \beta_{46}, 0, 0].[1, 0, 0, \beta_{47}, 0].[1, 0, 0, 0, \beta_{48}]$$

et que, d'autre part

$$[1, \beta_{45}, 0, 0, 0] = [1, c_1^{(45)}.\omega_1, 0, 0, 0].[1, c_2^{(45)}.\omega_2, 0, 0, 0].[1, c_3^{(45)}.\omega_3, 0, 0, 0].[1, c_4^{(45)}.\omega_4, 0, 0, 0],$$

. . . . . ,

. . . . . ,

$$[1, 0, 0, 0, \beta_{48}] = [1, 0, 0, 0, c_1^{(48)}.\omega_1].[1, 0, 0, 0, c_2^{(48)}.\omega_2].[1, 0, 0, 0, c_3^{(48)}.\omega_3].[1, 0, 0, 0, c_4^{(48)}.\omega_4].$$

On a, en outre, d'après le théorème précédent

$$\begin{aligned}
[1, c_1^{(45)}.\omega_1, 0, 0, 0] &= [E_{45}^{(1)}]^{c_1^{(45)}}, \\
[1, c_2^{(45)}.\omega_2, 0, 0, 0] &= [E_{45}^{(2)}]^{c_2^{(45)}}, \\
&\cdots\cdots\cdots \\
[1, 0, 0, c_3^{(47)}.\omega_3, 0] &= [E_{47}^{(3)}]^{c_3^{(47)}}, \\
&\cdots\cdots\cdots \\
[1, 0, 0, 0, c_4^{(48)}.\omega_4] &= [E_{48}^{(4)}]^{c_4^{(48)}}.
\end{aligned}$$

Il s'ensuit que

$$\begin{aligned}
E_4 &= [E_{45}^{(1)}]^{c_1^{(45)}}.[E_{45}^{(2)}]^{c_2^{(45)}}.[E_{45}^{(3)}]^{c_3^{(45)}}\ldots.[E_{46}^{(4)}]^{c_4^{(46)}}\ldots.[E_{48}^{(4)}]^{c_4^{(48)}} \\
&= \prod_{k=1}^{4}[E_{45}^{(k)}]^{c_k^{(45)}}.\prod_{k=1}^{4}[E_{46}^{(k)}]^{c_k^{(46)}}.\prod_{k=1}^{4}[E_{47}^{(k)}]^{c_k^{(47)}}.\prod_{k=1}^{4}[E_{48}^{(k)}]^{c_k^{(48)}}.
\end{aligned}$$

Dans le cas général

$$E_n = \prod_{k=1}^{4}[E_{n,n+1}^{(k)}]^{c_k^{(n,n+1)}}.\prod_{k=1}^{4}[E_{n,n+2}^{(k)}]^{c_k^{(n,n+2)}}\ldots.\prod_{k=1}^{4}[E_{(n,m)}^{(k)}]^{c_k^{(n,m)}}.$$

Exemple. Dans le corps des tritettarions réduits à gauche ($m = 3$), on a

$$\begin{aligned}
&\begin{Vmatrix} 1, & \Sigma a_k.\omega_k, & \Sigma b_k.\omega_k \\ 0, & 1, & \Sigma c_k.\omega_k \\ 0, & 0, & 1 \end{Vmatrix} = \begin{Vmatrix} 1, & 0, & 0 \\ 0, & 1, & \Sigma c_k.\omega_k \\ 0, & 0, & 1 \end{Vmatrix}.\begin{Vmatrix} 1, & \Sigma a_k.\omega_k, & \Sigma b_k.\omega_k \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{Vmatrix} \\
&= \prod_{k=1}^{4}\begin{Vmatrix} 1, & 0, & 0 \\ 0, & 1, & c_k.\omega_k \\ 0, & 0, & 1 \end{Vmatrix}.\prod_{k=1}^{4}\begin{Vmatrix} 1, & a_k.\omega_k, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{Vmatrix}.\prod_{k=1}^{4}\begin{Vmatrix} 1, & 0, & b_k.\omega_k \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{Vmatrix} \\
&= \prod_{k=1}^{4}\begin{Vmatrix} 1, & 0, & 0 \\ 0, & 1, & \omega_k \\ 0, & 0, & 1 \end{Vmatrix}^{c_k}.\prod_{k=1}^{4}\begin{Vmatrix} 1, & \omega_k, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{Vmatrix}^{a_k}.\prod_{k=1}^{4}\begin{Vmatrix} 1, & 0, & \omega_k \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{Vmatrix}^{b_k}
\end{aligned}$$

$$= [E_{23}^{(1)}]^{c_1}.[E_{23}^{(2)}]^{c_2}.[E_{23}^{(3)}]^{c_3}.[E_{23}^{(4)}]^{c_4}.[E_{12}^{(1)}]^{a_1}.[E_{12}^{(2)}]^{a_2}.[E_{12}^{(3)}]^{a_3}.[E_{12}^{(4)}]^{a_4}.[E_{13}^{(1)}]^{b_1}.[E_{13}^{(2)}]^{b_2}.[E_{13}^{(3)}]^{b_3}.[E_{13}^{(4)}]^{b_4}.$$

9. Théorème. — *Toute unité du corps* Ω *peut se mettre sous la forme d'un produit dont les facteurs sont*

1) des nombres diagonaux unités ;

2) des unités du corps Ω de la forme spéciale $E_{rs}^{(k)}$.

