

SUR LES CORPS  
ALGÈBRIQUES

J. CRIZE

UNAM



3864

TESIS-BCCT

GXJ  
1932  
I-3

3864



INSTITUTO DE GEOLOGIA  
BIBLIOTECA





SUR LES  
**CORPS ALGÈBRIQUES**

DONT LES NOMBRES S'EXPRIMENT RATIONNELLEMENT  
À L'AIDE DE

**RACINES CARRÉES**

ET SUR LES

**QUATERNIONS COMPLEXES**

THÈSE

PRÉSENTÉE À LA FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE NEUCHÂTEL  
POUR OBTENIR LE GRADE DE DOCTEUR ÈS SCIENCES

PAR

**JEAN GRIZE**

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES



INSTITUTO DE GEOLOGIA  
BIBLIOTECA

*La présente publication est un résumé de la thèse susmentionnée  
Le manuscrit complet de la thèse est déposé à l'Université de Neuchâtel*



LAUSANNE  
IMPRIMERIE LA CONCORDE  
1932



GEOFISICA

*1 ejemplar  
96 p.*

*3864*

CLASIF 512.168465  
ADQUIS Zf. 269  
FECHA .....  
PROCED. ....  
\$ .....

GXJ  
1932  
I-3

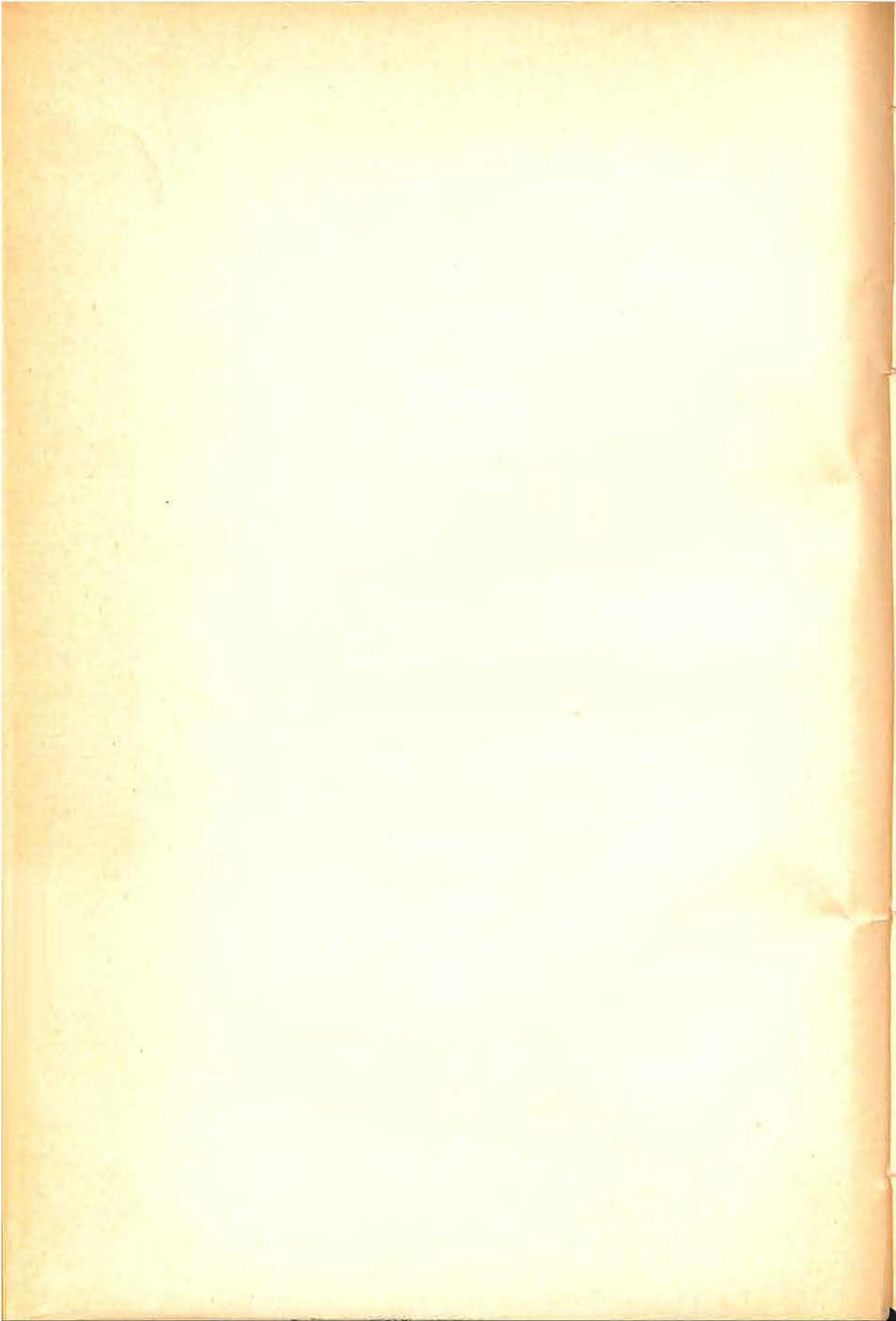
UNIVERSITÉ DE NEUCHÂTEL  
FACULTÉ DES SCIENCES

La Faculté des Sciences de l'Université de Neuchâtel, sur le rapport de MM. les professeurs L.-G. DU PASQUIER et L. GABEREL, autorise l'impression de la présente thèse sans exprimer d'opinion sur les propositions qui y sont contenues.

Neuchâtel, mai 1932.

*Le Doyen :*  
L.-GUSTAVE DU PASQUIER.

*A mon cher professeur,  
Monsieur L.-Gustave Du Pasquier,  
Hommage d'affectueuse reconnaissance  
JEAN GRIZE.*

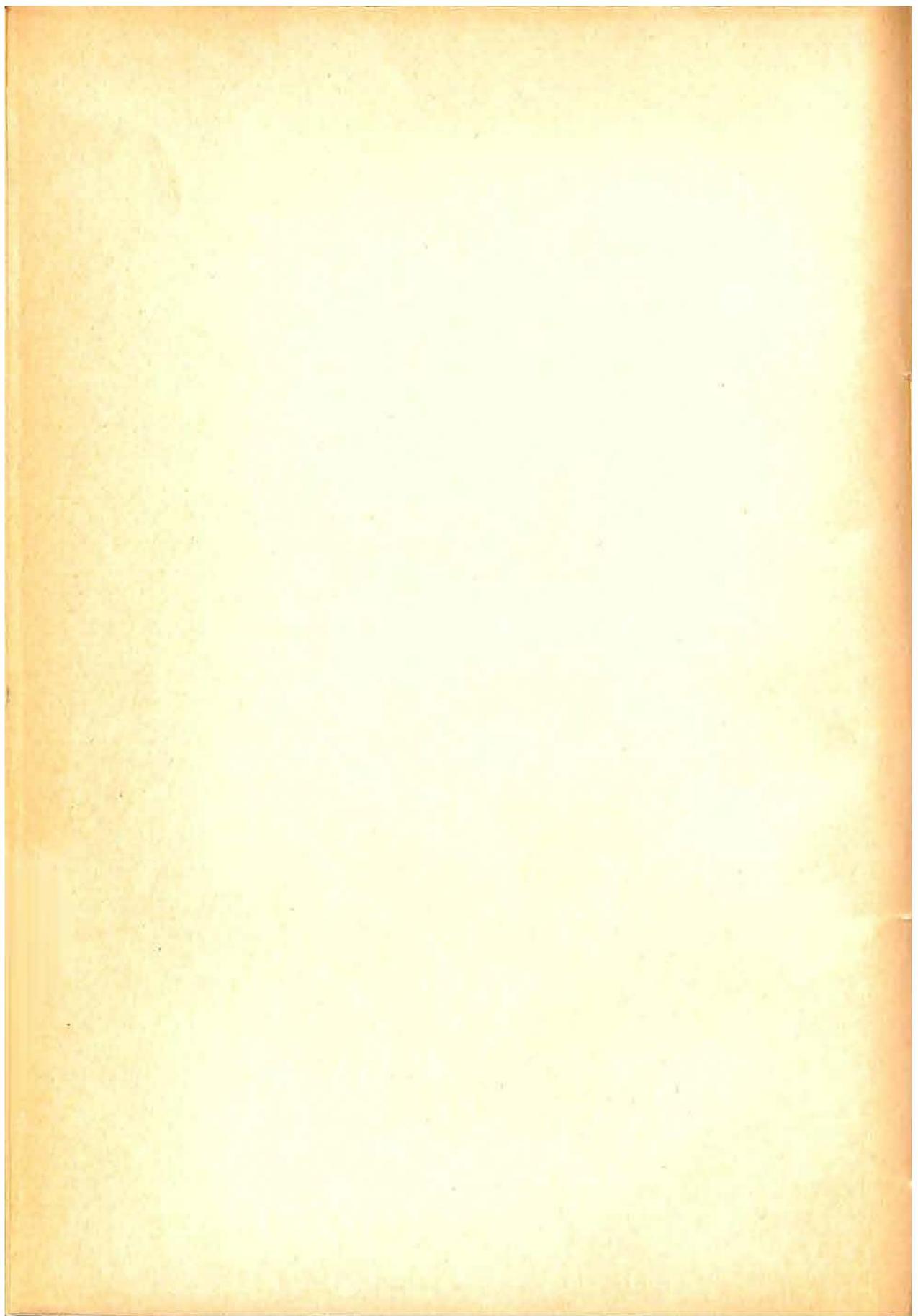


L'idée du présent travail m'a été suggérée par

Monsieur le professeur *L.-Gustave Du Pasquier*.

Qu'il veuille bien trouver ici l'expression de ma vive gratitude pour les conseils qu'il m'a donnés et pour l'intérêt qu'il m'a témoigné au cours de mes travaux.

JEAN GRIZE.



## INTRODUCTION

---

Un *corps de nombres* est un ensemble de grandeurs se reproduisant par quatre opérations dites addition, soustraction, multiplication et division (les « opérations fondamentales »). Par exemple, l'ensemble des nombres rationnels forme un corps de nombres, le plus simple de tous ; nous le désignerons par  $R$ .

Si l'on adjoint à un corps donné  $K$  un élément  $\alpha$  qui n'y est pas contenu, ainsi que toutes les grandeurs qui prennent naissance quand on combine  $\alpha$  avec les éléments de  $K$  à l'aide des opérations fondamentales, on obtient un corps plus général,  $K'$ , entièrement déterminé par  $K$  et  $\alpha$  ; il contient, en particulier, tous les éléments de  $K$ .

Adjoignons par exemple à  $R$ , corps des nombres rationnels, le nombre  $i \equiv \sqrt{-1}$  ; on obtient le corps des nombres complexes ordinaires de la forme  $x + yi$ , où  $x$  et  $y$  sont des nombres rationnels.

Considérons une équation algébrique, supposée irréductible, de la forme

$$(1) \quad x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n = 0.$$

Adjoignons au corps  $R$  une racine  $\alpha$  de l'équation (1). Par cette adjonction, nous obtenons un corps algébrique de degré  $n$ . La théorie des corps algébriques a été exposée par D. Hilbert dans son ouvrage magistral « Théorie des Corps de nombres algébriques »\* auquel je renvoie le lecteur.

Si l'on adjoint au corps  $R$  des nombres rationnels deux racines carrées,  $\sqrt{p}$  et  $\sqrt{q}$ , où  $p$  et  $q$  sont deux nombres entiers ordinaires, positifs ou négatifs et ne contenant aucun facteur carré, on obtient

\* D. Hilbert, « Théorie des Corps de nombres algébriques », ouvrage traduit de l'allemand par A. Lévy et Th. Got, Paris, 1913.

un corps algébrique  $K(\sqrt{p}, \sqrt{q})$  de degré 4; ce corps contient tous les nombres de la forme  $x_0 + x_1\sqrt{p} + x_2\sqrt{q} + x_3\sqrt{pq}$ , où  $x_0, x_1, x_2$  et  $x_3$  sont rationnels, et ne contient que ces nombres-là. Les corps de cette forme ont été étudiés par M. E.-J. Amberg dans sa thèse de doctorat intitulée : « Über den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen ». Zurich, 1897.

M. le professeur L.-G. Du Pasquier m'a proposé d'étudier les corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  dont les nombres s'expriment à l'aide de trois racines carrées :  $\sqrt{A}, \sqrt{B}, \sqrt{C}$ , où  $A, B$  et  $C$  sont trois nombres entiers ordinaires, positifs ou négatifs et dont aucun ne contient un facteur carré. Ces corps sont du huitième degré. Dans le cours de mes travaux, j'ai été amené à étendre mes recherches aux corps dont les nombres s'expriment rationnellement à l'aide de  $n$  racines carrées; ces corps sont algébriques de degré  $2^n$ .

L'étude de ces corps-là fait l'objet de la première partie de ce mémoire.

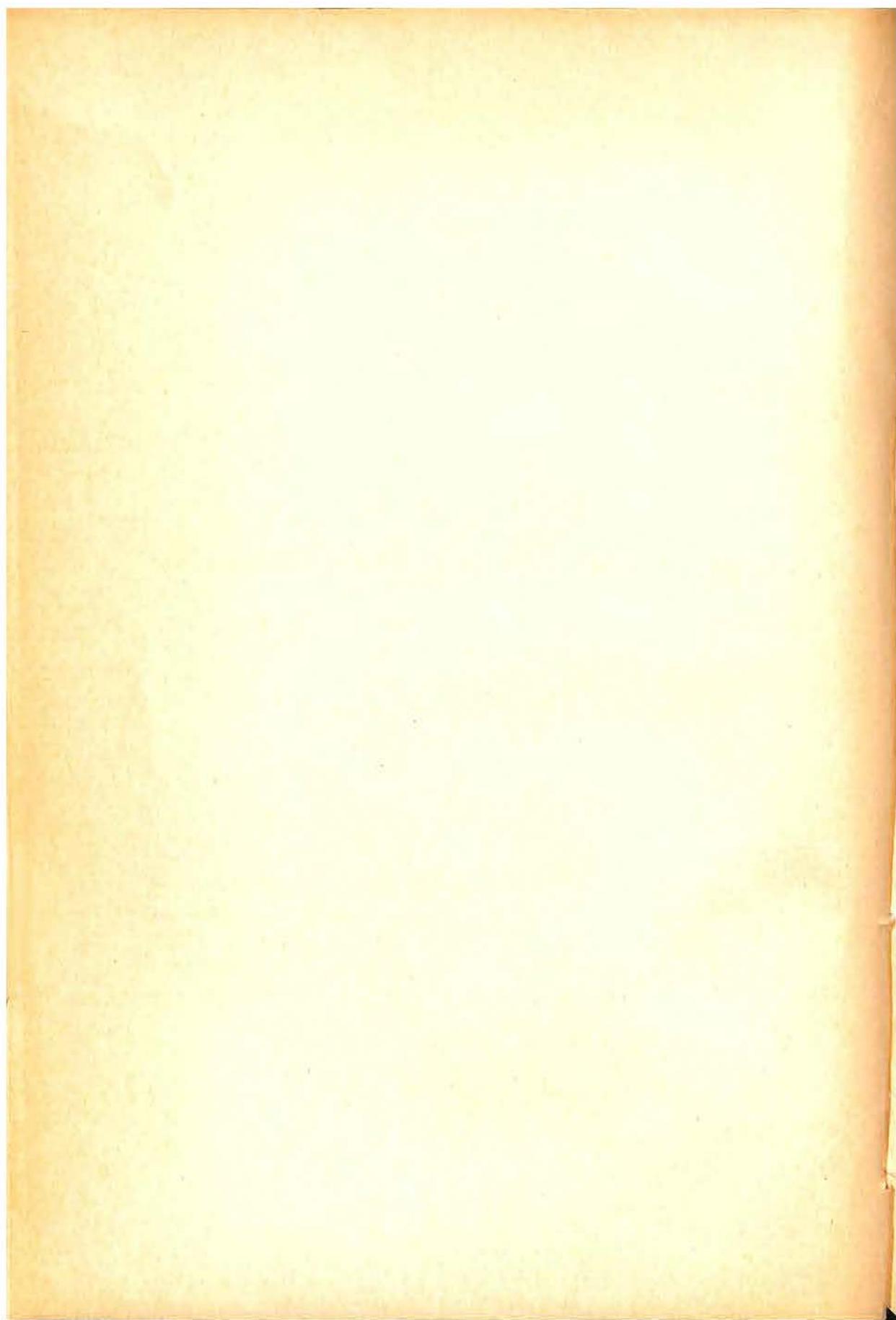
Sur la proposition de M. L.-G. Du Pasquier, j'étudie dans la seconde partie de ce travail les quaternions à coordonnées tirées du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  de degré 8. Ces quaternions sont appelés *quaternions complexes*, par opposition aux quaternions à coordonnées rationnelles dits *quaternions rationnels*.\*

Les quaternions complexes présentent plusieurs particularités. Tout d'abord, comme dans le cas des quaternions rationnels, la multiplication n'est en général pas commutative. En outre, tandis que dans le corps des quaternions rationnels tous les idéaux sont principaux, le domaine  $\Omega$  des quaternions complexes contient des idéaux non principaux. Suivant en cela l'exemple de M. Boris Seitz\*\*, j'ai modifié la définition classique de l'idéal. J'appelle *idéal* dans le domaine des quaternions complexes, et je représente par  $\mathfrak{A} \equiv \text{id } \mathfrak{a}$ , l'ensemble infini des quaternions complexes dont les quatre coordonnées parcourent, indépendamment les unes des autres, les nombres de l'idéal  $\mathfrak{a}$  du corps primordial  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Cette définition de l'idéal m'a permis de simplifier beaucoup la théorie de la divisibilité. J'ai généralisé ensuite la théorie des congruences et obtenu le théorème de Fermat étendu au domaine des quaternions complexes.

\* On entend par *quaternions hamiltoniens* les quaternions dont les coordonnées sont des nombres réels. D'après cela, un « quaternion complexe », au sens que nous donnons à ce mot, peut être quaternion hamiltonien ou non.

\*\* Boris Seitz, *Sur l'arithmomie des nombres de Weierstrass généralisés* et de quelques systèmes de polytettarions complexes. Thèse, Neuchâtel, 1926.

- Dans mes recherches, j'ai utilisé surtout les ouvrages suivants :
- D. HILBERT, *Théorie des corps de nombres algébriques*, traduit de l'allemand par A. Lévy et Th. Got, Paris, 1913.
- J. SOMMER, *Introduction à la théorie des nombres algébriques*, traduit de l'allemand par A. Lévy, Paris, 1911.
- E. CAHEN, *Théorie des nombres*, t. I. Paris, 1914 ; t. II. Paris 1924.
- P.-G.-LEJEUNE DIRICHLET, *Vorlesungen über Zahlentheorie*, herausgegeben von R. Dedekind, 3<sup>ième</sup> édition, Braunschweig, 1879.
- L.-G. DU PASQUIER, *Zahlentheorie der Tettarionen* ; Inaugural-Dissertation, Zurich, 1896.
- L.-G. DU PASQUIER, *Sur l'arithmétique des nombres hypercomplexes*. L'Enseignement mathématique, Genève, 1916.
- E.-J. AMBERG, *Über den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen*. Inaugural-Dissertation, Zurich, 1897.
- A. HURWITZ, *Vorlesungen über die Zahlentheorie der Quaternionen*. Berlin, 1919.
- NIELS NIELSEN, *Tables numériques des équations de Lagrange*, Copenhague et Paris, 1925.
-



## PREMIÈRE PARTIE

### Sur les corps algébriques dont les nombres s'expriment rationnellement à l'aide de racines carrées.

#### CHAPITRE PREMIER

1. Envisageons le corps de nombres formé en partant des trois racines carrées  $\sqrt{A}$ ,  $\sqrt{B}$  et  $\sqrt{C}$ , où  $A$ ,  $B$  et  $C$  représentent trois nombres entiers ordinaires, positifs ou négatifs et dont aucun ne contient un facteur carré. Désignons ce corps de nombres par  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  ou simplement par  $K$ .

Tout nombre  $\omega$  de  $K$  pourra s'écrire

$$\omega = m_0 + m_1\sqrt{A} + m_2\sqrt{B} + m_3\sqrt{C} + m_4\sqrt{AB} + m_5\sqrt{BC} \\ + m_6\sqrt{CA} + m_7\sqrt{ABC}.$$

Désignons par  $s$  le plus grand commun diviseur des trois nombres  $A$ ,  $B$  et  $C$  pris dans leur ensemble, de sorte que l'on ait

$$A = A's, \quad B = B's, \quad C = C's$$

où les entiers  $A'$ ,  $B'$  et  $C'$  sont premiers entre eux dans leur ensemble.

Si l'on pose encore

$$(A'/B') = q; \quad (B'/C') = r; \quad (C'/A') = p,$$

où  $(x/y)$  désigne le plus grand commun diviseur de  $x$  et de  $y$ , on voit que les trois nombres  $q$ ,  $r$  et  $p$  sont premiers entre eux deux à deux.

Si l'on désigne alors par  $a$ ,  $b$  et  $c$  trois entiers appropriés qui dépendent de  $A$ ,  $B$  et  $C$ , le nombre  $\omega$  peut s'écrire comme suit :

$$\text{I. 1.} \quad \omega = c_0 + c_1\sqrt{apqs} + c_2\sqrt{bqrs} + c_3\sqrt{crps} + c_4\sqrt{abrp} \\ + c_5\sqrt{bcpq} + c_6\sqrt{caqr} + c_7\sqrt{abcs},$$

expression dans laquelle les  $c_i$  sont des nombres rationnels et où les

produits  $apqs$ ,  $bqrs$ , ...,  $abcs$  sont des entiers dont aucun ne contient plus de facteur carré.

Le corps  $K$  ainsi défini est un corps algébrique du huitième degré.

2. Chacun des sept radicaux  $\sqrt{apqs}$ ,  $\sqrt{bqrs}$ ,  $\sqrt{crps}$ ,  $\sqrt{abrp}$ ,  $\sqrt{bcpq}$ ,  $\sqrt{caqr}$  et  $\sqrt{abcs}$  ayant deux déterminations, nous choisirons ces déterminations de telle manière que le produit des sept radicaux ait le même signe que le produit  $abcpqrs$ .

3. *Notations.* Soit  $a$  un entier quelconque. Pour désigner ce même entier débarrassé de ses facteurs carrés, nous écrirons  $\bar{a}$ . De même,  $\sqrt{\bar{a}}$  désignera la racine carrée du nombre  $a$  débarrassé préalablement de ses facteurs carrés.

Il suit de là qu'un nombre quelconque  $\omega$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  peut s'écrire :

$$\omega = m_0 + m_1 \sqrt{A} + m_2 \sqrt{B} + m_3 \sqrt{C} + m_4 \sqrt{AB} + m_5 \sqrt{BC} \\ + m_6 \sqrt{CA} + m_7 \sqrt{ABC}.$$

4. *Permutations du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .* Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est entièrement déterminé par les trois racines carrées  $\sqrt{A}$ ,  $\sqrt{B}$  et  $\sqrt{C}$ , les déterminations de ces radicaux ayant été choisies comme il a été dit plus haut (v. § 2).

Nous désignerons alors par  $\varphi_1$  la permutation qui change  $\sqrt{A}$  en  $-\sqrt{A}$ , ce qui entraîne le changement de  $\sqrt{CA}$  en  $-\sqrt{CA}$ , de  $\sqrt{AB}$  en  $-\sqrt{AB}$  et de  $\sqrt{ABC}$  en  $-\sqrt{ABC}$ .

$\varphi_2$  désignera la permutation qui change  $\sqrt{B}$  en  $-\sqrt{B}$  et, par suite,  $\sqrt{AB}$  en  $-\sqrt{AB}$ ,  $\sqrt{BC}$  en  $-\sqrt{BC}$  et  $\sqrt{ABC}$  en  $-\sqrt{ABC}$ .

$\varphi_3$  désignera la permutation qui change  $\sqrt{C}$  en  $-\sqrt{C}$  et, par suite,  $\sqrt{BC}$  en  $-\sqrt{BC}$ ,  $\sqrt{CA}$  en  $-\sqrt{CA}$  et  $\sqrt{ABC}$  en  $-\sqrt{ABC}$ .

$\varphi_4$  désignera la permutation qui change simultanément  $\sqrt{A}$  en  $-\sqrt{A}$  et  $\sqrt{B}$  en  $-\sqrt{B}$  et, par suite,  $\sqrt{CA}$  en  $-\sqrt{CA}$  et  $\sqrt{BC}$  en  $-\sqrt{BC}$ .

$\varphi_5$  désignera la permutation qui change simultanément  $\sqrt{B}$  en  $-\sqrt{B}$  et  $\sqrt{C}$  en  $-\sqrt{C}$  et, par suite,  $\sqrt{AB}$  en  $-\sqrt{AB}$  et  $\sqrt{CA}$  en  $-\sqrt{CA}$ .

$\varphi_6$  désignera la permutation qui change simultanément  $\sqrt{C}$  en  $-\sqrt{C}$  et  $\sqrt{A}$  en  $-\sqrt{A}$  et, par suite,  $\sqrt{AB}$  en  $-\sqrt{AB}$  et  $\sqrt{BC}$  en  $-\sqrt{BC}$ .

Enfin  $\varphi_7$  désignera la permutation qui change simultanément  $\sqrt{A}$  en  $-\sqrt{A}$ ,  $\sqrt{B}$  en  $-\sqrt{B}$  et  $\sqrt{C}$  en  $-\sqrt{C}$  et, par suite,  $\sqrt{ABC}$  en  $-\sqrt{ABC}$ .

Si l'on désigne, en outre, par  $\varphi_0$  la permutation identique qui ne change aucune des déterminations des sept radicaux  $\sqrt{A}$ ,  $\sqrt{B}$ , ...

...,  $\sqrt{ABC}$ , on voit que le nombre total des permutations du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est égal au nombre total des combinaisons des trois nombres  $A, B$  et  $C$  pris un à un, puis deux à deux, puis trois à trois ; ce nombre est donc bien

$$\binom{3}{1} + \binom{3}{2} + \binom{3}{3} = 7.$$

5. *Conjugués, norme.* — Soit  $\omega$  un nombre du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Mettons  $\omega$  sous la forme

$$\omega = c_0 + c_1 \sqrt{apqs} + c_2 \sqrt{bqrs} + c_3 \sqrt{crps} + c_4 \sqrt{abrp} + c_5 \sqrt{bcpq} \\ + c_6 \sqrt{caqr} + c_7 \sqrt{abcs}.$$

Si on applique au nombre  $\omega$  ci-dessus les sept permutations  $\varphi_1, \varphi_2, \dots, \varphi_7$ , du § 4, on obtient les sept nombres

$$\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(7)}$$

qui sont dits les *conjugués* de  $\omega$ .

Le produit de  $\omega$  par ses sept conjugués est un nombre rationnel dit la *norme* de  $\omega$  ; nous écrirons

$$\omega \omega^{(1)} \omega^{(2)} \dots \omega^{(7)} = N(\omega).$$

Si l'on applique à tous les nombres du corps  $K$  les permutations  $\varphi_1, \varphi_2, \dots, \varphi_7$ , on obtient les *corps conjugués* de  $K$ . Nous les désignerons par  $K^{(1)}, K^{(2)}, \dots, K^{(7)}$ .

Les sept corps conjugués de  $K$  étant identiques à  $K$ , ce dernier corps est un *corps normal* du huitième degré.

6. *Sous-corps.* Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  ou  $K(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps})$  a sept sous-corps quadratiques dont les bases sont

$$(1, \sqrt{apqs}); (1, \sqrt{bqrs}); (1, \sqrt{crps}); (1, \sqrt{abrp}); (1, \sqrt{bcpq}); \\ (1, \sqrt{caqr}); (1, \sqrt{abcs}).$$

Le corps  $K(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps})$  a également sept sous-corps du 4<sup>e</sup> degré \*. Ce sont

$$K_1(1, \sqrt{bqrs}, \sqrt{crps}, \sqrt{bcpq}); K_2(1, \sqrt{apqs}, \sqrt{crps}, \sqrt{caqr}); \\ K_3(1, \sqrt{apqs}, \sqrt{bqrs}, \sqrt{abrp}); K_4(1, \sqrt{crps}, \sqrt{abrp}, \sqrt{abcs}); \\ K_5(1, \sqrt{apqs}, \sqrt{bcpq}, \sqrt{abcs}); K_6(1, \sqrt{bqrs}, \sqrt{caqr}, \sqrt{abcs}); \\ K_7(1, \sqrt{abrp}, \sqrt{bcpq}, \sqrt{caqr}).$$

Les indices des sous-corps  $K_1, K_2, \dots, K_7$  ont été choisis de telle manière que la permutation  $\varphi_\lambda$ , d'indice  $\lambda$ , laisse inchangé précisément le sous-corps  $K_\lambda$  de même indice.

\* Ils ont été étudiés par M. E.-J. Amberg, « Über den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen », Zurich, 1897.

Il en résulte qu'étant donné un nombre quelconque  $\omega$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , si on applique à ce nombre  $\omega$  la permutation  $\varphi_\lambda$  qui transforme  $\omega$  en  $\omega^{(\lambda)}$ , le produit  $\omega\omega^{(\lambda)}$  est un nombre du sous-corps  $K_\lambda$ .

7. *Première généralisation, le corps du seizième degré.* Envisageons le corps de nombres formé en partant de quatre racines carrées  $\sqrt{A_1}$ ,  $\sqrt{A_2}$ ,  $\sqrt{A_3}$  et  $\sqrt{A_4}$ , où  $A_1$ ,  $A_2$ ,  $A_3$  et  $A_4$  représentent quatre nombres entiers ordinaires, positifs ou négatifs et dont aucun ne contient un facteur carré. Désignons ce corps par  $K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$  ou simplement par  $K$ .

Tout nombre  $\omega$  du corps  $K$  peut s'écrire

$$\begin{aligned} \omega = & m_0 + m_1 \sqrt{A_1} + m_2 \sqrt{A_2} + m_3 \sqrt{A_3} + m_4 \sqrt{A_4} \\ & + m_5 \sqrt{A_1 A_2} + m_6 \sqrt{A_1 A_3} + m_7 \sqrt{A_1 A_4} + m_8 \sqrt{A_2 A_3} + m_9 \sqrt{A_2 A_4} + m_{10} \sqrt{A_3 A_4} \\ & + m_{11} \sqrt{A_1 A_2 A_3} + m_{12} \sqrt{A_1 A_2 A_4} + m_{13} \sqrt{A_1 A_3 A_4} + m_{14} \sqrt{A_2 A_3 A_4} \\ & + m_{15} \sqrt{A_1 A_2 A_3 A_4}. \end{aligned}$$

Soit, comme plus haut (v. § 1),  $s$  le plus grand commun diviseur des quatre nombres  $A_1$ ,  $A_2$ ,  $A_3$  et  $A_4$  pris dans leur ensemble, de sorte que l'on ait

$$I. 2. \quad A_1 = A'_1 s; \quad A_2 = A'_2 s; \quad A_3 = A'_3 s; \quad A_4 = A'_4 s,$$

où les entiers  $A'_1$ ,  $A'_2$ ,  $A'_3$  et  $A'_4$  sont premiers entre eux dans leur ensemble.

Désignons ensuite par  $d_1$ ,  $d_2$ ,  $d_3$  et  $d_4$  les p. g. c. d. des entiers  $A'_1$ ,  $A'_2$ ,  $A'_3$  et  $A'_4$  pris trois à trois, ce qu'on écrira

$$(A'_1/A'_2/A'_3) = d_4; \quad (A'_1/A'_2/A'_4) = d_3; \quad (A'_1/A'_3/A'_4) = d_2; \quad (A'_2/A'_3/A'_4) = d_1,$$

où  $(x/y/z)$  signifie « le p. g. c. d. des nombres  $x$ ,  $y$  et  $z$  pris dans leur ensemble ».

On voit que les nombres  $d_1$ ,  $d_2$ ,  $d_3$  et  $d_4$  sont premiers entre eux deux à deux. On peut alors écrire, si l'on désigne par  $A''_1$ ,  $A''_2$ ,  $A''_3$  et  $A''_4$  quatre facteurs appropriés qui dépendent de  $A_1$ ,  $A_2$ ,  $A_3$  et  $A_4$  mais sans facteur carré aucun,

$$I. 3. \quad A_1 = A''_1 d_2 d_3 d_4; \quad A_2 = A''_2 d_1 d_3 d_4; \quad A_3 = A''_3 d_1 d_2 d_4; \quad A_4 = A''_4 d_1 d_2 d_3,$$

expressions dans lesquelles les nombres  $A''_1$ ,  $A''_2$ ,  $A''_3$  et  $A''_4$  sont premiers entre eux trois à trois.

Désignons enfin par  $\delta_1$ ,  $\delta_2$ ,  $\delta_3$ ,  $\delta_4$ ,  $\delta_5$ ,  $\delta_6$  les p. g. c. d. des nombres  $A''_1$ ,  $A''_2$ ,  $A''_3$  et  $A''_4$  pris deux à deux, ce qu'on écrira

$$\begin{aligned} (A''_1/A''_2) = \delta_1; \quad (A''_1/A''_3) = \delta_2; \quad (A''_1/A''_4) = \delta_3 \\ (A''_2/A''_3) = \delta_4; \quad (A''_2/A''_4) = \delta_5; \quad (A''_3/A''_4) = \delta_6. \end{aligned}$$

Les formules précédentes montrent que les nombres  $\delta_\lambda$  sont premiers entre eux deux à deux. On peut alors écrire

$$I. 4. \quad A_1'' = a_1 \delta_1 \delta_2 \delta_3; \quad A_2'' = a_2 \delta_1 \delta_4 \delta_5; \quad A_3'' = a_3 \delta_2 \delta_4 \delta_6; \quad A_4'' = a_4 \delta_3 \delta_5 \delta_6,$$

où les  $a_\lambda$  désignent quatre nombres appropriés qui dépendent des  $A_\lambda''$  et sont premiers entre eux deux à deux.

On voit finalement qu'on peut écrire, en s'appuyant sur les formules I. 2, I. 3 et I. 4,

$$I. 5. \quad \begin{aligned} A_1 &= a_1 \delta_1 \delta_2 \delta_3 d_2 d_3 d_4 s \\ A_2 &= a_2 \delta_1 \delta_4 \delta_5 d_1 d_3 d_4 s \\ A_3 &= a_3 \delta_2 \delta_4 \delta_6 d_1 d_2 d_4 s \\ A_4 &= a_4 \delta_3 \delta_5 \delta_6 d_1 d_2 d_3 s. \end{aligned}$$

On obtient alors

$$I. 6. \quad \begin{aligned} \overline{A_1 A_2} &= a_1 a_2 \delta_2 \delta_3 \delta_4 \delta_5 d_1 d_2; & \overline{A_1 A_3} &= a_1 a_3 \delta_1 \delta_3 \delta_4 \delta_6 d_1 d_3 \\ \overline{A_1 A_4} &= a_1 a_4 \delta_1 \delta_2 \delta_5 \delta_6 d_1 d_4; & \overline{A_2 A_3} &= a_2 a_3 \delta_1 \delta_2 \delta_5 \delta_6 d_2 d_3 \\ \overline{A_2 A_4} &= a_2 a_4 \delta_1 \delta_3 \delta_4 \delta_6 d_2 d_4; & \overline{A_3 A_4} &= a_3 a_4 \delta_2 \delta_3 \delta_4 \delta_5 d_3 d_4 \\ \overline{A_1 A_2 A_3} &= a_1 a_2 a_3 \delta_3 \delta_5 \delta_6 d_4 s; & \overline{A_1 A_2 A_4} &= a_1 a_2 a_4 \delta_3 \delta_4 \delta_6 d_3 s \\ \overline{A_1 A_3 A_4} &= a_1 a_3 a_4 \delta_1 \delta_4 \delta_5 d_2 s; & \overline{A_2 A_3 A_4} &= a_2 a_3 a_4 \delta_1 \delta_2 \delta_3 d_1 s \\ \overline{A_1 A_2 A_3 A_4} &= a_1 a_2 a_3 a_4 d_1 d_2 d_3 d_4. \end{aligned}$$

Aucun des produits  $\overline{A_1 A_2}, \dots, \overline{A_1 A_2 A_3 A_4}$  ne contient un facteur carré.

Il résulte de ce qui précède que tout nombre  $\omega$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  peut se mettre sous la forme

$$\begin{aligned} \omega &= c_0 + c_1 \sqrt{A_1} + c_2 \sqrt{A_2} + c_3 \sqrt{A_3} + c_4 \sqrt{A_4} \\ &\quad + c_5 \sqrt{A_1 A_2} + c_6 \sqrt{A_1 A_3} + c_7 \sqrt{A_1 A_4} + c_8 \sqrt{A_2 A_3} + c_9 \sqrt{A_2 A_4} + c_{10} \sqrt{A_3 A_4} \\ &\quad + c_{11} \sqrt{A_1 A_2 A_3} + c_{12} \sqrt{A_1 A_2 A_4} + c_{13} \sqrt{A_1 A_3 A_4} + c_{14} \sqrt{A_2 A_3 A_4} \\ &\quad + c_{15} \sqrt{A_1 A_2 A_3 A_4}, \end{aligned}$$

expression dans laquelle les nombres qui figurent sous les radicaux ont les valeurs données par les formules I. 5 et I. 6.

8. *Sous-corps quadratiques et sous-corps du huitième degré du corps  $K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$ .* Le corps  $K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$  admet  $2^{4-1} - 1 = 15$  sous-corps quadratiques et 15 sous-corps du huitième degré.

9. *Permutations du corps  $K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$ .* On voit, en procédant comme dans le cas du corps du 8<sup>e</sup> degré (v. § 4), que le corps

$K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$  admet  $\binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 15$  permutations.

Nous les désignerons par  $\varphi_1, \varphi_2, \dots, \varphi_{15}$  et nous adjoindrons à ces quinze permutations la permutation  $\varphi_0$  qui transforme le corps  $K$  en lui-même.

10. *Conjugués, norme.* Etant donné un nombre  $\omega$  du corps  $K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$ , on appelle *conjugués de  $\omega$* , et on représente par  $\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(15)}$ , les quinze nombres obtenus en appliquant à  $\omega$  successivement les quinze permutations  $\varphi_1, \varphi_2, \dots, \varphi_{15}$  du corps  $K(\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \sqrt{A_4})$ .

Le produit  $\omega \omega^{(1)} \omega^{(2)} \dots \omega^{(15)}$ , du nombre  $\omega$  par ses quinze conjugués, est un nombre rationnel dit la *norme de  $\omega$* . Nous la désignerons par  $N(\omega)$ .

Si on applique à tous les nombres du corps  $K$  les quinze permutations  $\varphi_1, \varphi_2, \dots, \varphi_{15}$ , on obtient les *corps conjugués de  $K$* ; nous les désignerons par  $K^{(1)}, K^{(2)}, \dots, K^{(15)}$ . Ils sont identiques. Dès lors, le corps  $K$  est un corps normal du 16<sup>e</sup> degré.

11. *Corps de degré  $2^n$ .* En partant de  $n$  racines carrées

$$\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \dots, \sqrt{A_n}.$$

où les  $A_j$  sont  $n$  entiers ordinaires, positifs ou négatifs et dont aucun ne contient un facteur carré, on définit le corps  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$  de degré  $2^n$ .

Ce corps admet  $2^n - 1$  sous-corps quadratiques et également  $2^n - 1$  sous-corps de degré  $2^{n-1}$ .

Le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  admet  $2^n$  permutations  $\varphi_0, \varphi_1, \dots, \varphi_{m-1}$ , où  $m \equiv 2^n$ .

Si on applique à un nombre  $\omega$  du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  les  $2^n - 1$  permutations  $\varphi_1, \varphi_2, \dots, \varphi_{m-1}$ , on obtient les *conjugués de  $\omega$* , conjugués que nous désignerons par

$$\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(m-1)}, \text{ où } m \equiv 2^n.$$

Le produit  $\omega \omega^{(1)} \omega^{(2)} \dots \omega^{(m-1)}$ , du nombre  $\omega$  par ses  $2^n - 1$  conjugués, est un nombre rationnel dit la *norme de  $\omega$* . Nous la désignerons par  $N(\omega)$ .

Si l'on applique à tous les nombres du corps  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$  les  $2^n - 1$  permutations  $\varphi_1, \varphi_2, \dots, \varphi_{m-1}$ , où  $m \equiv 2^n$ , on obtient les *corps conjugués de  $K$* ; nous les désignerons par

$$K^{(1)}, K^{(2)}, \dots, K^{(m-1)}.$$

## CHAPITRE II

### Les entiers du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

1. *Forme générale des entiers.* Désignons par  $\omega$  un nombre supposé entier dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , et mettons  $\omega$  sous la forme I. 1. Posons, pour simplifier l'écriture,

$$\text{II. 1. } a_1 \equiv apqs; a_2 \equiv bqrs; a_3 \equiv crps; a_4 \equiv abrp; a_5 \equiv bcpq; \\ a_6 \equiv caqr; a_7 \equiv abcs.$$

Le nombre  $\omega$  prend la forme

$$\text{II. 2. } \omega = c_0 + c_1 \sqrt{a_1} + c_2 \sqrt{a_2} + c_3 \sqrt{a_3} + c_4 \sqrt{a_4} + c_5 \sqrt{a_5} \\ + c_6 \sqrt{a_6} + c_7 \sqrt{a_7}.$$

Appliquons aux deux membres de l'égalité précédente les sept permutations  $\varphi_1, \varphi_2, \dots, \varphi_7$  (v. ch. I. 4); on obtient les conjugués de  $\omega$ , savoir:  $\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(7)}$  (v. ch. I. 5).