Ce théorème est une conséquence des théorèmes 3, 5 et 8 de ce paragraphe.

10. Il semble impossible[1] d'exprimer les unités $E_{rs}^{(k)}$ en fonction les unes des autres sans faire usage des polytettarions unités généraux, donc sans sortir du corps Ω des tettarions réduits à gauche. On peut dès lors dire que l'ensemble des unités $E_{rs}^{(k)}$ est multiplicativement irréductible dans notre corps de polytettarions complexes réduits à gauche.

Définition. — Nous appellerons *système d'unités fondamentales du corps* Ω, le système des unités $E_{rs}^{(k)}$ élargi par l'adjonction des $m.n$ unités fondamentales du sous-corps des nombres diagonaux. Les éléments qui forment ce système seront dits *des unités fondamentales du corps* Ω.

11. Théorème. — Le nombre des éléments d'un système d'unités fondamentales du corps Ω est égal à

$$2\,m.(m-1)+m.n=m.(2\,m-2+n)$$

où n est le nombre des éléments d'un système d'unités fondamentales du corps K.

Démonstration. Pour calculer ce nombre, il suffit de déterminer :

1) le nombre des unités d'un système d'unités fondamentales du corps Ω_d des nombres diagonaux ; il est égal à

$$m.n\,;$$

2) le nombre, dans le corps Ω, des unités de la forme spéciale

$$E_{rs}^{(k)}\begin{pmatrix} r=1,\,2,\ldots,\,m \\ s=r+1,\,r+2,\ldots,\,m \\ k=1,\,2,\,3,\,4 \end{pmatrix}.$$

Calculons ce nombre. Dans l'indice rs de l'unité $E_{rs}^{(k)}$ en question, r est le numéro de la ligne et s celui de la colonne, occupées par ω_k qui figure dans l'expression de $E_{rs}^{(k)}$ (v. § 4. 6). Soit r l'un des nombres 1, 2, ..., m, arbitrairement choisi mais fixe. Dans la $r^{ième}$ ligne, ω_k peut occuper $m-r$ places différentes, savoir, à droite de la diagonale principale, la place de chacune des coordonnées non-diagonales. Il s'ensuit que pour chacune des valeurs de l'indice r, il y a $4\,(m-r)$ possibilités, donc $4\,(m-r)$ unités $E_{rs}^{(k)}$ différentes, puisque le raisonnement est valable pour ω_1, ω_2, ω_3 et ω_4. Or, r peut prendre toutes les valeurs entières de 1 à m ; on obtient donc, pour le nombre des unités $E_{rs}^{(k)}$, l'expression

---

[1] Du Pasquier, *Zahlentheorie der Tettarionen*, § 7 et § 8.

$$\sum_{r=1}^{m} 4\,(m-r)$$

$$= 4 \sum_{r=1}^{m-1} (m-r) = 4\,|\,(m-1) + (m-2) + (m-3) + \ldots + 2 + 1\,|$$

$$= 4 \,.\, \frac{m\,.\,(m-1)}{2} = 2\,.\,m\,.\,(m-1).$$

Un système d'unités fondamentales du corps Ω contient donc

$$2\,(m-1) + m\,.\,n = m\,(2\,m - 2 + n)$$

éléments.

Remarque. Dans la démonstration précédente nous avons admis que la base du corps K contient $k = 4$ entiers. Mais si toute base du corps K contenait $k \neq 4$ nombres entiers, ce qui est le cas général, le nombre des éléments d'un système d'unités fondamentales du corps Ω serait égal à

$$\frac{k\,.\,m\,(m-1)}{2} + m\,n = \frac{1}{2}\,m\,(k\,m - k + 2n).$$

En effet, dans ce cas, le nombre des unités $E_{rs}^{(k)}$ serait

$$\sum_{r=1}^{m} k\,(m-r) = k \sum_{r=1}^{m} (m-r) = k\,.\,|\,(m-1) + (m-2) + \ldots + 2 + 1\,|$$

$$= k\,.\,\frac{m\,(m-1)}{2}\,.$$

Lausanne. — Imp. La Concorde