Formons les sept nombres :

$$\text{II. 3. } \begin{aligned} \Omega_1 &\equiv \omega + \omega^{(1)} = 2c_0 + 2c_2 \sqrt{a_2} + 2c_3 \sqrt{a_3} + 2c_5 \sqrt{a_5} \\ \Omega_2 &\equiv \omega + \omega^{(2)} = 2c_0 + 2c_1 \sqrt{a_1} + 2c_3 \sqrt{a_3} + 2c_6 \sqrt{a_6} \\ \Omega_3 &\equiv \omega + \omega^{(3)} = 2c_0 + 2c_1 \sqrt{a_1} + 2c_2 \sqrt{a_2} + 2c_4 \sqrt{a_4} \\ \Omega_4 &\equiv \omega + \omega^{(4)} = 2c_0 + 2c_3 \sqrt{a_3} + 2c_4 \sqrt{a_4} + 2c_7 \sqrt{a_7} \\ \Omega_5 &\equiv \omega + \omega^{(5)} = 2c_0 + 2c_1 \sqrt{a_1} + 2c_5 \sqrt{a_5} + 2c_7 \sqrt{a_7} \\ \Omega_6 &\equiv \omega + \omega^{(6)} = 2c_0 + 2c_2 \sqrt{a_2} + 2c_6 \sqrt{a_6} + 2c_7 \sqrt{a_7} \\ \Omega_7 &\equiv \omega + \omega^{(7)} = 2c_0 + 2c_4 \sqrt{a_4} + 2c_5 \sqrt{a_5} + 2c_6 \sqrt{a_6} \end{aligned}$$

Les nombres  $\Omega_\lambda$  sont entiers dans les sous-corps du 4<sup>e</sup> degré dont ils font partie.

Désignons par  $\sqrt{a}$  et  $\sqrt{b}$  deux racines carrées déterminant un corps  $K(\sqrt{a}, \sqrt{b})$  du 4<sup>e</sup> degré,  $a$  et  $b$  étant deux entiers ordinaires, positifs ou négatifs, ne contenant aucun facteur carré. Tout nombre  $\theta$  du corps  $K(\sqrt{a}, \sqrt{b})$  a la forme

$$\theta = x + y\sqrt{a} + z\sqrt{b} + t\sqrt{ab},$$

où  $x, y, z$  et  $t$  sont des nombres rationnels.

Posons encore  $\sqrt{c} \equiv \sqrt{ab}$  et le nombre  $\theta$  s'écrit

$$\text{II. 4.} \quad \theta = x + y\sqrt{a} + z\sqrt{b} + t\sqrt{c}.$$

Or, on sait \* que le nombre  $\theta$  (formule II. 4) est entier dans le corps  $K(\sqrt{a}, \sqrt{b})$  dans les trois cas suivants :

- $\alpha$ ) Si  $x, y, z$  et  $t$  sont quatre nombres entiers ordinaires.
- $\beta$ ) Si l'un ou plusieurs des quatre nombres  $x, y, z$  et  $t$  sont des fractions irréductibles de dénominateur 2, les autres étant des entiers ordinaires.
- $\gamma$ ) Si les quatre nombres  $x, y, z$  et  $t$  sont des fractions irréductibles de dénominateur 4.

Dans le cas  $\gamma$ ), l'hypothèse que le nombre II. 4 est entier dans le corps  $K(\sqrt{a}, \sqrt{b})$  entraîne les congruences

$$a \equiv b \equiv c \equiv 1 \pmod{4}.$$

Si on applique ce qui précède aux nombres  $\Omega_\lambda$  (formules II. 3), on arrive à la conclusion suivante :

Tout entier du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  peut être mis sous la forme suivante :

$$\text{II. 5.} \quad \omega = \frac{h_0 + h_1 \sqrt{apqs} + h_2 \sqrt{bqrs} + h_3 \sqrt{crps} + h_4 \sqrt{abrp} + h_5 \sqrt{bcprq} + h_6 \sqrt{caqr} + h_7 \sqrt{abcs}}{8}$$

1° Si les sept produits  $apqs, bqrs, \dots, abcs$  ne sont pas tous congrus à 1 modulo 4, les  $h_\lambda$ , dans l'expression II. 5, sont des nombres entiers ordinaires pairs. (Ils peuvent d'ailleurs, comme cas particuliers, être tous divisibles par 4 ou par 8).

2° Si les sept produits  $apqs, bqrs, \dots, abcs$  sont tous congrus à 1 modulo 4, les  $h_\lambda$  sont des entiers de même parité (en particulier, si un seul des nombres  $h_\lambda$  est impair, ils sont tous impairs).

2. Forme générale des entiers du corps  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$ . En procédant dans ce cas comme au § précédent, on arrive au résultat suivant :

La forme générale des entiers du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  de degré  $2^n$  est

$$\text{II. 6.} \quad \omega = \frac{h_0 + h_1 \sqrt{a_1} + h_2 \sqrt{a_2} + \dots + h_{m-1} \sqrt{a_{m-1}}}{2^n}$$

où l'on a posé

$$a_1 \equiv A_1, \quad a_2 \equiv A_2, \quad \dots, \quad a_n \equiv A_n, \quad a_{n+1} \equiv A_1 A_2, \quad \dots, \\ a_{m-1} \equiv A_1 A_2 \dots A_n \text{ et } m \equiv 2^n.$$

Comme pour le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , deux cas sont à distinguer :

\* Voir Amberg, op. cit., § 2.

1° Si les nombres  $a_\lambda$  ( $\lambda = 1, 2, \dots, m-1$ ) ne sont pas tous congrus à 1 modulo 4, tous les  $h_\lambda$ , dans l'expression II. 6, sont des nombres entiers ordinaires *pairs*.

2° Si, au contraire, les  $m-1$  nombres  $a_\lambda$  sont tous congrus à 1 modulo 4, les entiers  $h_\lambda$ , dans l'expression II. 6, sont de *même parité*.

BASE DES ENTIERS DU CORPS  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

3. Nous devons distinguer les quatre cas suivants :

- a) Les trois nombres  $A, B$  et  $C$  sont congrus à 1 modulo 4.
- b) Deux des trois nombres  $A, B, C$  sont congrus à 1 modulo 4.
- c) Un seul des trois nombres  $A, B, C$  est congru à 1 modulo 4.
- d) Aucun des trois nombres  $A, B, C$  n'est congru à 1 modulo 4.

4. *Cas a.* Les trois nombres  $A, B$  et  $C$  sont congrus à 1 modulo 4.

Dans ce cas, on a les sept congruences suivantes :

$$apqs \equiv bqrs \equiv crps \equiv abrp \equiv bcpq \equiv caqr \equiv abcs \equiv 1 \pmod{4}.$$

On voit facilement, en outre, que l'on peut toujours supposer satisfaites les sept autres congruences suivantes :

$$ps \equiv qs \equiv rs \equiv pq \equiv qr \equiv rp \equiv pqrs \equiv 1 \pmod{4}.$$

Il résulte de ces dernières congruences que l'on a

$$ps + rs + rp - 3 \equiv 0 \pmod{8}.$$

Désignons par  $\omega$  un nombre entier du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

Mettons  $\omega$  sous la forme II. 5.

$$\omega = \frac{h_0 + h_1\sqrt{apqs} + h_2\sqrt{bqrs} + h_3\sqrt{crps} + h_4\sqrt{abrp} + h_5\sqrt{bcpq} + h_6\sqrt{caqr} + h_7\sqrt{abcs}}{8}$$

où les  $h_\lambda$  sont des entiers de même parité.

Formons le nombre

$$\omega_7 = \frac{1 + \sqrt{apqs} + \sqrt{bqrs} + \sqrt{crps} + \sqrt{abrp} + \sqrt{bcpq} + \sqrt{caqr} + \sqrt{abcs}}{8}.$$

Le nombre  $\omega_7$  est entier dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . On le voit en mettant  $\omega_7$  sous la forme

$$\begin{aligned} \omega_7 = & \frac{1 + \sqrt{apqs} + \sqrt{bqrs} + \sqrt{abrp}}{4} \cdot \frac{1 + \sqrt{crps}}{2} - \frac{ps-1}{4} \cdot \frac{1 + \sqrt{caqr}}{2} \\ & - \frac{rs-1}{4} \cdot \frac{1 + \sqrt{bcpq}}{2} - \frac{rp-1}{4} \cdot \frac{1 + \sqrt{abcs}}{2} + \frac{ps + rs + rp - 3}{8}. \end{aligned}$$

Le nombre  $\omega - h_7\omega_7$  est donc aussi entier dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , et l'on a

$$\text{II. 7. } \omega - h_7\omega_7 = \frac{h_0 - h_7 + (h_1 - h_7)\sqrt{apqs} + \dots + (h_6 - h_7)\sqrt{caqr}}{8}.$$

Or, on a vu plus haut que les entiers  $h_\lambda$  sont de même parité (v. ch. II. 1). Les différences  $h_\lambda - h_7$  sont donc divisibles par 2. En posant

$$h_\lambda - h_7 = 2h'_\lambda \quad \text{pour } \lambda = 0, 1, \dots, 6,$$

l'égalité II. 7 peut s'écrire

$$\omega - h_7\omega_7 = \frac{h'_0 + h'_1\sqrt{apqs} + h'_2\sqrt{bqrs} + h'_3\sqrt{crps} + h'_4\sqrt{abrp} + h'_5\sqrt{bcpq} + h'_6\sqrt{caqr}}{4}.$$

Si l'on pose maintenant

$$\omega_4 \equiv \frac{1 + \sqrt{apqs} + \sqrt{bqrs} + \sqrt{abrp}}{4}; \quad \omega_5 \equiv \frac{1 + \sqrt{bqrs} + \sqrt{crps} + \sqrt{bcpq}}{4};$$

$$\omega_6 \equiv \frac{1 + \sqrt{crps} + \sqrt{apqs} + \sqrt{caqr}}{4},$$

les trois nombres  $\omega_4$ ,  $\omega_5$  et  $\omega_6$  sont entiers dans les corps du 4<sup>e</sup> degré dont ils font partie\*.

On forme alors le nombre  $\omega - h_7\omega_7 - h'_6\omega_6 - h'_5\omega_5 - h'_4\omega_4$ . Ce nombre peut s'écrire

$$\text{II. 8. } \omega - h_7\omega_7 - h'_6\omega_6 - h'_5\omega_5 - h'_4\omega_4 = \frac{H_0 + H_1\sqrt{apqs} + H_2\sqrt{bqrs} + H_3\sqrt{crps}}{4},$$

expression dans laquelle les  $H_\lambda$  sont des entiers ordinaires. On démontre que les entiers  $H_0$ ,  $H_1$ ,  $H_2$  et  $H_3$  sont pairs. Si l'on pose alors

$$H_\lambda \equiv 2H'_\lambda, \quad \text{pour } \lambda = 0, 1, 2, 3,$$

le nombre II. 8 s'écrit

$$\omega - h_7\omega_7 - h'_6\omega_6 - h'_5\omega_5 - h'_4\omega_4 = \frac{H'_0 + H'_1\sqrt{apqs} + H'_2\sqrt{bqrs} + H'_3\sqrt{crps}}{2}.$$

Posons enfin

$$\omega_3 \equiv \frac{1 + \sqrt{crps}}{2}; \quad \omega_2 \equiv \frac{1 + \sqrt{bqrs}}{2}; \quad \omega_1 \equiv \frac{1 + \sqrt{apqs}}{2},$$

les trois nombres  $\omega_1$ ,  $\omega_2$  et  $\omega_3$  sont entiers dans les corps quadratiques dont ils font partie; par suite ils sont aussi entiers dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Il en résulte que le nombre

$$\text{II. 9. } \omega - h_7\omega_7 - h'_6\omega_6 - h'_5\omega_5 - h'_4\omega_4 - H'_3\omega_3 - H'_2\omega_2 - H'_1\omega_1 = \frac{H'_0 - H'_1 - H'_2 - H'_3}{2}$$

\* Voir Amberg, op. cit., § 2.

est aussi entier dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ ; mais le second membre de l'égalité II. 9 est un nombre rationnel, c'est donc un entier ordinaire.

Si on pose

$$2H_0 \equiv H'_0 - H'_1 - H'_2 - H'_3 \quad \text{et} \quad \omega_0 \equiv 1,$$

l'égalité II. 9 devient

$$\omega - h_7\omega_7 - h'_6\omega_6 - h'_5\omega_5 - h'_4\omega_4 - H'_3\omega_3 - H'_2\omega_2 - H'_1\omega_1 - H_0\omega_0 = 0$$

ou, si on modifie les notations,

$$\omega = h_0\omega_0 + h_1\omega_1 + h_2\omega_2 + h_3\omega_3 + h_4\omega_4 + h_5\omega_5 + h_6\omega_6$$

II. 10.

$$+ h_7\omega_7 = \sum_{\lambda=0}^7 h_\lambda\omega_\lambda,$$

expression dans laquelle les  $h_\lambda$  sont des entiers ordinaires.

L'égalité II. 10 montre que  $\omega_0, \omega_1, \dots, \omega_7$  forment une *base* des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Nous résumons ci-dessous les valeurs des nombres  $\omega_\lambda$ :

$$\begin{aligned} \omega_0 &= 1; & \omega_1 &= \frac{1+\sqrt{apqs}}{2}; & \omega_2 &= \frac{1+\sqrt{bqrs}}{2}; & \omega_3 &= \frac{1+\sqrt{crps}}{2}; \\ \omega_4 &= \frac{1+\sqrt{apqs}+\sqrt{bqrs}+\sqrt{abrp}}{4}; & \omega_5 &= \frac{1+\sqrt{bqrs}+\sqrt{crps}+\sqrt{bcpq}}{4}; \\ \omega_6 &= \frac{1+\sqrt{crps}+\sqrt{apqs}+\sqrt{caqr}}{4}; \\ \omega_7 &= \frac{1+\sqrt{apqs}+\sqrt{bqrs}+\sqrt{crps}+\sqrt{abrp}+\sqrt{bcpq}+\sqrt{caqr}+\sqrt{abcs}}{8}. \end{aligned}$$

5. *Cas b* (v. § 3). Deux des trois nombres  $A, B, C$ , par exemple  $A$  et  $B$ , sont congrus à 1 modulo 4. Il faut distinguer deux sous-cas, suivant que  $C$  est congru à 2 ou à 3 modulo 4.

*1<sup>er</sup> sous-cas.*  $C$  est congru à 2 modulo 4.

Si on met  $A, B$  et  $C$  sous la forme

$$A = apqs, \quad B = bqrs, \quad C = crps, \quad \text{on a} \\ apqs \equiv bqrs \equiv 1 \pmod{4} \quad \text{et} \quad crps \equiv 2 \pmod{4}.$$

On obtient, tous calculs faits,

$$\text{II. 12.} \quad \left\{ \begin{array}{l} apqs \equiv bqrs \equiv abrp \equiv 1 \pmod{4}, \\ crps \equiv bcpq \equiv caqr \equiv abcs \equiv 2 \pmod{4}. \end{array} \right.$$

*2<sup>e</sup> sous-cas.*  $C$  est congru à 3 modulo 4.

On obtient, dans ce cas,

$$\text{II. 13.} \quad \left\{ \begin{array}{l} apqs \equiv bqrs \equiv abrp \equiv 1 \pmod{4}, \\ crps \equiv bcpq \equiv caqr \equiv abcs \equiv 3 \pmod{4}. \end{array} \right.$$

En utilisant la méthode employée dans le § précédent, on trouve pour base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , dans le cas des formules II. 12 et II. 13, les nombres suivants :

$$\begin{aligned} \omega_0 &= 1; & \omega_1 &= \frac{1 + \sqrt{apqs}}{2}; & \omega_2 &= \frac{1 + \sqrt{bqrs}}{2}; & \omega_3 &= \sqrt{crps}; \\ \omega_4 &= \frac{1 + \sqrt{apqs} + \sqrt{bqrs} + \sqrt{abrp}}{4}; & \omega_5 &= \frac{1 + \sqrt{bqrs} + \sqrt{crps} + \sqrt{bcpr}}{2}; \\ \text{II. 14.} & & \omega_6 &= \frac{1 + \sqrt{crps} + \sqrt{apqs} + \sqrt{caqr}}{2}; \\ \omega_7 &= \frac{1 + \sqrt{apqs} + \sqrt{bqrs} + \sqrt{crps} + \sqrt{abrp} + \sqrt{bcpr} + \sqrt{caqr} + \sqrt{abcs}}{4}. \end{aligned}$$

6. Cas  $c$  (v. § 3). Un seul des trois nombres  $A, B, C$  est congru à 1 modulo 4.

Supposons que l'on ait  $A \equiv 1 \pmod{4}$ .

Il faut alors distinguer les sous-cas suivants :

$$\begin{aligned} 1^\circ & B \equiv C \equiv 2 \pmod{4}, \\ 2^\circ & B \equiv 2; C \equiv 3 \pmod{4}, \\ 3^\circ & B \equiv C \equiv 3 \pmod{4}. \end{aligned}$$

1<sup>er</sup> sous-cas :  $A \equiv 1; B \equiv C \equiv 2 \pmod{4}$ .

On peut donc écrire

$$apqs \equiv 1 \pmod{4}; \quad bqrs \equiv crps \equiv 2 \pmod{4}.$$

Si on forme les produits  $AB, BC, CA$  et  $ABC$ , on constate qu'il y a deux possibilités, savoir :

1<sup>re</sup> possibilité :

$$\text{II. 15.} \quad \begin{cases} apqs \equiv bcpq \equiv abcs \equiv 1 \pmod{4}, \\ bqrs \equiv crps \equiv abrp \equiv caqr \equiv 2 \pmod{4}. \end{cases}$$

2<sup>e</sup> possibilité :

$$\text{II. 16.} \quad \begin{cases} apqs \equiv 1 \pmod{4}, \\ bcpq \equiv abcs \equiv 3 \pmod{4}, \\ bqrs \equiv crps \equiv abrp \equiv caqr \equiv 2 \pmod{4}. \end{cases}$$

2<sup>e</sup> sous-cas :  $A \equiv 1; B \equiv 2; C \equiv 3 \pmod{4}$ .

On obtient dans ce cas

$$\text{II. 17.} \quad \begin{cases} apqs \equiv 1 \pmod{4}, \\ bqrs \equiv abrp \equiv bcpq \equiv abcs \equiv 2 \pmod{4}, \\ crps \equiv caqr \equiv 3 \pmod{4}. \end{cases}$$

3<sup>e</sup> sous-cas :  $A \equiv 1; B \equiv C \equiv 3 \pmod{4}$ .

On obtient dans ce cas

$$\text{II. 18. } \left\{ \begin{array}{l} apqs \equiv bcpq \equiv abcs \equiv 1 \pmod{4}, \\ bqrs \equiv crps \equiv abrp \equiv caqr \equiv 3 \pmod{4}. \end{array} \right.$$

Les formules II. 15 et II. 18 ne diffèrent pas essentiellement des résultats obtenus dans le cas  $b$  (formules II. 12 et II. 13). En effet, dans les quatre résultats résumés par les formules II. 12-13-15-18, trois produits, déterminant un sous-corps du 4<sup>e</sup> degré, sont congrus à 1 modulo 4. Si on répète les calculs qui ont permis d'obtenir une base des entiers du corps  $K$  dans le cas  $b$ , on obtient, dans le cas des formules II. 15 et II. 18, des résultats analogues à ceux des formules II. 14.

Par contre, dans le cas des formules II. 16 et II. 17, un seul des nombres de la suite  $apqs, bqrs, \dots, abcs$  est congru à 1 modulo 4. Nous allons rechercher une base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  dans ce dernier cas.

7. Base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  quand un seul nombre de la suite  $apqs, bqrs, \dots, abcs$  est congru à 1 modulo 4.

Prenons comme point de départ les formules II. 17\*.

Désignons de nouveau par  $\omega$  un nombre supposé entier dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , et mettons  $\omega$  sous la forme suivante (v. ch. II. 1) :

$$\text{II. 19. } \omega = \frac{h_0 + h_1\sqrt{apqs} + h_2\sqrt{bqrs} + h_3\sqrt{crps} + \dots + h_7\sqrt{abcs}}{4}.$$

Le nombre

$$\omega_7 \equiv \frac{\sqrt{bqrs} + \sqrt{abrp} + \sqrt{bcpq} + \sqrt{abcs}}{4}$$

est un nombre entier dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . On le voit immédiatement en mettant  $\omega_7$  sous la forme suivante :

$$\omega_7 = \frac{1 + \sqrt{apqs}}{2} \cdot \frac{\sqrt{bqrs} + \sqrt{bcpq}}{2} - \frac{qs-1}{4} \sqrt{abrp} - \frac{pq-1}{4} \sqrt{abcs}.$$

En conduisant alors le calcul comme au § 4 de ce chapitre, on voit que les nombres suivants forment une base du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

\* Les formules II. 16 donneraient une base analogue.

$$\begin{aligned} \omega_0 &= 1; \\ \omega_1 &= \frac{1 + \sqrt{apqs}}{2}; & \omega_2 &= \sqrt{crps}; & \omega_3 &= \sqrt{bqrs}; \\ \text{II. 20. } \omega_4 &= \frac{\sqrt{abrp} + \sqrt{bqrs}}{2}; & \omega_5 &= \frac{\sqrt{abrp} + \sqrt{bcpq}}{2}; \\ \omega_6 &= \frac{1 + \sqrt{apqs} + \sqrt{crps} + \sqrt{caqr}}{2}; \\ \omega_7 &= \frac{\sqrt{bqrs} + \sqrt{abrp} + \sqrt{bcpq} + \sqrt{abcs}}{4}. \end{aligned}$$

8. *Cas d* (v. § 3). *Aucun des trois nombres A, B, C n'est congru à 1 modulo 4.*

L'examen de ce dernier cas n'apporte aucune possibilité nouvelle.

9. En résumé, si tous les nombres de la suite

$$\text{II. 21.} \quad apqs, bqrs, \dots, abcs$$

sont congrus à 1 modulo 4, la base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est donnée par les formules II. 11.

Si trois nombres de la suite II. 21 sont congrus à 1 modulo 4, la base des entiers est donnée par les formules II. 14.

Enfin, si un seul des nombres de la suite II. 21 est congru à 1 modulo 4, la base des entiers est donnée par les formules II. 20.

10. *Remarque sur les dénominateurs des « entiers ».* On sait que dans le corps quadratique  $K(\sqrt{A})$  les « entiers » ont pour dénominateur 1 ou 2. Ils ont en effet l'une des formes  $h_0 + h_1\sqrt{A}$  ou  $\frac{h_0 + h_1\sqrt{A}}{2}$ , où  $h_0$  et  $h_1$  sont des nombres entiers ordinaires.

M. Amberg a montré que dans le corps du 4<sup>e</sup> degré  $K(\sqrt{A}, \sqrt{B})$  les dénominateurs des « entiers » peuvent être 1, 2 ou 4.

L'étude qui précède prouve que dans le corps du 8<sup>e</sup> degré  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  les dénominateurs des « entiers » peuvent être l'un des nombres 1, 2, 4 ou 8.

Enfin, la formule II. 6 montre que dans le corps  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$ , de degré  $2^n$ , les dénominateurs des « entiers » peuvent prendre l'une des valeurs 1, 2,  $2^2$ ,  $2^3$ , ...,  $2^n$ .

### CHAPITRE III

#### Le discriminant et la forme fondamentale du corps

$$K(\sqrt{A_1}, \dots, \sqrt{A_n}).$$

1. Désignons par  $\omega_0, \omega_1, \dots, \omega_{m-1}$ , où  $m \equiv 2^n$ , une base des entiers du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ . On appelle *discriminant* de ce corps, et l'on représente par  $D$ , l'expression

$$\text{III. 1.} \quad D \equiv \begin{vmatrix} \omega_0 & \omega_1 & \omega_2 & \dots & \omega_{m-1} \\ \omega_0^{(1)} & \omega_1^{(1)} & \omega_2^{(1)} & \dots & \omega_{m-1}^{(1)} \\ \omega_0^{(2)} & \omega_1^{(2)} & \omega_2^{(2)} & \dots & \omega_{m-1}^{(2)} \\ \dots & \dots & \dots & \dots & \dots \\ \omega_0^{(m-1)} & \omega_1^{(m-1)} & \omega_2^{(m-1)} & \dots & \omega_{m-1}^{(m-1)} \end{vmatrix}^2$$

dans laquelle  $\omega_\lambda^{(1)}, \omega_\lambda^{(2)}, \dots, \omega_\lambda^{(m-1)}$  sont les conjugués de  $\omega_\lambda$  ( $\lambda = 0, 1, \dots, m-1$ ). Le discriminant  $D$  est un nombre entier ordinaire\*.

2. Pour calculer le discriminant  $D$  du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , nous utiliserons la propriété connue suivante :

Soient deux systèmes de  $r$  nombres, tous tirés d'un même corps algébrique,

$$\begin{array}{c} \mu_1, \mu_2, \dots, \mu_r \\ \nu_1, \nu_2, \dots, \nu_r \end{array}$$

\* Voir par exemple, D. Hilbert, ch. IV.



Si l'on forme le discriminant  $D_\nu$  relatif aux  $\nu_\lambda$  (v. formules III. 1 et III. 4), on obtient

$$\text{III. 6.} \quad D_\nu = 16^6 (abcpqrs)^4.$$

D'autre part, le déterminant  $\Delta$  des coefficients des  $\nu_\lambda$ , dans les égalités III. 5, a pour valeur

$$\text{III. 7.} \quad \Delta = \frac{1}{16^3} \quad \text{d'où} \quad \Delta^2 = \frac{1}{16^6}.$$

La formule III. 3 donne, si l'on tient compte des formules III. 6 et III. 7,

$$\text{III. 8.} \quad D = D_\mu = (abcpqrs)^4.$$

*2<sup>e</sup> cas.* La base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est donnée par les formules II. 14.

Par un calcul analogue à celui que nous venons de faire, on obtient dans ce cas, pour le discriminant  $D$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ ,

$$\text{III. 9.} \quad D = 16^2 (abcpqrs)^4.$$

*3<sup>e</sup> cas.* La base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est donnée par les formules II. 20.

On obtient dans ce cas, par un calcul analogue, pour le discriminant  $D$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ ,

$$\text{III. 10.} \quad D = 16^3 (abcpqrs)^4.$$

*4. Relation entre le discriminant du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  et les discriminants des sous-corps quadratiques\*.*

On sait\*\* que le discriminant du corps quadratique  $K(\sqrt{m})$  est  $D = m$  quand  $m \equiv 1 \pmod{4}$  et  $D = 4m$  quand  $m \not\equiv 1 \pmod{4}$ . Appliquons cela dans les trois cas du § précédent.

*1<sup>er</sup> cas.* La base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est donnée par les formules II. 11.

On a vu (v. ch. II, 4) que, dans ce cas, les sept nombres de la suite

$$\text{III. 11.} \quad apqs, bqrs, crps, abrp, bcpq, caqr, abcs$$

sont tous congrus à 1 modulo 4. Il résulte de là que les discriminants

\* Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  sera désigné, dans la suite de ce chapitre, par  $K$ .

\*\* Voir Sommer, « Introduction à la théorie des nombres algébriques », p. 24.

des sept sous-corps quadratiques  $K(\sqrt{apqs})$ ,  $K(\sqrt{bqrs})$ , ...,  $K(\sqrt{abcs})$  ont respectivement pour valeur

$$D_1 = apqs, D_2 = bqrs, \dots, D_7 = abcs.$$

Le produit des sept discriminants  $D_1, D_2, \dots, D_7$  est donc

$$D_1 D_2 \cdot \dots \cdot D_7 = (abcqrs)^4.$$

En vertu de la formule III. 8, qui donne le discriminant  $D$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , on peut écrire

$$D = D_1 D_2 \cdot \dots \cdot D_7.$$

2<sup>e</sup> cas. La base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est donnée par les formules II. 14.

On a vu au ch. II. 5 que trois nombres de la suite III. 11 sont congrus à 1 modulo 4. Nous supposons que l'on a

$$apqs \equiv bqrs \equiv abrp \equiv 1 \pmod{4}.$$

Les trois discriminants des corps quadratiques  $K(\sqrt{apqs})$ ,  $K(\sqrt{bqrs})$  et  $K(\sqrt{abrp})$  étant désignés respectivement par  $D_1, D_2$  et  $D_3$ , on peut écrire

$$D_1 = apqs; \quad D_2 = bqrs; \quad D_3 = abrp.$$

Les discriminants des quatre autres sous-corps quadratiques étant désignés par  $D_4, D_5, D_6$  et  $D_7$ , on a

$$D_4 = 4crps; \quad D_5 = 4bcpq; \quad D_6 = 4caqr; \quad D_7 = 4abcs.$$

On déduit de là

$$D_1 D_2 \cdot \dots \cdot D_7 = 16^3 (abcqrs)^4.$$

On a, par suite, en vertu de la formule III. 9,

$$D = D_1 D_2 \cdot \dots \cdot D_7.$$

3<sup>e</sup> cas. La base des entiers du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est donnée par les formules II. 20.

Un seul des nombres de la suite III. 11 est congru à 1 modulo 4. Nous supposons, pour fixer les idées, que  $apqs \equiv 1 \pmod{4}$ . Si  $D_1$  désigne le discriminant du sous-corps quadratique  $K(\sqrt{apqs})$ , on a  $D_1 = apqs$ .

Les six autres discriminants des sous-corps quadratiques étant désignés par  $D_2, \dots, D_7$ , on peut écrire

$$D_2 = 4bqrs; \quad D_3 = 4crps; \quad D_4 = 4abrp; \quad D_5 = 4bcpq; \\ D_6 = 4caqr; \quad D_7 = 4abcs.$$

On a, par suite,

$$D_1 D_2 \cdot \dots \cdot D_7 = 16^3 (abcprqs)^4$$

et, en vertu de la formule III. 10,

$$D = D_1 D_2 \cdot \dots \cdot D_7.$$

On peut donc énoncer le

THÉORÈME. *Le discriminant  $D$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est égal au produit des discriminants des sept sous-corps quadratiques.*

LA FORME FONDAMENTALE DU CORPS  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$ .

5. Désignons par  $\omega_0, \omega_1, \dots, \omega_{m-1}$ , où  $m \equiv 2^n$ , une base des entiers du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  de degré  $2^n$ .

Soient, d'autre part,  $m$  quantités  $u_0, u_1, \dots, u_{m-1}$  que nous laissons indéterminées.

Posons

$$\text{III. 12.} \quad \xi \equiv \omega_0 u_0 + \omega_1 u_1 + \omega_2 u_2 + \dots + \omega_{m-1} u_{m-1}.$$

La forme  $\xi$  est dite la *forme fondamentale* du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ . Soient  $\xi^{(1)}, \xi^{(2)}, \dots, \xi^{(m-1)}$  les conjugués de  $\xi$  (v. ch. I. 5); la forme fondamentale satisfait à l'équation suivante, de degré  $m$  en  $x$ :

$$\text{III. 13.} \quad (x - \xi)(x - \xi^{(1)}) \cdot \dots \cdot (x - \xi^{(m-1)}) = 0.$$

Cette équation est dite *l'équation fondamentale* du corps

$$K(\sqrt{A_1}, \dots, \sqrt{A_n}).$$

La norme d'un nombre du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  (v. ch. I. 5 et 11) étant le produit de ce nombre par ses  $m-1$  conjugués, on peut écrire l'équation fondamentale III. 13 comme suit :

$$\text{III. 14.} \quad N(x - \xi) = 0,$$

où  $N$  désigne la norme et où  $x$  est dit la *variable de l'équation*. Le nombre 1 faisant partie du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , on peut écrire

$$1 = a_0 \omega_0 + a_1 \omega_1 + \dots + a_{m-1} \omega_{m-1},$$

d'où

$$\begin{aligned} (x - \xi) &= (a_0 x - u_0) \omega_0 + (a_1 x - u_1) \omega_1 + \dots + (a_{m-1} x - u_{m-1}) \omega_{m-1} \\ &= \sum_{\lambda=0}^{m-1} (a_\lambda x - u_\lambda) \omega_\lambda. \end{aligned}$$

Posons encore

$$a_\lambda x - u_\lambda \equiv v_\lambda \quad \text{pour } \lambda = 0, 1, 2, \dots, m-1.$$

L'équation fondamentale III. 14 s'écrit alors

$$N(\nu_0\omega_0 + \nu_1\omega_1 + \dots + \omega_{m-1}\omega_{m-1}) = 0$$

ou

$$\text{III. 15. } N(V_0 + V_1\sqrt{A_1} + V_2\sqrt{A_2} + \dots \\ \dots + V_{m-1}\sqrt{A_1 A_2 \dots A_n}) = 0,$$

expression dans laquelle les  $V_\lambda$  sont des fonctions linéaires des  $\nu_\lambda$ .

6. *Application au corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .* L'équation fondamentale III. 15 prend la forme

$$N(V_0 + V_1\sqrt{A} + V_2\sqrt{B} + V_3\sqrt{C} + V_4\sqrt{AB} + V_5\sqrt{BC} \\ + V_6\sqrt{CA} + V_7\sqrt{ABC}) = 0,$$

ou

$$\text{III. 16. } N(V_0 + V_1\sqrt{apqs} + V_2\sqrt{bqrs} + V_3\sqrt{crps} + V_4\sqrt{abrp} \\ + V_5\sqrt{bcpq} + V_6\sqrt{caqr} + V_7\sqrt{abcs}) = 0.$$

---

## CHAPITRE IV

### Décomposition des nombres rationnels en facteurs idéaux.

1. Envisageons un nombre premier rationnel  $\pi$ .

Pour décomposer l'idéal principal rationnel  $(\pi)$  en facteurs idéaux du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})^*$ , nous ferons usage des deux théorèmes connus suivants \*\* :

I. Soit  $\mathfrak{p}$  un idéal premier diviseur de  $(\pi)$  et de degré  $f$ ; on peut toujours construire une fonction  $\Pi(x; u_1, u_2, \dots, u_n)$  de degré  $f$  en  $x$ , irréductible suivant  $\pi$  et qui, lorsqu'on y remplace  $x$  par la forme fondamentale  $\xi$  (v. ch. III), a les propriétés suivantes: les coefficients des puissances et des produits des  $u_1, u_2, \dots, u_n$  dans cette fonction sont tous divisibles par  $\mathfrak{p}$  et ne le sont pas par  $\mathfrak{p}^2$ ; en outre ils ne sont pas tous divisibles par un idéal premier différent de  $\mathfrak{p}$  et diviseur de  $(\pi)$ .

II. Si  $(\pi)$ , décomposé en facteurs premiers idéaux, donne

$$(\pi) = \mathfrak{p}^e \mathfrak{p}'^{e'} \dots$$

on a, pour le premier membre de l'équation fondamentale,

$$N \equiv \Pi^e \Pi'^{e'} \dots \pmod{\pi}$$

où  $\Pi, \Pi', \dots$  représentent certaines fonctions, irréductibles suivant  $\pi$ , de  $x; u_1, u_2, \dots, u_n$ ; de plus on peut poser

$$N = \Pi^e \Pi'^{e'} \dots + \pi G$$

où  $G$  est une fonction entière à coefficients entiers, fonction contenant les variables  $x; u_1, u_2, \dots, u_n$ , et qui n'est divisible, suivant  $\pi$  par aucune des fonctions irréductibles  $\Pi, \Pi', \dots$

2. Application au corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Nous distinguerons les deux cas suivants :

1<sup>er</sup> cas.  $\pi$  est un nombre premier impair.

2<sup>e</sup> cas.  $\pi$  est égal à 2.

\* Dans tout ce chapitre,  $K$  désignera toujours le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$

\*\* Voir D. Hilbert, op. cit., ch. IV.

CAS OÙ  $\pi$  EST UN NOMBRE PREMIER IMPAIR.

3. Il faut distinguer deux sous-cas :

*Sous-cas  $\alpha$ .* Aucun des nombres  $a, b, c, p, q, r, s$  n'est divisible par  $\pi$  (v. ch. I, 1).

*Sous-cas  $\beta$ .* L'un des nombres de la suite  $a, b, c, p, q, r, s$  est divisible par  $\pi^*$ .

4. *Sous-cas  $\alpha$ .* Aucun des nombres  $a, b, c, p, q, r, s$  n'est divisible par  $\pi$ . L'équation fondamentale du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est la suivante (v. formule III. 16)

$$\text{IV. 1.} \quad N(V_0 + V_1\sqrt{apqs} + V_2\sqrt{bqrs} + V_3\sqrt{crps} + V_4\sqrt{abrp} \\ + V_5\sqrt{bcpq} + V_6\sqrt{caqr} + V_7\sqrt{abcs}) = 0$$

dans laquelle les  $V_\lambda$  ont les valeurs indiquées au chap. III, et où  $N$  désigne la norme. Le premier membre de l'égalité IV. 1 est donc le produit de huit facteurs se déduisant de  $V_0 + V_1\sqrt{apqs} + \dots + V_7\sqrt{abcs}$  à l'aide des permutations  $\varphi_0, \varphi_1, \dots, \varphi_7$  (v. ch. I, 4).

Le dénominateur du premier membre de IV. 1 est une puissance de 2. Cela résulte du fait que les entiers  $\omega_0, \omega_1, \dots, \omega_7$ , qui constituent la base des entiers du corps  $K$ , ont pour dénominateurs des puissances de 2 (v. formules II. 11-14-20). Comme, d'autre part,  $\pi$  est supposé impair, on peut, dans la décomposition du premier membre de l'équation fondamentale, faire abstraction de ce dénominateur.

Nous désignerons le premier membre de l'équation fondamentale IV. 1 par  $N$  et nous l'écrirons sous la forme

$$\text{IV. 2.} \quad N = FF_1 \dots F_7$$

expression dans laquelle on a

$$\text{IV. 2 a.} \quad F \equiv V_0 + V_1\sqrt{apqs} + V_2\sqrt{bqrs} + V_3\sqrt{crps} + V_4\sqrt{abrp} \\ + V_5\sqrt{bcpq} + V_6\sqrt{caqr} + V_7\sqrt{abcs}$$

et où  $F_1, \dots, F_7$  se déduisent de  $F$  à l'aide des permutations  $\varphi_1, \dots, \varphi_7$ .

En ce qui concerne les sept nombres de la suite

$$\text{IV. 3.} \quad apqs, bqrs, crps, abrp, bcpq, caqr, abcs,$$

il est facile de se rendre compte que les deux seules possibilités suivantes peuvent se présenter :

1° ou bien les sept nombres de la suite IV. 3 sont résidus quadratiques de  $\pi$  :

\* Les nombres  $a, b, c, p, q, r$  et  $s$  sont premiers entre eux deux à deux (v. ch. I, 1), de sorte qu'un seul d'entre eux peut être divisible par  $\pi$ .

2° ou bien trois nombres de la suite IV. 3 sont résidus quadratiques de  $\pi$ ; en outre, ces trois nombres forment la base de l'un des sous-corps du 4<sup>e</sup> degré (v. ch. I, 6).

Nous allons étudier séparément ces deux possibilités.

5. — 1° *Les sept nombres de la suite IV. 3 sont résidus quadratiques de  $\pi$ .* Il existe alors sept nombres  $\rho_1, \rho_2, \dots, \rho_7$  tels que

$$\begin{aligned} \text{IV. 4.} \quad & apqs \equiv \rho_1^2 \pmod{\pi}; & bqrs & \equiv \rho_2^2 \pmod{\pi}; \\ & crps \equiv \rho_3^2 \pmod{\pi}; & abrp & \equiv \rho_4^2 \pmod{\pi}; \\ & bcpq \equiv \rho_5^2 \pmod{\pi}; & caqr & \equiv \rho_6^2 \pmod{\pi}; \\ & & abcs & \equiv \rho_7^2 \pmod{\pi}. \end{aligned}$$

L'égalité IV. 2a peut alors s'écrire, modulo  $\pi$ ,

$$\text{IV. 5.} \quad F \equiv V_0 + V_1\rho_1 + V_2\rho_2 + V_3\rho_3 + V_4\rho_4 + V_5\rho_5 + V_6\rho_6 + V_7\rho_7 \pmod{\pi}.$$

Par l'emploi des permutations  $\varphi_1, \dots, \varphi_7$ , on obtient les autres facteurs  $F_1, \dots, F_7$  de l'égalité IV. 2. Il résulte alors des théorèmes rappelés en tête de ce chapitre que l'idéal  $(\pi)$  se décompose, dans ce cas, en un produit de huit facteurs idéaux premiers, et l'on a

$$\text{IV. 6.} \quad (\pi) = \mathfrak{p}_1 \dots \mathfrak{p}_7. \quad (\text{idéaux du 1<sup>er</sup> degré}).$$

On peut poser en outre

$$\mathfrak{p} = \text{id} \mid \pi, F \mid$$

où  $F$  a la valeur IV. 5 et l'on a, en outre,

$$\mathfrak{p}_\lambda = \text{id} \mid \pi, F_\lambda \mid \quad \text{pour } \lambda = 1, 2, \dots, 7.$$

Si on désigne par  $D_1, D_2, \dots, D_7$  les discriminants des sept sous-corps quadratiques de  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , il résulte des hypothèses faites sur les nombres  $apqs, \dots, abcs$  que les sept discriminants  $D_\lambda$  sont résidus quadratiques de  $\pi$ . Désignons par  $\left(\frac{x}{\pi}\right)$  le symbole de Legendre, où  $x$  désigne un entier ordinaire. Ce symbole est, par définition, égal à  $+1$  quand  $x$  est résidu quadratique de  $\pi$ , égal à  $-1$  quand  $x$  est non résidu et, enfin, égal à zéro quand  $x$  est divisible par  $\pi$ .

La formule IV. 6 correspond au cas

$$\left(\frac{D_1}{\pi}\right) = \left(\frac{D_2}{\pi}\right) = \dots = \left(\frac{D_7}{\pi}\right) = +1.$$

2° *Trois des nombres de la suite IV. 3 sont résidus quadratiques de  $\pi$ .* Nous savons que les trois nombres de la suite IV. 3 qui sont résidus quadratiques de  $\pi$  déterminent un des sous-corps du 4<sup>e</sup> degré.

Supposons qu'il s'agisse du sous-corps  $K_1(\sqrt{bqrs}, \sqrt{crps}, \sqrt{bcpq})$  (v. ch. I. 6). Il existe donc trois nombres entiers ordinaires  $\rho_1, \rho_2$  et  $\rho_3$  tels que les congruences suivantes sont satisfaites :

$$\text{IV. 7.} \quad bqrs \equiv \rho_1^2 \pmod{\pi}; \quad crps \equiv \rho_2^2 \pmod{\pi}; \quad bc pq \equiv \rho_3^2 \pmod{\pi}.$$

Reprenons le premier membre de l'équation fondamentale sous la forme IV. 2.

$$\text{IV. 8.} \quad N = F F_1 F_2 \dots F_7.$$

$F_1$  se déduisant de  $F$  à l'aide de la permutation  $\varphi_1$ , le produit  $FF_1$  fait partie du sous-corps  $K_1$  (v. ch. I. 6), on peut donc écrire

$$\text{IV. 9.} \quad FF_1 = A_0 + A_1 \sqrt{bqrs} + A_2 \sqrt{crps} + A_3 \sqrt{bc pq}$$

expression dans laquelle les  $A_\lambda$  sont des fonctions des quantités  $V_s$  qui figurent dans l'expression IV. 5.

Posons

$$FF_1 \equiv F'.$$

Les produits des six facteurs  $F_2, \dots, F_7$  de l'égalité IV. 8, pris deux à deux de façon convenable, donnent les conjugués de  $F'$  dans le sous-corps  $K_1$ . Désignons ces conjugués par  $F'_1, F'_2$  et  $F'_3$ . L'égalité IV. 8 devient

$$\text{IV. 10.} \quad N = F' F'_1 F'_2 F'_3.$$

Dans cette dernière égalité,  $F'$  a la valeur IV. 9 et peut s'écrire modulo  $\pi$  en vertu des congruences IV. 7,

$$F' \equiv A_0 + A_1 \rho_1 + A_2 \rho_2 + A_3 \rho_3 \pmod{\pi}.$$

Il résulte alors de l'égalité IV. 10 et des théorèmes rappelés au début de ce chapitre que l'on a

$$\text{IV. 11} \quad (\pi) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \quad (\text{idéaux du 2}^\circ \text{ degré})$$

$$\text{où} \quad \mathfrak{p} = \text{id} \mid \pi, F' \mid$$

et où  $\mathfrak{p}_1, \mathfrak{p}_2$  et  $\mathfrak{p}_3$  se déduisent de  $\mathfrak{p}$  à l'aide des permutations  $\varphi_\lambda$ .

Si alors  $D_1, D_2$  et  $D_3$  désignent respectivement les discriminants des trois sous corps quadratiques  $K(\sqrt{bqrs}), K(\sqrt{crps})$  et  $K(\sqrt{bc pq})$ , et  $D_4, D_5, D_6$  et  $D_7$  les discriminants des quatre autres sous-corps quadratiques, on a

$$\left(\frac{D_1}{\pi}\right) = \left(\frac{D_2}{\pi}\right) = \left(\frac{D_3}{\pi}\right) = +1$$

$$\left(\frac{D_4}{\pi}\right) = \left(\frac{D_5}{\pi}\right) = \left(\frac{D_6}{\pi}\right) = \left(\frac{D_7}{\pi}\right) = -1.$$

6. Sous-cas  $\beta$  (v. § 3). Un et un seul des nombres de la suite  $a, b, c, p, q, r, s$  est divisible par  $\pi$ .

Supposons que l'on ait  $a \equiv 0 \pmod{\pi}$ . On en déduit

$$\begin{aligned} apqs &\equiv abrp \equiv caqr \equiv abcs \equiv 0 \pmod{\pi} \quad \text{mais} \\ bqrs &\not\equiv 0, \quad crps \not\equiv 0, \quad bcpq \not\equiv 0 \pmod{\pi}. \end{aligned}$$

Si l'on forme les huit facteurs  $F, F_1, \dots, F_7$  du premier membre de l'équation fondamentale (formule IV. 2), on voit que ces huit facteurs sont égaux deux à deux modulo  $\pi$ , et on peut écrire

$$\text{IV. 12.} \quad N \equiv F^2 F_2^2 F_3^2 F_5^2 \pmod{\pi}.$$

1° Si les trois nombres  $bqrs, crps$  et  $bcpq$  sont tous les trois résidus quadratiques de  $\pi$ , il existe trois nombres  $\rho_1, \rho_2$  et  $\rho_3$  tels que

$$bqrs \equiv \rho_1^2 \pmod{\pi}; \quad crps \equiv \rho_2^2 \pmod{\pi}; \quad bcpq \equiv \rho_3^2 \pmod{\pi}.$$

Le facteur  $F$  s'écrit alors, mod  $\pi$  (v. formule IV, 2a),

$$\text{IV. 13.} \quad F \equiv V_0 + V_2 \rho_1 + V_3 \rho_2 + V_5 \rho_3 \pmod{\pi}$$

et les facteurs  $F_2, F_3$  et  $F_5$  se déduisent de  $F$  à l'aide des permutations  $\varphi_\lambda$ .

En vertu des théorèmes rappelés au début de ce chapitre et de l'égalité IV. 12, l'idéal  $(\pi)$  se décompose comme suit :

$$\text{IV. 14.} \quad (\pi) = \mathfrak{p}^2 \mathfrak{p}_1^2 \mathfrak{p}_2^2 \mathfrak{p}_3^2 \quad (\text{idéaux du 1}^\text{er} \text{ degré})$$

où  $\mathfrak{p} = \text{id} \mid \pi, F \mid$ ,  $F$  ayant la valeur IV. 13.

Si  $D_1, D_2$  et  $D_3$  désignent les discriminants des trois sous-corps quadratiques  $K(\sqrt{bqrs}), K(\sqrt{crps})$  et  $K(\sqrt{bcpq})$  on a, dans ce cas,

$$\begin{aligned} \left(\frac{D_1}{\pi}\right) &= \left(\frac{D_2}{\pi}\right) = \left(\frac{D_3}{\pi}\right) = +1 \\ \left(\frac{D_4}{\pi}\right) &= \left(\frac{D_5}{\pi}\right) = \left(\frac{D_6}{\pi}\right) = \left(\frac{D_7}{\pi}\right) = 0. \end{aligned}$$

2° Si, au contraire, un seul des trois nombres  $bqrs, crps$  et  $bcpq$ , par exemple  $crps$ , est résidu quadratique de  $\pi$ , le premier membre de l'équation fondamentale IV. 2 peut s'écrire

$$\text{IV. 15.} \quad N \equiv (A_0 + A_1 \rho)^2 (A_0 - A_1 \rho)^2 \pmod{\pi}$$

où l'on a posé

$$\begin{aligned} A_0 &\equiv V_0^2 - V_2^2 bqrs + V_3^2 crps - V_5^2 bcpq \\ A_1 &\equiv 2(V_0 V_3 - V_2 V_5 bq) \end{aligned}$$

et où  $\rho$  satisfait à la congruence  $crps \equiv \rho^2 \pmod{\pi}$ .

La formule IV. 15 montre que l'idéal  $(\pi)$  se décompose comme suit :

$$\text{IV. 16.} \quad (\pi) = [\text{id} \mid \pi, A_0 + A_1 \rho]^2 [\text{id} \mid \pi, A_0 - A_1 \rho]^2 \quad (\text{idéaux du 2}^\text{e} \text{ degré}).$$

En outre, dans ce cas, quatre symboles  $\left(\frac{D_i}{\pi}\right)$  sont nuls, deux sont égaux à  $-1$  et un seul symbole est égal à  $+1$ .

7. DÉCOMPOSITION D'UN NOMBRE PREMIER IMPAIR  $\pi$  DANS LE CORPS

$$K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n}).$$

Les nombres  $A_1, A_2, \dots, A_n, A_1A_2, \dots, A_1A_2A_3, \dots, A_1A_2\dots A_n$  peuvent se mettre sous la forme

IV. 17.

$$a_\lambda d_1^{(2)} d_2^{(2)} \dots d_1^{(3)} d_2^{(3)} \dots d_1^{(4)} d_2^{(4)} \dots d_1^{(n-2)} d_2^{(n-2)} \dots d_2^{(n-1)} d_2^{(n-1)} \dots s,$$

expression dans laquelle les nombres  $a_\lambda, d_k^{(l)}$  et  $s$  sont premiers entre eux deux à deux. Il y a donc deux cas possibles, suivant qu'aucun des nombres  $a_\lambda, d_k^{(l)}, s$  n'est divisible par  $\pi$  ou que, au contraire, un et un seul de ces nombres est divisible par  $\pi$ .

8. 1<sup>er</sup> cas. Aucun des nombres  $a_\lambda, d_k^{(l)}, s$  n'est divisible par  $\pi$ .

THÉORÈME. — Etant donné le corps  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$  tel que les  $2^n - 1$  nombres

IV. 18.  $A_1, A_2, \dots, A_n, \overline{A_1A_2}, \dots, \overline{A_1A_2A_3}, \dots, \overline{A_1A_2\dots A_n}$

ont la forme IV. 17, les deux possibilités suivantes peuvent seules se présenter :

1<sup>re</sup> possibilité. Les  $2^n - 1$  nombres de la suite IV. 18 sont résidus quadratiques de  $\pi$ .

2<sup>e</sup> possibilité.  $2^{n-1} - 1$  nombres de la suite IV. 18 sont résidus quadratiques de  $\pi$  et  $2^{n-1}$  nombres de la même suite sont non résidus.

Esquisse de la démonstration. Il est tout d'abord évident qu'au lieu de raisonner sur le nombre  $\overline{A_1A_2\dots A_s}$  ( $1 \leq s \leq n$ ), on peut raisonner sur le nombre  $A_1A_2\dots A_s$ , puisque ces deux nombres sont les mêmes à un facteur carré près.

1<sup>o</sup> Si les  $n$  nombres  $A_1, \dots, A_n$  sont tous résidus quadratiques de  $\pi$ , les  $2^n - 1$  nombres de la suite IV. 18 sont évidemment tous résidus quadratiques de  $\pi$ .

2<sup>o</sup> Si un et un seul des nombres  $A_1, \dots, A_n$ , par exemple  $A_1$ , est non-résidu quadratique de  $\pi$ , on peut dénombrer comme suit le nombre des non-résidus de la suite IV. 18 :

Parmi les nombres  $A_r$ , il y a 1 non-résidu,  
 » » »  $A_r A_s$ , il y a  $n - 1 = \binom{n-1}{1}$  non-résidus,  
 » » »  $A_r A_s A_t$ , il y a  $\binom{n-1}{2}$  non-résidus,  
 et ainsi de suite.

Le total des non-résidus de la suite IV. 18 est alors

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \dots + 1 = 2^{n-1}.$$

3° Si deux des nombres  $A_1, A_2, \dots, A_n$  sont non-résidus quadratiques de  $\pi$ , il y a :

parmi les nombres  $A_r$ , 2 non-résidus,  
 » » »  $A_r A_s$ ,  $2(n-2)$  » »  
 » » »  $A_r A_s A_t$ ,  $(n-2)(n-3)$  » »  
 etc...

On trouve, pour le nombre total des non-résidus de la suite IV. 18,

$$2 + 2(n-2) + (n-2)(n-3) + \frac{(n-2)(n-3)(n-4)}{3} \\
 + \frac{(n-2)(n-3)(n-4)(n-5)}{3.4} + \dots + \frac{(n-2)(n-3)\dots(n-k)}{3.4\dots(k-1)} \\
 + \dots + \frac{(n-2)(n-3)\dots 3.2.1}{3.4\dots(n-2)} = 2^{n-1}.$$

La démonstration se fait de la même manière lorsque 3, 4, ..., n nombres de la suite  $A_1, A_2, \dots, A_n$  sont non résidus quadratiques de  $\pi$ . Il y a donc  $2^{n-1} - 1$  résidus.

Dans la première possibilité, c'est-à-dire quand les  $2^n - 1$  nombres de la suite IV. 18 sont résidus quadratiques de  $\pi$ , l'idéal  $(\pi)$  admet, dans le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , la décomposition suivante :

$$(\pi) = \mathfrak{p} \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_{m-1} \quad \text{où} \quad m \equiv 2^n,$$

les idéaux  $\mathfrak{p}_\lambda$  étant des idéaux du 1<sup>er</sup> degré.

Si on désigne par  $D_\lambda (\lambda = 1, 2, \dots, m-1)$  les discriminants des  $2^n - 1 = m - 1$  sous-corps quadratiques, on a, dans ce cas,

$$\left(\frac{D_1}{\pi}\right) = \left(\frac{D_2}{\pi}\right) = \left(\frac{D_3}{\pi}\right) = \dots = \left(\frac{D_{m-1}}{\pi}\right) = +1.$$

Dans la deuxième possibilité, soit lorsque  $2^{n-1} - 1$  nombres de la

suite IV.18 sont résidus quadratiques de  $\pi$ , l'idéal  $(\pi)$  se décompose comme suit :

$$(\pi) = \mathfrak{p} \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_{\frac{m}{2}-1} \quad \text{où } m \equiv 2^n$$

les idéaux  $\mathfrak{p}_\lambda$  étant, cette fois, du second degré.

En outre,  $2^{n-1} - 1$  symboles  $\left(\frac{D_\lambda}{\pi}\right)$  sont égaux à  $+1$  et  $2^{n-1}$  symboles sont égaux à  $-1$ .

9. 2<sup>e</sup> CAS. Un et un seul des nombres  $a_\lambda, d_k^{(l)}, s$  est divisible par  $\pi$ .

Dans ce cas,  $2^{n-1}$  symboles  $\left(\frac{D_\lambda}{\pi}\right)$  sont nuls.

1<sup>o</sup> Si alors les  $2^{n-1} - 1$  symboles  $\left(\frac{D_\lambda}{\pi}\right)$  qui sont  $\neq 0$  sont égaux à  $+1$ , l'idéal  $(\pi)$  se décompose comme suit :

$$(\pi) = \mathfrak{p}^2 \mathfrak{p}_1^2 \dots \mathfrak{p}_{\frac{m}{2}-1}^2$$

où  $m \equiv 2^n$  et où les  $\mathfrak{p}_\lambda$  sont des idéaux du premier degré.

2<sup>o</sup> Si,  $2^{n-1}$  symboles  $\left(\frac{D_\lambda}{\pi}\right)$  étant nuls,  $2^{n-2} - 1$  symboles sont égaux à  $+1$  et  $2^{n-2}$  symboles sont égaux à  $-1$ , la décomposition de l'idéal  $(\pi)$  est la suivante :

$$(\pi) = \mathfrak{p}^2 \mathfrak{p}_1^2 \dots \mathfrak{p}_{\frac{m}{4}-1}^2$$

où  $\mathfrak{p}, \mathfrak{p}_1, \dots$  sont des idéaux du second degré.

Il n'y a pas d'autre possibilité.

#### 10. CAS DE $\pi = 2$ .

Nous nous bornerons au cas du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  que nous désignerons par  $K$ . Il y a lieu de distinguer trois cas suivant la forme de la base des entiers du corps  $K$ . (Voir ch. II, formules II. 11, II. 14 et II. 20).

1<sup>er</sup> CAS. La base des entiers est donnée par les formules II. 11.

Dans ce cas, les sept nombres de la suite

$$\text{IV. 19.} \quad apqs, bqrs, crps, abrp, bcpq, caqr, abcs$$

sont congrus à 1 modulo 4.

Le dénominateur commun des nombres  $\omega_0, \omega_1, \dots, \omega_7$  qui forment la base des entiers du corps  $K$  (formules II.11) est  $2^3 = 8$ . Le dénominateur du premier membre  $N$  de l'équation fondamentale (v. ch. III. 5 et 6) est  $2^{24}$ . Si nous multiplions par  $2^{24}$  les deux membres de l'équation

fondamentale  $N = 0$  (v. formules IV.2 et IV.2a), nous devons opérer la décomposition de  $N$  modulo  $2^{25}$ .

Il n'y a alors que deux cas possibles :

1° Les sept produits IV.19 sont résidus quadratiques de  $2^{25}$ .

2° Trois seulement des produits IV.19 sont résidus quadratiques de  $2^{25}$ .

1° Dans ce cas, il existe sept nombres  $\rho_1, \dots, \rho_7$  tels que les congruences suivantes sont satisfaites :

$$\text{IV. 20. } apqs \equiv \rho_1^2 \pmod{2^{25}}; \quad bqrs \equiv \rho_2^2 \pmod{2^{25}}; \quad \dots; \\ abc s \equiv \rho_7^2 \pmod{2^{25}}.$$

Le premier membre de l'équation fondamentale (formule IV.2) peut s'écrire, modulo 2,

$$N \equiv F' F'_1 F'_2 \dots F'_7,$$

l'accent rappelant que l'on a multiplié par  $2^{24}$ . On a (v. formule IV.2a)

$$F' = V'_0 + V'_1 \sqrt{apqs} + V'_2 \sqrt{bqrs} + \dots + V'_7 \sqrt{abc s},$$

$F'_1, \dots, F'_7$  se déduisant de  $F'$  à l'aide des permutations  $\varphi_1, \dots, \varphi_7$ .

L'idéal (2) se décompose comme suit, dans ce cas :

$$(2) = \mathfrak{p} \mathfrak{p}_1 \dots \mathfrak{p}_7 \quad (\text{idéaux du 1}^\text{er} \text{ degré})$$

où l'on a  $\mathfrak{p} = \text{id} \mid 2, F'$ .

Désignons par  $\left(\frac{D_\lambda}{2}\right)$  le symbole de Legendre généralisé, symbole défini comme suit :

$$\left(\frac{D_\lambda}{2}\right) = +1 \quad \text{quand } D_\lambda \equiv 1 \pmod{8} \\ \left(\frac{D_\lambda}{2}\right) = -1 \quad \text{quand } D_\lambda \equiv -1 \text{ ou } \pm 3 \pmod{8} \\ \left(\frac{D_\lambda}{2}\right) = 0 \quad \text{quand } D_\lambda \equiv 0 \text{ ou } \equiv \pm 2 \text{ ou } \equiv 4 \pmod{8}.$$

On voit qu'on a, dans le cas ci-dessus,

$$\left(\frac{D_1}{2}\right) = \left(\frac{D_2}{2}\right) = \left(\frac{D_3}{2}\right) = \left(\frac{D_4}{2}\right) = \dots = \left(\frac{D_7}{2}\right) = +1.$$

2° Trois symboles sont égaux à  $+1$  et les quatre autres sont égaux à  $-1$ . En effet, les sept produits de la suite IV.19 étant congrus à 1 modulo 4, ces sept produits sont des nombres impairs.

La décomposition de l'idéal (2) est alors la suivante :

$$(2) = \mathfrak{p} \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3,$$

expression dans laquelle  $\mathfrak{p}, \dots, \mathfrak{p}_3$  sont des idéaux du second degré.

2<sup>e</sup> CAS : La base est donnée par les formules II.14 ou II.20. Dans ces deux cas, quatre nombres de la suite IV.19 sont incongrus à 1 modulo 4.

Il en résulte que quatre au moins des symboles  $\left(\frac{D_\lambda}{2}\right)$  sont nuls. Les différentes possibilités suivantes peuvent alors se présenter :

- a) Quatre symboles  $\left(\frac{D_\lambda}{2}\right)$  sont nuls, trois symboles  $\left(\frac{D_\lambda}{2}\right)$  sont égaux à +1.
- b) Quatre symboles  $\left(\frac{D_\lambda}{2}\right)$  sont nuls, un symbole est égal à +1 et deux symboles sont égaux à -1.
- c) Six symboles sont nuls, un symbole est égal à +1.
- d) Six symboles sont nuls, un symbole est égal à -1.

Après discussion de ces possibilités, on peut établir le tableau suivant qui résume toute la discussion précédente :

11. Soit  $\pi$  un nombre premier quelconque et soient d'autre part  $D_1, D_2, \dots, D_7$  les discriminants des sept sous-corps quadratiques du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . L'idéal  $(\pi)$ , dans ce corps  $K$ , se décompose conformément au tableau ci-après :

- |         |  |  |
|---------|--|--|
| 1.      | Les sept symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à +1.  | $(\pi) = p p_1 \dots p_7$ (idéaux du 1 <sup>er</sup> degré).       |
| 2.      | $\left\{ \begin{array}{l} \text{Trois symboles } \left(\frac{D_\lambda}{\pi}\right) \text{ sont égaux à } +1 \\ \text{Quatre } \text{ » } \text{ » } \text{ » } \text{ » } -1 \end{array} \right\}$  | $(\pi) = p p_1 p_2 p_3$ (idéaux du 2 <sup>e</sup> degré).          |
| 3.      | $\left\{ \begin{array}{l} \text{Quatre symboles } \left(\frac{D_\lambda}{\pi}\right) \text{ sont égaux à } 0 \\ \text{Trois } \text{ » } \text{ » } \text{ » } \text{ » } +1 \end{array} \right\}$   | $(\pi) = p^2 p_1^2 p_2^2 p_3^2$ (idéaux du 1 <sup>er</sup> degré). |
| IV. 21. | $\left\{ \begin{array}{l} \text{Quatre symboles } \left(\frac{D_\lambda}{\pi}\right) \text{ sont égaux à } 0 \\ \text{Deux } \text{ » } \text{ » } \text{ » } \text{ » } -1 \\ \text{Un symbole } \text{ » } \text{ est égal } \text{ » } +1 \end{array} \right\}$ | $(\pi) = p^2 p_1^2$ (idéaux du 2 <sup>e</sup> degré).              |
| 5.      | $\left\{ \begin{array}{l} \text{Six symboles } \left(\frac{D_\lambda}{\pi}\right) \text{ sont égaux à } 0 \\ \text{Un symbole } \text{ » } \text{ est égal } \text{ à } +1 \end{array} \right\}$   | $(\pi) = p^4 p_1^4$ (idéaux du 1 <sup>er</sup> degré).             |
| 6.      | $\left\{ \begin{array}{l} \text{Six symboles } \left(\frac{D_\lambda}{\pi}\right) \text{ sont égaux à } 0 \\ \text{Un symbole } \text{ » } \text{ est égal } \text{ à } -1 \end{array} \right\}$   | $(\pi) = p^4$ (idéal du 2 <sup>e</sup> degré).                     |

Ce tableau épuise toutes les possibilités.

## CHAPITRE V

### Les unités du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})^*$ .

1. DÉFINITION. Une unité du corps  $K$  est un nombre  $\varepsilon$ , entier dans le corps  $K$ , et dont le réciproque  $\frac{1}{\varepsilon}$  est un nombre entier dans le même corps. On démontre que la norme d'une unité est  $+1$  ou  $-1$  et que, réciproquement, si la norme d'un entier du corps  $K$  est  $+1$  ou  $-1$ , cet entier est une unité du corps  $K$ .

Le corps des nombres rationnels ne contient que les deux unités  $+1$  et  $-1$ . Le corps  $K(\sqrt{-1})$  contient les quatre unités  $+1, -1, +i, -i$ , où  $i \equiv \sqrt{-1}$ .

Le corps  $K(\sqrt{-3})$  contient les six unités suivantes :

$$+1, -1, \frac{1 + \sqrt{-3}}{2}, -\frac{1 + \sqrt{-3}}{2}, \frac{1 - \sqrt{-3}}{2}, -\frac{1 - \sqrt{-3}}{2}.$$

Tout corps quadratique imaginaire autre que  $K(\sqrt{-1})$  et  $K(\sqrt{-3})$  n'a que deux unités  $+1$  et  $-1$ .

Dans chaque corps quadratique réel  $K(\sqrt{m})$ , avec  $m > 0$ , il y a une infinité d'unités différentes de  $\pm 1$  et parmi celles-là il y a une unité fondamentale  $\varepsilon$  telle que  $|\varepsilon| > 1$  et que toute autre unité de ce corps puisse être mise sous la forme  $\pm \varepsilon^a$ , où l'exposant  $a$  est un entier rationnel, positif ou négatif \*\*.

Pour un corps algébrique de degré quelconque, le nombre des unités

\* Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  sera désigné, dans ce chapitre, par  $K$ .

\*\* Voir Sommer, op. cit. § 22.

fondamentales est déterminé par le théorème de Dirichlet suivant, théorème dont nous ferons usage dans ce qui suivra \* :

**THÉORÈME DE DIRICHLET.** *Soit  $K$  un corps de degré  $m$ ; si parmi les corps conjugués  $K = K^{(1)}, K^{(2)}, \dots, K^{(m)}$  il y a  $r_1$  corps réels et  $r_2 \equiv \frac{m-r_1}{2}$  couples de corps imaginaires conjugués, le corps  $K$  contient un système de  $r \equiv r_1 + r_2 - 1$  unités  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ , dites unités fondamentales, telles que toute autre unité  $\varepsilon$  du corps  $K$  puisse se mettre sous la forme*

$$\varepsilon = \rho \varepsilon_1^{a_1} \varepsilon_2^{a_2} \dots \varepsilon_r^{a_r}$$

et cela d'une seule manière, les  $a_1, a_2, \dots, a_r$  étant des entiers ordinaires et  $\rho$  une racine de l'unité contenue dans  $K$ .

2. On a, pour le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  de degré  $2^n$ , le théorème suivant :

**THÉORÈME.** — *Le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , de degré  $2^n$ , contient  $2^{n-1} - 1$  unités fondamentales si l'un au moins des radicaux  $\sqrt{A_\lambda}$  est imaginaire, et  $2^n - 1$  unités fondamentales si les  $n$  radicaux  $\sqrt{A_\lambda}$  sont tous réels.*

Ce théorème résulte immédiatement du théorème de Dirichlet.

3. **COROLLAIRE.** *Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  admet, en vertu du théorème précédent, trois unités fondamentales si l'un au moins des trois radicaux  $\sqrt{A}, \sqrt{B}, \sqrt{C}$  est imaginaire, et sept unités fondamentales si les trois radicaux  $\sqrt{A}, \sqrt{B}, \sqrt{C}$  sont réels.*

**CAS OÙ LE CORPS  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  NE CONTIENT QUE TROIS UNITÉS FONDAMENTALES ET LES RACINES DE L'UNITÉ  $+1$  et  $-1$ .** \*\*

4. L'une au moins des quantités  $\sqrt{A}, \sqrt{B}$  et  $\sqrt{C}$  est complexe. Un et un seul sous-corps du 4<sup>e</sup> degré (v. chap. I. 6) est réel. Cela résulte de la façon même dont ces sous-corps sont formés. Nous supposons, pour fixer les idées, que le sous-corps réel est  $K_1$  dont la base est  $[1, \sqrt{bqrs}, \sqrt{crps}, \sqrt{bcpg}]$  (v. ch. I. 6). Les trois sous-corps quadratiques  $K(\sqrt{bqrs})$ ,  $K(\sqrt{crps})$  et  $K(\sqrt{bcpg})$  étant réels, ils admettent chacun une et une seule unité fondamentale (v. § 1 de ce chap.). Désignons par  $\varepsilon_1$  l'unité fondamentale de  $K(\sqrt{bqrs})$ , par  $\varepsilon_2$  celle de  $K(\sqrt{crps})$  et par  $\varepsilon_3$  celle de  $K(\sqrt{bcpg})$ .

\* Voir D. Hilbert, op. cit. p. 44.

\*\* Voir ch. VII le cas où le corps  $K$  contient encore d'autres racines de l'unité.

Le corps  $K_1(\sqrt{bqrs}, \sqrt{crps})$  admet trois unités fondamentales que nous désignerons par  $\gamma_1, \gamma_2$  et  $\gamma_3$ . Enfin  $\zeta_1, \zeta_2$  et  $\zeta_3$  seront trois unités fondamentales du corps envisagé  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

5. PROBLÈME. — *Connaissant les trois unités fondamentales  $\varepsilon_1, \varepsilon_2$  et  $\varepsilon_3$  des sous-corps quadratiques réels  $K(\sqrt{bqrs}), K(\sqrt{crps})$  et  $K(\sqrt{bcprq})$ , ainsi que trois unités fondamentales  $\gamma_1, \gamma_2$  et  $\gamma_3$  du sous-corps réel  $K_1(\sqrt{bqrs}, \sqrt{crps})$  du 4<sup>e</sup> degré, trouver trois unités fondamentales  $\zeta_1, \zeta_2$  et  $\zeta_3$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .*

Pour résoudre ce problème, on peut procéder comme suit : Les trois unités  $\gamma_1, \gamma_2$  et  $\gamma_3$ , qui sont trois unités fondamentales du sous-corps  $K_1(\sqrt{bqrs}, \sqrt{crps})$ , peuvent s'exprimer, en fonction des unités fondamentales de  $K$ , de la façon suivante :

$$\begin{aligned}\gamma_1 &= \pm \zeta_1^{a_1} \zeta_2^{a_2} \zeta_3^{a_3} \\ \gamma_2 &= \pm \zeta_1^{b_1} \zeta_2^{b_2} \zeta_3^{b_3} \\ \gamma_3 &= \pm \zeta_1^{c_1} \zeta_2^{c_2} \zeta_3^{c_3}\end{aligned}$$

formules qui peuvent s'écrire aussi

$$\begin{aligned}\gamma_1 &= \pm \lambda_1^a \\ \text{V. 1.} \quad \gamma_2 &= \pm \lambda_1^b \lambda_2^c \\ \gamma_3 &= \pm \lambda_1^d \lambda_2^e \lambda_3^f.\end{aligned}$$

Ici,  $a$  désigne le plus grand commun diviseur des trois nombres  $a_1, a_2$  et  $a_3$ , plus grand commun diviseur que nous prendrons positivement ;  $\lambda_1, \lambda_2$  et  $\lambda_3$  sont de nouvelles unités fondamentales de  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  et  $b, c, \dots, f$  sont des entiers ordinaires.

On a d'abord le

6. THÉORÈME. — *Dans les formules V. 1, chacun des trois entiers  $a, c$  et  $f$  ne peut prendre que les valeurs 1 et 2.*

Pour démontrer ce théorème, il suffit d'appliquer aux deux membres de chacune des égalités V. 1 l'une des permutations  $\varphi_\lambda$  (v. ch. I. 4) choisie convenablement.

Considérons, par exemple, la première des égalités V. 1, et appliquons-lui la permutation  $\varphi_1$  qui laisse inchangé le sous-corps réel  $K_1$ . Cette égalité devient, puisque  $\gamma_1$  fait partie de  $K_1$ ,

$$\text{V. 2.} \quad \gamma_1 = \pm \lambda_1^{(1)a}$$

où  $\lambda_1^{(1)}$  désigne ce que devient  $\lambda_1$  par l'application de la permutation  $\varphi_1$ .

Multiplions membre à membre la première des égalités V. 1 et l'égalité V. 2, on obtient

V. 3. 
$$\gamma_1^2 = (\lambda_1 \lambda_1^{(1)})^a.$$

Mais  $\lambda_1 \lambda_1^{(1)}$  fait partie du sous-corps  $K_1$  (v. ch. I. 6). L'unité  $\lambda_1 \lambda_1^{(1)}$  peut donc se mettre sous la forme

V. 4. 
$$\lambda_1 \lambda_1^{(1)} = \pm \gamma_1^{m_1} \gamma_2^{m_2} \gamma_3^{m_3}. \quad (m_\lambda \text{ entiers ordinaires})$$

L'égalité V. 3 s'écrit, en vertu de V. 4,

$$\gamma_1^2 = \pm \gamma_1^{am_1} \gamma_2^{am_2} \gamma_3^{am_3}$$

de laquelle on déduit

$$am_1 = 2; \quad am_2 = am_3 = 0.$$

Puisque  $a$  est un entier ordinaire positif, la première des égalités ci-dessus montre que  $a = 1$  ou  $2$ .

7. Il y a lieu, dès lors, de distinguer huit possibilités, résumées par le tableau suivant :

		1 <sup>re</sup>	2 <sup>e</sup>	3 <sup>e</sup>	4 <sup>e</sup>	5 <sup>e</sup>	6 <sup>e</sup>	7 <sup>e</sup>	8 <sup>e</sup>
V. 5.	$a$	=	1	1	1	2	1	2	2
	$c$	=	1	1	2	1	2	1	2
	$f$	=	1	2	1	1	2	2	1

Nous ferons tout d'abord la remarque suivante :

Si  $\lambda_1, \lambda_2$  et  $\lambda_3$  sont trois unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , les unités  $\lambda_1^x \lambda_2, \lambda_1^y \lambda_2^z \lambda_3$ , où  $x, y$  et  $z$  désignent des nombres entiers ordinaires, peuvent être prises pour unités fondamentales à la place de  $\lambda_2$  et de  $\lambda_3$  respectivement. En effet, si

$$H \equiv \pm \lambda_1^{a_1} \lambda_2^{a_2} \lambda_3^{a_3}, \quad \text{où les } a_\lambda \text{ sont des entiers}$$

ordinaires, est une unité quelconque du corps  $K$ , on peut écrire

$$H = \pm \lambda_1^{a_1 - a_3 y - z(a_2 - a_3 z)} \cdot (\lambda_1^x \lambda_2)^{a_2 - a_3 z} \cdot (\lambda_1^y \lambda_2^z \lambda_3)^{a_3},$$

expression dans laquelle les exposants sont des entiers ordinaires.

8. Il est alors possible, en vertu de la remarque précédente, de remplacer, dans chacune des huit possibilités du tableau V. 5, les unités fondamentales  $\lambda_1, \lambda_2$  et  $\lambda_3$  (v. formules V. I) par d'autres unités fondamentales plus faciles à calculer.

Considérons, par exemple, la première possibilité du tableau V. 5, savoir :

$$a = c = f = 1.$$

Les formules V. 1 s'écrivent, dans ce cas,

$$\begin{aligned} \eta_1 &= \pm \lambda_1 \\ \eta_2 &= \pm \lambda_1^b \lambda_2 \\ \eta_3 &= \pm \lambda_1^d \lambda_2^e \lambda_3 \end{aligned}$$

La remarque faite au § précédent permet de prendre pour unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  les unités suivantes :

$$\lambda_1, \lambda_1^b \lambda_2 \text{ et } \lambda_1^d \lambda_2^e \lambda_3$$

c'est-à-dire  $\eta_1, \eta_2$  et  $\eta_3$ .

Prenons encore, à titre d'exemple, la deuxième possibilité du tableau V. 5 soit

$$a = c = 1; \quad f = 2.$$

Les formules V. 1 s'écrivent, dans ce cas,

$$\begin{aligned} \eta_1 &= \pm \lambda_1 \\ \eta_2 &= \pm \lambda_1^b \lambda_2 \\ \eta_3 &= \pm \lambda_1^d \lambda_2^e \lambda_3^2 \end{aligned}$$

En vertu de la remarque faite plus haut, les trois unités fondamentales  $\lambda_1, \lambda_2$  et  $\lambda_3$  peuvent être remplacées respectivement par  $\lambda_1, \lambda_1^b \lambda_2$  et  $\lambda_3$ .

Supposons, par exemple, que l'on ait

$$d \equiv e \equiv 0 \pmod{2}$$

et posons, par suite,

$$d = 2d_1 \text{ et } e = 2e_1.$$

La troisième des égalités V. 6 peut alors s'écrire

$$\eta_3 = \pm (\lambda_1^{d_1} \lambda_2^{e_1} \lambda_3)^2.$$

L'unité  $\lambda_3$  peut être remplacée par  $\lambda_1^{d_1} \lambda_2^{e_1} \lambda_3$ , de sorte qu'on peut prendre pour unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  les trois unités  $\lambda_1, \lambda_1^b \lambda_2$  et  $\lambda_1^{d_1} \lambda_2^{e_1} \lambda_3$ , c'est-à-dire

$$\eta_1, \eta_2 \text{ et } \sqrt{\pm \eta_3}.$$

Si l'on fait toutes les hypothèses possibles au sujet des valeurs que peuvent prendre les exposants  $b, d$  et  $e$  (formules V. 1) suivant le module 2, on obtient, après discussion des huit possibilités du tableau V. 5, le résultat suivant :

$\gamma_1, \gamma_2$  et  $\gamma_3$  désignant trois unités fondamentales du sous-corps réel  $K_1(\sqrt{bqrs}, \sqrt{crps})$ , les unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  qui en résultent peuvent prendre les formes suivantes :

Valeur du produit $acf$ (formules V. 1.)	Forme des unités fondamentales du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .		
$acf = 1$	$\gamma_r,$	$\gamma_s,$	$\gamma_u$
$acf = 2$	$\left\{ \begin{array}{l} \gamma_r, \\ \gamma_r, \\ \gamma_r, \end{array} \right.$	$\left\{ \begin{array}{l} \gamma_s, \\ \gamma_s, \\ \gamma_s, \end{array} \right.$	$\left\{ \begin{array}{l} \sqrt{\pm \gamma_u} \\ \sqrt{\pm \gamma_r \gamma_u} \text{ ou } \sqrt{\pm \gamma_s \gamma_u} \\ \sqrt{\pm \gamma_r \gamma_s \gamma_u} \end{array} \right.$
$acf = 4$	$\left\{ \begin{array}{l} \gamma_r, \\ \gamma_r, \\ \gamma_r, \\ \gamma_r, \\ \gamma_r, \\ \gamma_r, \\ \gamma_r, \end{array} \right.$	$\left\{ \begin{array}{l} \sqrt{\pm \gamma_s}, \\ \sqrt{\pm \gamma_s}, \\ \sqrt{\pm \gamma_s}, \\ \sqrt{\pm \gamma_s}, \\ \sqrt{\pm \gamma_r \gamma_s}, \\ \sqrt{\pm \gamma_r \gamma_s}, \\ \sqrt{\pm \gamma_r \gamma_s}, \end{array} \right.$	$\left\{ \begin{array}{l} \sqrt{\pm \gamma_u} \\ \sqrt{\pm \gamma_r \gamma_u} \\ \sqrt[3]{\pm \gamma_s \gamma_u^2} \\ \sqrt[3]{\pm \gamma_r^2 \gamma_s \gamma_u^2} \\ \sqrt{\pm \gamma_r \gamma_u} \\ \sqrt[3]{\pm \gamma_r \gamma_s^2 \gamma_u^2} \\ \sqrt[3]{\pm \gamma_r \gamma_s \gamma_u^2} \end{array} \right.$
$acf = 8$	$\left\{ \begin{array}{l} \sqrt{\pm \gamma_r}, \\ \sqrt{\pm \gamma_r}, \end{array} \right.$	$\left\{ \begin{array}{l} \sqrt{\pm \gamma_s}, \\ \sqrt{\pm \gamma_s}, \\ \sqrt{\pm \gamma_s}, \\ \sqrt[3]{\pm \gamma_r \gamma_s^2}, \\ \sqrt[3]{\pm \gamma_r \gamma_s^2}, \\ \sqrt[3]{\pm \gamma_r \gamma_s^2}, \\ \sqrt[4]{\pm \gamma_r \gamma_s^2}, \end{array} \right.$	$\left\{ \begin{array}{l} \sqrt{\pm \gamma_u} \\ \sqrt[4]{\pm \gamma_s \gamma_u^2} \\ \sqrt[4]{\pm \gamma_r \gamma_s \gamma_u^2} \\ \sqrt[3]{\pm \gamma_r \gamma_u^2} \\ \sqrt[8]{\pm \gamma_r^3 \gamma_s^2 \gamma_u^3} \\ \sqrt[8]{\pm \gamma_r \gamma_s^2 \gamma_u^4} \end{array} \right.$

9. Certaines formes d'unités fondamentales que nous avons obtenues par le calcul précédent ne peuvent pas se présenter. Je dis que les racines 4<sup>ièmes</sup> et les racines 8<sup>ièmes</sup> du tableau précédent ne peuvent pas être des unités du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

Nous nous bornerons à le démontrer pour  $\sqrt[4]{\gamma_1 \gamma_2 \gamma_3^2}$ .

Posons

V. 8.  $\lambda \equiv \sqrt[4]{\gamma_1 \gamma_2 \gamma_3^2}$

et supposons que  $\lambda$  soit une unité du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Appliquons aux deux membres de l'égalité V. 8 la permutation  $\varphi_1$  qui laisse

inchangé le sous-corps  $K_1$ . Les trois unités  $\gamma_1, \gamma_2$  et  $\gamma_3$  faisant partie du sous-corps  $K_1$ , elles ne changent pas, et l'égalité V. 8 devient

V. 9. 
$$\lambda^{(1)} = \sqrt[4]{\gamma_1 \gamma_2 \gamma_3^2}.$$

La multiplication membre à membre des égalités V. 8 et V. 9 donne

V. 10. 
$$\lambda \lambda^{(1)} = \gamma_3 \sqrt{\gamma_1 \gamma_2}.$$

Mais  $\lambda \lambda^{(1)}$  fait partie du sous-corps  $K_1$  (v. ch. I. 6). Comme  $\gamma_1, \gamma_2$  et  $\gamma_3$  sont trois unités fondamentales de  $K_1$ , on peut écrire

V. 11. 
$$\lambda \lambda^{(1)} = \pm \gamma_1^{a_1} \gamma_2^{a_2} \gamma_3^{a_3},$$

où  $a_1, a_2$  et  $a_3$  sont des nombres entiers ordinaires.

L'égalité V. 10 devient, si on tient compte de V. 11,

$$\gamma_1^{a_1} \gamma_2^{a_2} \gamma_3^{a_3} = \gamma_3 \sqrt{\gamma_1 \gamma_2}$$

ou

$$\gamma_1^{2a_1} \gamma_2^{2a_2} \gamma_3^{2a_3} = \gamma_1 \gamma_2 \gamma_3^2.$$

De cette égalité on tire, en identifiant les exposants,

$$2a_1 = 1, \quad 2a_2 = 1, \quad 2a_3 = 2.$$

Mais les deux premières de ces égalités sont impossibles puisque  $a_1$  et  $a_2$  sont des entiers ordinaires. L'hypothèse qui nous y a conduit, à savoir que  $\lambda \equiv \sqrt[4]{\gamma_1 \gamma_2 \gamma_3^2}$  est une unité du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , est donc inadmissible.

Le tableau V. 7 se réduit au tableau suivant :

*Tableau des différentes formes des unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .*

Valeur du produit <i>a c f</i>	Forme des unités fondamentales.
1	$\gamma_r, \quad \gamma_s, \quad \gamma_u$
$2^1 = 2$	$\left\{ \begin{array}{l} \gamma_r, \quad \gamma_s, \quad \sqrt{\pm \gamma_u} \\ \gamma_r, \quad \gamma_s, \quad \sqrt{\pm \gamma_r \gamma_u} \\ \gamma_r, \quad \gamma_s, \quad \sqrt{\pm \gamma_r \gamma_s \gamma_u} \end{array} \right.$
$2^2 = 4$	$\left\{ \begin{array}{l} \gamma_r, \quad \sqrt{\pm \gamma_s}, \quad \sqrt{\pm \gamma_u} \\ \gamma_r, \quad \sqrt{\pm \gamma_s}, \quad \sqrt{\pm \gamma_r \gamma_u} \\ \gamma_r, \quad \sqrt{\pm \gamma_r \gamma_s}, \quad \sqrt{\pm \gamma_r \gamma_u} \end{array} \right.$
$2^3 = 8$	$\sqrt{\pm \gamma_r}, \quad \sqrt{\pm \gamma_s}, \quad \sqrt{\pm \gamma_u}$

V. 12.

CAS OÙ LE CORPS  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  CONTIENT SEPT UNITÉS  
FONDAMENTALES \*.

10. On sait que, dans ce cas, les sept sous-corps quadratiques de  $K$  sont réels. Nous désignerons dans ce qui suit par

$\varepsilon_1$	l'unité fondamentale du corps	$K(\sqrt{bqrs})$
$\varepsilon_2$	»	»
$\varepsilon_3$	»	»
$\varepsilon_4$	»	»
$\varepsilon_5$	»	»
$\varepsilon_6$	»	»
$\varepsilon_7$	»	»

Chacun des sept sous-corps du 4<sup>e</sup> degré est réel et admet trois unités fondamentales. On sait en outre que, si  $\varepsilon_r, \varepsilon_s$  et  $\varepsilon_u$  sont les trois unités fondamentales des trois sous-corps quadratiques d'un corps  $K_j$  du 4<sup>e</sup> degré (v. ch. I. 6), les trois unités fondamentales de  $K_j$  peuvent prendre l'une des sept formes suivantes \*\* :

1.	$\varepsilon_r, \varepsilon_s,$	$\varepsilon_u$
2.	$\varepsilon_r, \varepsilon_s,$	$\sqrt{\varepsilon_u}$
3.	$\varepsilon_r, \varepsilon_s,$	$\sqrt{\varepsilon_r \varepsilon_u}$ ou $\sqrt{\varepsilon_s \varepsilon_u}$
4.	$\varepsilon_r, \varepsilon_s,$	$\sqrt{\varepsilon_r \varepsilon_s \varepsilon_u}$
5.	$\varepsilon_r, \sqrt{\varepsilon_s},$	$\sqrt{\varepsilon_u}$
6.	$\varepsilon_r, \sqrt{\varepsilon_s},$	$\sqrt{\varepsilon_r \varepsilon_u}$
7.	$\varepsilon_r, \sqrt{\varepsilon_r \varepsilon_s},$	$\sqrt{\varepsilon_r \varepsilon_u}$

V. 13.

Enfin, les unités  $\varepsilon_j$  contenues dans les différents sous-corps du 4<sup>e</sup> degré sont données par le tableau suivant :

le corps	$K_1(1, \sqrt{bqrs}, \sqrt{crps}, \sqrt{bcpq})$	contient	$\varepsilon_1, \varepsilon_2, \varepsilon_3$
»	$K_2(1, \sqrt{apqs}, \sqrt{crps}, \sqrt{caqr})$	»	$\varepsilon_4, \varepsilon_5, \varepsilon_6$
»	$K_3(1, \sqrt{apqs}, \sqrt{bqrs}, \sqrt{abrp})$	»	$\varepsilon_4, \varepsilon_{11}, \varepsilon_5$
»	$K_4(1, \sqrt{crps}, \sqrt{abrp}, \sqrt{abcs})$	»	$\varepsilon_2, \varepsilon_5, \varepsilon_7$
»	$K_5(1, \sqrt{apqs}, \sqrt{bcpq}, \sqrt{abcs})$	»	$\varepsilon_4, \varepsilon_{11}, \varepsilon_7$
»	$K_6(1, \sqrt{bqrs}, \sqrt{caqr}, \sqrt{abcs})$	»	$\varepsilon_1, \varepsilon_6, \varepsilon_7$
»	$K_7(1, \sqrt{abrp}, \sqrt{bcpq}, \sqrt{caqr})$	»	$\varepsilon_5, \varepsilon_{11}, \varepsilon_6$

Nous désignerons dans la suite par  $\alpha_1, \beta_1, \gamma_1$  un système d'unités fondamentales du sous-corps du 4<sup>e</sup> degré  $K_1$ ; par  $\alpha_2, \beta_2, \gamma_2$  un système

\* Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  sera désigné par  $K$ .

\*\* Voir Amberg, op. cit., § 5.

d'unités fondamentales du sous-corps  $K_2$ , etc... ; par  $\alpha_n, \beta_n, \gamma_n$  un système d'unités fondamentales du sous-corps  $K_n$ . De plus, les unités fondamentales des trois corps quadratiques contenues dans  $K_n$  seront désignées par  $\varepsilon_r^{(n)}, \varepsilon_s^{(n)}, \varepsilon_u^{(n)}$ ; par exemple, on aura pour le sous-corps  $K_3$ , si on se reporte au tableau V. 14,  $\varepsilon_r^{(3)} \equiv \varepsilon_4$ ;  $\varepsilon_u^{(3)} \equiv \varepsilon_1$ ;  $\varepsilon_s^{(3)} \equiv \varepsilon_5$ .

11. Nous avons tout d'abord le théorème suivant :

THÉORÈME. *On peut toujours choisir, parmi les 21 unités  $\alpha_n, \beta_n, \gamma_n$  ( $n = 1, 2, \dots, 7$ ) qui constituent les systèmes d'unités fondamentales des sept sous-corps du quatrième degré  $K_\lambda$ , sept unités  $\mu_1, \mu_2, \dots, \mu_7$ , telles que, si on les met sous la forme suivante :*

$$\begin{aligned} \mu_1 &= \pm \lambda_1^{a_1} \\ \mu_2 &= \pm \lambda_1^{b_1} \lambda_2^{a_2} \\ \mu_3 &= \pm \lambda_1^{c_1} \lambda_2^{b_2} \lambda_3^{a_3} \\ \mu_4 &= \pm \lambda_1^{d_1} \lambda_2^{c_2} \lambda_3^{b_3} \lambda_4^{a_4} \\ \mu_5 &= \pm \lambda_1^{e_1} \lambda_2^{d_2} \lambda_3^{c_3} \lambda_4^{b_4} \lambda_5^{a_5} \\ \mu_6 &= \pm \lambda_1^{f_1} \lambda_2^{e_2} \lambda_3^{d_3} \lambda_4^{c_4} \lambda_5^{b_5} \lambda_6^{a_6} \\ \mu_7 &= \pm \lambda_1^{g_1} \lambda_2^{f_2} \lambda_3^{e_3} \lambda_4^{d_4} \lambda_5^{c_5} \lambda_6^{b_6} \lambda_7^{a_7}, \end{aligned}$$

V. 15.

où  $\lambda_1, \lambda_2, \dots, \lambda_7$  forment un système d'unités fondamentales de  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , chacun des sept entiers  $a_1, a_2, \dots, a_7$  ne prenne que les valeurs 1 et 2.

Pour démontrer ce théorème, nous montrons

a) que, quelle que soit la forme des unités fondamentales des sous-corps du 4<sup>e</sup> degré (v. tableau V. 13), on peut toujours trouver, parmi les dites unités fondamentales, une unité fondamentale  $\mu_1$  qui soit telle que l'entier  $a_1$ , dans la première des égalités V. 15, ne puisse prendre que les valeurs 1 et 2.

b) qu'ayant choisi les unités  $\mu_1, \mu_2, \dots, \mu_{m-1}$  ( $m < 7$ ), des égalités V. 15, de telle manière que les entiers  $a_1, \dots, a_{m-1}$  ne puissent prendre que les valeurs 1 et 2, il est toujours possible de choisir  $\mu_m$  de telle façon que  $a_m$  jouisse de la même propriété.

De ces deux propriétés résulte le théorème énoncé.

12. Reprenons les égalités V.15 et posons

$$R \equiv a_1 a_2 \dots a_7.$$

$R$  est donc égal à 1 si les sept entiers  $a_\lambda$  sont égaux à 1 ;  $R = 2$  si un et un seul des entiers  $a_\lambda$  est égal à 2, les autres étant égaux à 1.

D'une manière générale,  $R = 2^k$  ( $1 \leq k \leq 7$ ) si  $k$  entiers de la suite  $a_1, a_2, \dots, a_7$  sont égaux à 2, et  $7 - k$  entiers de la même suite sont égaux à 1. La plus grande valeur de  $R$  est donc  $2^7 = 128$ .

13. *Cas particulier.* Supposons que quatre sous-corps du 4<sup>e</sup> degré aient des unités fondamentales de la forme (1), tableau V. 13.

Admettons, par exemple, (v. tableau V. 14) que  $\varepsilon_1, \varepsilon_2$  et  $\varepsilon_3$  soient les unités fondamentales de  $K_1$ ;  $\varepsilon_4, \varepsilon_2$  et  $\varepsilon_6$  celles de  $K_2$ ;  $\varepsilon_4, \varepsilon_1$  et  $\varepsilon_5$  celles de  $K_3$  et  $\varepsilon_2, \varepsilon_5, \varepsilon_7$  celles de  $K_4$ .

Les formules V. 15 s'écrivent, dans ce cas,

$$\begin{aligned}
 \varepsilon_1 &= \pm \lambda_1^{a_1} \\
 \varepsilon_2 &= \pm \lambda_1^{b_1} \lambda_2^{a_2} \\
 \varepsilon_3 &= \pm \lambda_1^{c_1} \lambda_2^{b_2} \lambda_3^{a_3} \\
 \varepsilon_4 &= \pm \lambda_1^{d_1} \lambda_2^{c_2} \lambda_3^{b_3} \lambda_4^{a_4} \\
 \varepsilon_5 &= \pm \lambda_1^{e_1} \lambda_2^{d_2} \lambda_3^{c_3} \lambda_4^{b_4} \lambda_5^{a_5} \\
 \varepsilon_6 &= \pm \lambda_1^{f_1} \lambda_2^{e_2} \lambda_3^{d_3} \lambda_4^{c_4} \lambda_5^{b_5} \lambda_6^{a_6} \\
 \varepsilon_7 &= \pm \lambda_1^{g_1} \lambda_2^{f_2} \lambda_3^{e_3} \lambda_4^{d_4} \lambda_5^{c_5} \lambda_6^{b_6} \lambda_7^{a_7}.
 \end{aligned}$$

V. 16.

On a alors le

THÉORÈME. — *Dans le cas particulier des formules V. 16, le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  n'admet aucune unité de la forme  $\sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \dots \varepsilon_k^{\alpha_k}}$  ( $k \leq 7$ ) dans laquelle l'entier  $n$  est supérieur à 2.*

*Démonstration.* Tout d'abord, il est évident que l'entier  $n$  est pair et, si  $n > 2$ , c'est un multiple de 4, soit  $n = 4n_1$ . Il en résulte que l'un au moins des exposants  $\alpha_1, \alpha_2, \dots, \alpha_k$ , dans l'expression  $\sqrt[n]{\pm \varepsilon_1^{\alpha_1} \dots \varepsilon_k^{\alpha_k}}$ , est impair. Supposons, pour fixer les idées, que  $\alpha_1$  soit impair et posons  $\alpha_1 \equiv 2\alpha'_1 + 1$ .

Posons encore

$$\theta \equiv \sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \dots \varepsilon_k^{\alpha_k}}.$$

V. 17.

Si on applique aux deux membres de V. 17 la permutation  $\varphi_1$  (v. ch. I. 4), les unités  $\varepsilon_1, \varepsilon_2$  et  $\varepsilon_3$  ne changent pas, puisque ces trois unités font partie de  $K_1$ , tandis que l'unité  $\varepsilon_\lambda^{\alpha_\lambda}$ , pour  $\lambda > 3$ , se transforme en son conjugué  $\varepsilon'_\lambda{}^{\alpha_\lambda}$ .

L'égalité V. 17 devient

$$\theta' \equiv \sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \varepsilon_3^{\alpha_3} \varepsilon'_4{}^{\alpha_4} \dots}$$

V. 18.

On obtient, par multiplication membre à membre des égalités V. 17 et V. 18,

$$\theta\theta' = \sqrt[n]{\pm \varepsilon_1^{2\alpha_1} \varepsilon_2^{2\alpha_2} \varepsilon_3^{2\alpha_3}} \quad \text{ou}$$

V. 19.  $(\theta\theta')^n = \pm \varepsilon_1^{2\alpha_1} \varepsilon_2^{2\alpha_2} \varepsilon_3^{2\alpha_3}.$

Mais  $\theta\theta'$  fait partie du sous-corps  $K_1$  dont les unités fondamentales sont, par hypothèse,  $\varepsilon_1, \varepsilon_2$  et  $\varepsilon_3$  (v. ch. I. 6). On peut donc écrire comme suit le produit  $\theta\theta'$  :

V. 20.  $\theta\theta' = \pm \varepsilon_1^{a_1} \varepsilon_2^{a_2} \varepsilon_3^{a_3}$

où  $a_1, a_2$  et  $a_3$  sont des entiers ordinaires.

L'égalité V.19 devient, en vertu de V. 20,

$$\pm \varepsilon_1^{a_1 n} \varepsilon_2^{a_2 n} \varepsilon_3^{a_3 n} = \pm \varepsilon_1^{2\alpha_1} \varepsilon_2^{2\alpha_2} \varepsilon_3^{2\alpha_3}.$$

On en déduit

$$na_1 = 2\alpha_1; \quad na_2 = 2\alpha_2; \quad na_3 = 2\alpha_3.$$

Si on rappelle que  $n = 4n_1$  et  $\alpha_1 = 2\alpha'_1 + 1$ , la première des égalités ci-dessus s'écrit

$$4a_1 n_1 = 4\alpha'_1 + 2$$

d'où

$$2a_1 n_1 = 2\alpha'_1 + 1.$$

Cette dernière égalité étant impossible, l'hypothèse qui nous y a conduit doit être rejetée. Le nombre  $\theta = \sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \dots \varepsilon_k^{\alpha_k}}$  ne peut pas être une unité du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  dès que  $n$  est supérieur à 2.

14. *Forme des unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  dans le cas particulier du n° 13.*

*Notations.* Pour simplifier l'écriture, nous admettrons ce qui suit :

1)  $\sqrt{\varepsilon_1}$  représentera l'une quelconque des sept unités

$$\sqrt{\pm \varepsilon_1}, \sqrt{\pm \varepsilon_2}, \dots, \sqrt{\pm \varepsilon_7}.$$

2)  $\sqrt{\varepsilon_1 \varepsilon_2}$  représentera l'une quelconque des  $\frac{7 \cdot 6}{2} = 21$  unités

$$\sqrt{\pm \varepsilon_1 \varepsilon_2}, \dots, \sqrt{\pm \varepsilon_6 \varepsilon_7}.$$

3) Dans un système d'unités fondamentales du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , système qui comprend 7 unités, nous n'écrirons que les unités  $\varepsilon_\lambda$  situées sous un radical. Par exemple, le système  $\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7$  s'écrira comme suit :

$$[\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}].$$

4) Nous ne considérerons pas comme distincts deux systèmes tels que les deux suivants :

$$[\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}] \quad \text{et} \quad [\sqrt{\varepsilon_3}, \sqrt{\varepsilon_4}].$$

Dans ce cas, nous n'indiquerons que l'un d'eux, par exemple  $[\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}]$  et ce dernier représentera tous les systèmes d'unités fondamentales qui contiennent deux unités de la forme  $\sqrt{\varepsilon_i}$  et cinq unités de la forme  $\varepsilon_j$ .

5) Enfin, au lieu d'écrire  $\sqrt{\varepsilon_1 \varepsilon_2}$ , nous écrirons  $\sqrt{\varepsilon_{1,2}}$ .

*Tableau des différentes formes que peuvent prendre les unités fondamentales de  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .*

Posons, comme plus haut,

$$R \equiv a_1 a_2 \cdot \dots \cdot a_7.$$

Si  $R = 1$ , le seul système d'unités fondamentales est  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_7$  (1 forme).

Si  $R = 2$ , les systèmes possibles sont les suivants :

$$[\sqrt{\varepsilon_1}]; [\sqrt{\varepsilon_{1,2}}]; [\sqrt{\varepsilon_{1,2,3}}]; [\sqrt{\varepsilon_{1,2,3,4}}]; [\sqrt{\varepsilon_{1,2,\dots,5}}]; [\sqrt{\varepsilon_{1,\dots,6}}]; [\sqrt{\varepsilon_{1,\dots,7}}].$$

(7 formes.)

Si  $R = 4$

$$\begin{array}{lll} [\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}]; & [\sqrt{\varepsilon_{1,2}}, \sqrt{\varepsilon_{1,3}}]; & [\sqrt{\varepsilon_{1,2,3}}, \sqrt{\varepsilon_{1,2,4}}]; \\ [\sqrt{\varepsilon_1}, \sqrt{\varepsilon_{2,3}}]; & [\sqrt{\varepsilon_{1,2}}, \sqrt{\varepsilon_{1,3,4}}]; & [\sqrt{\varepsilon_{1,2,3}}, \sqrt{\varepsilon_{1,2,4,5}}]; \\ [\sqrt{\varepsilon_1}, \sqrt{\varepsilon_{2,3,4}}]; & [\sqrt{\varepsilon_{1,2}}, \sqrt{\varepsilon_{1,3,4,5}}]; & [\sqrt{\varepsilon_{1,2,3}}, \sqrt{\varepsilon_{1,2,4,5,6}}]; \\ [\sqrt{\varepsilon_1}, \sqrt{\varepsilon_{2,\dots,5}}]; & [\sqrt{\varepsilon_{1,2}}, \sqrt{\varepsilon_{1,3,\dots,6}}]; & [\sqrt{\varepsilon_{1,2,3}}, \sqrt{\varepsilon_{1,2,4,5,6,7}}]; \\ [\sqrt{\varepsilon_1}, \sqrt{\varepsilon_{2,\dots,6}}]; & [\sqrt{\varepsilon_{1,2}}, \sqrt{\varepsilon_{1,3,\dots,7}}]; & \\ [\sqrt{\varepsilon_1}, \sqrt{\varepsilon_{2,\dots,7}}]; & & \\ [\sqrt{\varepsilon_{1,2,3,4}}, \sqrt{\varepsilon_{1,2,3,5}}]; & [\sqrt{\varepsilon_{1,2,\dots,5}}, \sqrt{\varepsilon_{1,2,3,4,6}}]; & [\sqrt{\varepsilon_{1,2,\dots,6}}, \sqrt{\varepsilon_{1,2,\dots,5,7}}]. \\ [\sqrt{\varepsilon_{1,2,3,4}}, \sqrt{\varepsilon_{1,2,3,5,6}}]; & [\sqrt{\varepsilon_{1,2,\dots,5}}, \sqrt{\varepsilon_{1,2,3,4,6,7}}]; & \\ [\sqrt{\varepsilon_{1,2,3,4}}, \sqrt{\varepsilon_{1,2,3,5,6,7}}]; & & \end{array}$$

(21 formes)

Pour  $R = 8$ , on obtient de même 35 formes différentes ; pour  $R = 16$ , 35 formes et pour  $R = 64$ , 7 formes. Enfin, pour  $R = 128$ , le seul système d'unités fondamentales est le suivant :

$$[\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \sqrt{\varepsilon_3}, \sqrt{\varepsilon_4}, \sqrt{\varepsilon_5}, \sqrt{\varepsilon_6}, \sqrt{\varepsilon_7}].$$

Il y a donc au total

$$1 + 7 + 21 + 35 + 35 + 21 + 7 + 1 = 128 = 2^7$$

systèmes d'unités fondamentales.

## CHAPITRE VI

### Nombre de classes d'idéaux.

1. Considérons le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , réel ou imaginaire, de degré  $2^n \equiv m$ . Soit, d'autre part,  $\omega_1^{(1)}, \omega_2^{(1)}, \dots, \omega_m^{(1)}$  une base des entiers du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ . Formons, à l'aide de  $m$  variables réelles quelconques  $u_1, u_2, \dots, u_m$ , les formes linéaires

$$\zeta^{(s)} \equiv \omega_1^{(s)} u_1 + \omega_2^{(s)} u_2 + \dots + \omega_m^{(s)} u_m \quad (s = 1, 2, \dots, m),$$

expression dans laquelle  $\omega_\lambda^{(2)}, \omega_\lambda^{(3)}, \dots, \omega_\lambda^{(m)}$  sont les conjugués de  $\omega_\lambda^{(1)}$ .

Nous écrirons, de plus,

$$\zeta^{(1)} \equiv \zeta.$$

Posons maintenant, si le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  est réel, (tous les corps conjugués de  $K$ , soit  $K^{(2)}, K^{(3)}, \dots, K^{(m)}$ , sont alors réels) et pour  $\zeta^{(s)}$  non nul,

$$\log |\zeta^{(s)}| \equiv l_s(\zeta).$$

Si le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  est imaginaire, il en est de même des corps conjugués  $K^{(2)}, \dots, K^{(m)}$ . Si  $K^{(s)}$  et  $K^{(s')}$  sont deux corps imaginaires conjugués, nous poserons

$$\log |\zeta^{(s)}| \equiv \frac{1}{2} l_s(\zeta) - i l_{s'}(\zeta)$$

$$\log |\zeta^{(s')}| \equiv \frac{1}{2} l_s(\zeta) + i l_{s'}(\zeta)$$

où l'on a

$$0 \leq l_{s'}(\zeta) < 2\pi.$$

Les grandeurs

VI. 1.

$$l_1(\zeta), l_2(\zeta), \dots, l_m(\zeta)$$

sont toutes réelles et elles ont une détermination unique en fonction des variables  $u_1, u_2, \dots, u_m$ . Les grandeurs VI. 1 sont appelées *les logarithmes de la forme  $\zeta$* .

Si  $N(\xi)$  désigne la norme de  $\xi$  on peut écrire, en vertu de la définition de la norme, (v. ch. I. 5)

$$\text{VI. 2.} \quad \xi^{(1)} \xi^{(2)} \dots \xi^{(m)} = N(\xi).$$

2. 1<sup>er</sup> cas. Le corps  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$  est réel.

Si  $u_1, u_2, \dots, u_m$  sont des entiers ordinaires non tous nuls, le nombre  $\xi = \xi^{(1)}$  est un entier du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , entier qui est différent de zéro. Posons  $\xi \equiv \alpha$ . Les grandeurs  $l_1(\alpha), l_2(\alpha), \dots, l_m(\alpha)$  sont dites les *logarithmes du nombre entier  $\alpha$* .

L'égalité VI. 2 devient, si on y remplace  $\xi$  par  $\alpha$  et si on pose  $\alpha^{(1)} \equiv \alpha$ ,

$$\alpha^{(1)} \alpha^{(2)} \alpha^{(3)} \dots \alpha^{(m)} = N(\alpha),$$

d'où l'on déduit

$$\text{VI. 3.} \quad l_1(\alpha) + l_2(\alpha) + l_3(\alpha) + \dots + l_m(\alpha) = lN(\alpha),$$

où  $lN(\alpha)$  désigne la partie réelle du logarithme de  $N(\alpha)$ .

Désignons par  $\lambda$  une unité quelconque du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ . Comme on a  $N(\lambda) = +1$  ou  $-1$ , l'égalité VI. 3 devient, si on y remplace  $\alpha$  par  $\lambda$ ,

$$\text{VI. 4.} \quad l_1(\lambda) + l_2(\lambda) + l_3(\lambda) + \dots + l_m(\lambda) = 0.$$

Or, le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  étant réel par hypothèse, il admet  $r \equiv m - 1$  unités fondamentales (v. ch. V). L'égalité VI. 4 peut donc s'écrire

$$\text{VI. 5.} \quad l_1(\lambda) + l_2(\lambda) + \dots + l_{r+1}(\lambda) = 0.$$

2<sup>e</sup> cas. Le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  est imaginaire.

Si on désigne, comme dans le cas précédent, par  $\alpha$  un nombre entier du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , l'égalité VI. 3 peut s'écrire

$$l_1(\alpha) + l_2(\alpha) + \dots + l_{\frac{m}{2}}(\alpha) = lN(\alpha).$$

Désignons par  $\lambda$  une unité du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , l'égalité ci-dessus s'écrit, pour  $\lambda = \alpha$ ,

$$\text{VI. 6.} \quad l_1(\lambda) + l_2(\lambda) + \dots + l_{\frac{m}{2}}(\lambda) = 0.$$

Mais le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  admet dans ce cas  $r \equiv \frac{m}{2} - 1$  unités fondamentales. L'égalité VI. 6 devient, si on y remplace  $\frac{m}{2}$  par  $r + 1$ ,

$$l_1(\lambda) + l_2(\lambda) + \dots + l_{r+1}(\lambda) = 0.$$

La relation VI. 5 reste donc valable quand le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  est imaginaire.

LE RÉGULATEUR DU CORPS  $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$ .

3. Désignons par  $\lambda_1, \lambda_2, \dots, \lambda_r$  un système d'unités fondamentales du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , le corps  $K$  pouvant être réel ou imaginaire. Formons le déterminant

$$\text{VI. 7. } \Delta_\lambda \equiv \begin{vmatrix} l_1(\lambda_1) & l_1(\lambda_2) & \dots & l_1(\lambda_r) \\ l_2(\lambda_1) & l_2(\lambda_2) & \dots & l_2(\lambda_r) \\ l_3(\lambda_1) & l_3(\lambda_2) & \dots & l_3(\lambda_r) \\ \dots & \dots & \dots & \dots \\ l_r(\lambda_1) & l_r(\lambda_2) & \dots & l_r(\lambda_r) \end{vmatrix}$$

On appelle *régulateur* du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})^*$ , et on désigne par  $E$ , l'expression

$$\text{VI. 8. } E \equiv \frac{\Delta_\lambda}{u},$$

où  $\Delta_\lambda$  est le déterminant VI. 7 et où  $u$  désigne le nombre des racines de l'unité contenues dans le corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ .

4. Désignons par  $h$  le nombre de classes d'idéaux du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$  et posons

$$\Omega(s) \equiv \prod \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}},$$

le symbole  $\Pi$  étant étendu à tous les idéaux premiers  $\mathfrak{p}$  du corps  $K(\sqrt{A_1}, \dots, \sqrt{A_n})$ , et  $N(\mathfrak{p})$  désignant la norme de l'idéal  $\mathfrak{p}$ .

Nous utiliserons dans la suite la formule suivante\*\* :

$$\text{VI. 9. } \lim_{s \rightarrow 1} (s - 1) \Omega(s) = gh,$$

où  $h$  désigne le nombre de classes d'idéaux, où l'on a posé

$$\text{VI. 10. } g \equiv \frac{\chi E (2\pi)^{n-\nu}}{\sqrt{D}} \quad \text{et où} \quad \chi \equiv 2^{2\nu-n-1}.$$

Dans cette dernière expression,  $E$  désigne le régulateur du corps (v. formule VI. 8),  $n$  est le degré du corps. Quant à  $\nu$ , c'est  $r_1 + r_2$  (v. ch. V. 1). Or, on a vu au chapitre V que  $r = r_1 + r_2 - 1$ . On a donc  $\nu = r_1 + r_2 = r + 1$ . Enfin,  $D$  est le discriminant du corps (v. ch. III).

\* Voir Lejeune Dirichlet, 3<sup>e</sup> édition, p. 569.

\*\* Voir Lejeune Dirichlet, op. cit., p. 578.

Si on désigne par  $p$  un nombre premier ordinaire, on peut écrire la fonction  $\Omega(s)$  comme suit \* :

$$\text{VI. 11. } \Omega(s) = \prod_{(p)} \left( \frac{1}{1 - p^{-n_1 s}} \cdot \frac{1}{1 - p^{-n_2 s}} \cdot \dots \cdot \frac{1}{1 - p^{-n_e s}} \right),$$

où  $n_1, n_2, \dots, n_e$  sont les degrés respectifs des idéaux contenus dans  $(p)$  et où l'on a donc

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_e$$

$$\text{et } N(\mathfrak{p}_1) = p^{n_1}, \quad N(\mathfrak{p}_2) = p^{n_2}, \quad N(\mathfrak{p}_e) = p^{n_e}.$$

Le produit  $\Pi$  est étendu à tous les nombres premiers  $p$ .

#### APPLICATION AU CORPS $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

5. Dans ce chapitre,  $p$  désignera un nombre premier rationnel. Reprenons les formules IV. 21 qui donnent les différentes décompositions en facteurs idéaux de l'idéal principal  $(\pi)$  que nous écrirons donc  $(p)$ .

*1<sup>er</sup> cas.* Les sept symboles  $\left(\frac{D_\lambda}{p}\right)$  sont égaux à  $+1$ .

$$\text{Dans ce cas, on a } (p) = \mathfrak{p}_1 \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_8,$$

expression dans laquelle  $\mathfrak{p}_1, \dots, \mathfrak{p}_8$  désignent des idéaux du 1<sup>er</sup> degré. Le facteur sous le symbole  $\Pi$  dans la formule VI. 11 s'écrit, si on remarque que  $n_1 = n_2 = \dots = n_8 = 1$ ,

$$\begin{aligned} & \left(\frac{1}{1 - p^{-s}}\right)^8 = (1 - p^{-s})^{-8} \\ & = (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_1}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_2}{p}\right) p^{-s}\right]^{-1} \cdot \dots \cdot \left[1 - \left(\frac{D_7}{p}\right) p^{-s}\right]^{-1}. \end{aligned}$$

*2<sup>e</sup> cas.* Trois symboles  $\left(\frac{D_\lambda}{p}\right)$  sont égaux à  $+1$  et les quatre autres à  $-1$ .

Le facteur sous le symbole  $\Pi$  dans la formule VI. 11 peut s'écrire

$$\begin{aligned} & (1 - p^{-2s})^{-4} = (1 - p^{-s}) \cdot \left[1 - \left(\frac{D_r}{p}\right) p^{-s}\right]^{-1} \\ & \cdot \left[1 - \left(\frac{D_u}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_v}{p}\right) p^{-s}\right]^{-1} \cdot \prod_w \left[1 - \left(\frac{D_w}{p}\right) p^{-s}\right]^{-1}, \end{aligned}$$

où  $\left(\frac{D_r}{p}\right)$ ,  $\left(\frac{D_u}{p}\right)$  et  $\left(\frac{D_v}{p}\right)$  sont les trois symboles qui sont égaux à

\* Voir Lejeune Dirichlet, op. cit., p. 579.

+ 1 et où  $w$  prend les quatre valeurs de la suite 1, 2, ..., 7 qui sont différentes de  $r$ ,  $u$  et  $v$ .

3<sup>e</sup> cas. Quatre symboles  $\left(\frac{D_\lambda}{p}\right)$  sont nuls et les trois autres sont égaux à + 1.

Le facteur sous le symbole  $\Pi$  dans la formule VI. 11 s'écrit, dans ce cas,

$$(1 - p^{-s})^{-4} = (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_r}{p}\right) p^{-s}\right]^{-1} \\ \cdot \left[1 - \left(\frac{D_u}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_v}{p}\right) p^{-s}\right]^{-1} \cdot \Pi_w \left[1 - \left(\frac{D_w}{p}\right) p^{-s}\right]^{-1}$$

où  $\left(\frac{D_r}{p}\right) = \left(\frac{D_u}{p}\right) = \left(\frac{D_v}{p}\right) = 1$ , tandis que  $\left(\frac{D_w}{p}\right) = 0$  pour  $w \neq r$ ,  $u$  et  $v$ .

4<sup>e</sup> cas. Quatre symboles  $\left(\frac{D_\lambda}{p}\right)$  sont nuls, deux symboles sont égaux à - 1 et un seul symbole est égal à + 1.

En posant

$$\left(\frac{D_r}{p}\right) = +1; \quad \left(\frac{D_u}{p}\right) = \left(\frac{D_v}{p}\right) = -1 \quad \text{et} \quad \left(\frac{D_w}{p}\right) = 0 \quad \text{pour} \quad w \neq r, u \text{ et } v,$$

le facteur sous le symbole  $\Pi$  dans la formule VI. 11 peut s'écrire

$$(1 - p^{-2s})^{-2} = (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_r}{p}\right) p^{-s}\right]^{-1} \\ \cdot \left[1 - \left(\frac{D_u}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_v}{p}\right) p^{-s}\right]^{-1} \cdot \Pi_w \left[1 - \left(\frac{D_w}{p}\right) p^{-s}\right]^{-1}.$$

5<sup>e</sup> cas. Un symbole est égal à + 1, soit  $\left(\frac{D_r}{p}\right) = +1$ ; les six autres symboles sont nuls; posons  $\left(\frac{D_w}{p}\right) = 0$  pour  $w \neq r$ .

Le facteur sous le symbole  $\Pi$  dans la formule VI. 11 s'écrit

$$(1 - p^{-s})^{-2} = (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_r}{p}\right) p^{-s}\right]^{-1} \cdot \Pi_w \left[1 - \left(\frac{D_w}{p}\right) p^{-s}\right]^{-1}.$$

6<sup>e</sup> cas. Un seul symbole, soit  $\left(\frac{D_r}{p}\right)$ , est égal à - 1 et les six autres symboles sont nuls.

On a, dans ce cas,

$$(1 - p^{-2s})^{-1} = (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_r}{p}\right) p^{-s}\right]^{-1} \cdot \prod_w \left[1 - \left(\frac{D_w}{p}\right) p^{-s}\right]^{-1}.$$

En résumé, dans les six cas du tableau IV. 21, c'est-à-dire quelle que soit la décomposition de l'idéal  $(p)$  en facteurs idéaux du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , le facteur sous le symbole  $\Pi$  dans la formule VI. 11 peut se mettre sous la forme

$$\text{VI. 12.} \quad (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_1}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_2}{p}\right) p^{-s}\right]^{-1} \cdot \dots \\ \dots \cdot \left[1 - \left(\frac{D_7}{p}\right) p^{-s}\right]^{-1}.$$

6. Reprenons la formule VI. 11. La fonction  $\Omega(s)$  peut alors s'écrire comme suit \* :

$$\text{VI. 13.} \quad \Omega(s) = \sum \frac{1}{m^s} \sum \frac{1}{m^s} \left(\frac{D_1}{m}\right) \sum \frac{1}{m^s} \left(\frac{D_2}{m}\right) \cdot \dots \cdot \sum \frac{1}{m^s} \left(\frac{D_7}{m}\right)$$

où les sommations s'étendent à tous les entiers ordinaires  $m$ .

La formule VI. 13 peut s'écrire, en vertu de VI. 9,

$$\text{VI. 14.} \quad \lim_{s \rightarrow 1} (s - 1) \Omega(s) = \lim_{s \rightarrow 1} \sum_m \frac{s-1}{m^s} \sum_m \frac{1}{m^s} \left(\frac{D_1}{m}\right) \cdot \dots \\ \dots \cdot \sum_m \frac{1}{m^s} \left(\frac{D_7}{m}\right) = gh.$$

Or, on a

$$\lim_{s \rightarrow 1} \sum_m \frac{s-1}{m^s} = 1 \quad \text{et} \quad \lim_{s \rightarrow 1} \sum_m \frac{1}{m^s} \left(\frac{D_\lambda}{m}\right) = \sum_m \frac{1}{m} \left(\frac{D_\lambda}{m}\right) \quad (\lambda = 1, 2, \dots, 7).$$

La formule VI. 14 devient alors

$$\text{VI. 15.} \quad \sum_m \frac{1}{m} \left(\frac{D_1}{m}\right) \sum_m \frac{1}{m} \left(\frac{D_2}{m}\right) \cdot \dots \cdot \sum_m \frac{1}{m} \left(\frac{D_7}{m}\right) = gh.$$

Si on pose, pour simplifier l'écriture,

$$\sum_m \frac{1}{m} \left(\frac{D_\lambda}{m}\right) \equiv \sum_\lambda \quad \text{pour } \lambda = 1, 2, \dots, 7,$$

et si on remplace  $g$  par sa valeur donnée par la formule VI. 10, on tire de la formule VI. 15

$$\text{VI. 16.} \quad h = \frac{\sum_1 \sum_2 \cdot \dots \cdot \sum_7 \sqrt{D}}{\chi E (2\pi)^{n-\nu}}.$$

\* Voir Lejeune Dirichlet, op. cit., p. 580 et 609.

Nous distinguerons maintenant deux cas suivant que le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  admet trois ou sept unités fondamentales.

7. Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  admet trois unités fondamentales. On a, dans ce cas, (v. ch. V) :

$$\nu = 4; \quad n = 8; \quad \chi = 2^{2\nu-n-1} = 2^{-1}; \quad n - \nu = 4.$$

La formule VI. 16 devient donc

$$\text{VI. 17.} \quad h = \frac{\sum_1 \sum_2 \dots \sum_7 \sqrt{D}}{2^{\frac{1}{2}} E \pi^4}.$$

Calcul du régulateur  $E$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

Reprenons les formules V. 1

$$\text{VI. 18.} \quad \begin{aligned} \eta_1 &= \pm \lambda_1^a \\ \eta_2 &= \pm \lambda_1^b \lambda_2^c \\ \eta_3 &= \pm \lambda_1^d \lambda_2^e \lambda_3^f \end{aligned}$$

où  $\lambda_1, \lambda_2$  et  $\lambda_3$  sont trois unités fondamentales de  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ , tandis que  $\eta_1, \eta_2$  et  $\eta_3$  sont trois unités fondamentales du sous-corps réel  $K_1(\sqrt{bqrs}, \sqrt{crps})$ .

Désignons par  $\Delta_\eta$  le déterminant VI. 7 relatif aux  $\eta$ , on a

$$\text{VI. 19.} \quad \Delta_\eta = \begin{vmatrix} l_1(\eta_1) & l_1(\eta_2) & l_1(\eta_3) \\ l_2(\eta_1) & l_2(\eta_2) & l_2(\eta_3) \\ l_3(\eta_1) & l_3(\eta_2) & l_3(\eta_3) \end{vmatrix}$$

où les  $l_r(\eta_s)$  ont la signification rappelée aux § 1 et 2 de ce chapitre. On tire des égalités VI. 18

$$\left. \begin{aligned} l_r(\eta_1) &= a l_r(\lambda_1) \\ l_r(\eta_2) &= b l_r(\lambda_1) + c l_r(\lambda_2) \\ l_r(\eta_3) &= d l_r(\lambda_1) + e l_r(\lambda_2) + f l_r(\lambda_3) \end{aligned} \right\} \text{ pour } r = 1, 2, 3.$$

Le déterminant  $\Delta_\eta$  (formule VI.19) peut s'écrire

$$\text{VI. 20.} \quad \Delta_\eta = acf \cdot \Delta_\lambda$$

où  $\Delta_\lambda$  désigne le déterminant VI. 7 relatif aux  $\lambda_r$ .

Pour calculer  $\Delta_\eta$  il faut distinguer six cas différents suivant la forme des unités fondamentales  $\eta_1, \eta_2$  et  $\eta_3$  du sous-corps réel  $K_1$ . Ces unités fondamentales sont données par le tableau V.13.

Si on calcule la valeur de  $\Delta_\eta$  pour les six cas de ce tableau, on voit que  $\Delta_\eta$  a la forme suivante :

$$\text{VI. 21.} \quad \Delta_\eta = 2^\rho l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3)$$

où  $\rho$ , entier ordinaire, est donné par le tableau suivant :

Cas	Unités fondamentales du sous-corps $K_1(\sqrt{bqrs}, \sqrt{rcps})$			Valeur de $\rho$	
VI. 22	1	$\varepsilon_1,$	$\varepsilon_2,$	$\varepsilon_3$	2
	2	$\varepsilon_1,$	$\varepsilon_2,$	$\sqrt{\varepsilon_3}$	1
	3	$\varepsilon_1,$	$\varepsilon_2,$	$\sqrt{\varepsilon_1 \varepsilon_3}$	1
	4	$\varepsilon_1,$	$\varepsilon_2,$	$\sqrt{\varepsilon_1 \varepsilon_2 \varepsilon_3}$	1
	5	$\varepsilon_1,$	$\sqrt{\varepsilon_2},$	$\sqrt{\varepsilon_3}$	0
	6	$\varepsilon_1,$	$\sqrt{\varepsilon_2},$	$\sqrt{\varepsilon_1 \varepsilon_3}$	0
	7	$\varepsilon_1,$	$\sqrt{\varepsilon_1 \varepsilon_2},$	$\sqrt{\varepsilon_1 \varepsilon_3}$	0

La formule VI.20 donne

VI. 23. 
$$\Delta_\lambda = \frac{\Delta_\eta}{acf}.$$

Or, le produit  $acf$  est une puissance de 2 que nous représenterons par  $2^\mu$ , où  $\mu = 0, 1, 2$  ou 3 (v. tableau V. 12). Par suite, la formule VI. 23 peut s'écrire, si on remplace  $\Delta_\eta$  par sa valeur VI. 21,

VI. 24. 
$$\Delta_\lambda = 2^\sigma l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3),$$

expression dans laquelle on a  $2^\sigma \equiv 2^{\rho-\mu}$ . L'exposant  $\sigma$ , qui dépend à la fois de la forme des unités fondamentales  $\eta_1, \eta_2$  et  $\eta_3$  du sous-corps réel  $K_1(\sqrt{bqrs}, \sqrt{rcps})$  (v. tableau VI. 22) et de la valeur du produit  $acf$ , est donné par le tableau suivant :

	$acf = 1$	$acf = 2$	$acf = 2^2$	$acf = 2^3$	
VI. 25	1	2	1	0	-1
	2	1	0	-1	-2
	3	1	0	-1	-2
	4	1	0	-1	-2
	5	0	-1	-2	-3
	6	0	-1	-2	-3
	7	0	-1	-2	-3

La valeur de  $\rho$  correspondant au cas  $n^e$  du tableau VI.22 et à une valeur donnée du produit  $acf$ , se trouve à l'intersection de la  $n^e$  ligne du tableau VI.25 et de la colonne qui porte en tête la valeur donnée de  $acf$ .

Reprenons la formule VI. 8 donnant le régulateur du corps

$$\text{VI. 26.} \quad E = \frac{\Delta_\lambda}{u}$$

où  $\Delta_\lambda$  a la valeur VI. 24 et où  $u$  désigne le nombre des racines de l'unité contenues dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . D'après les hypothèses faites,  $u = 2$ , et le régulateur VI. 26 devient, si on remplace  $\Delta_\lambda$  par sa valeur,

$$\text{VI. 27.} \quad E = 2^{\sigma-1} l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3).$$

La formule VI. 17 donnant le nombre de classes d'idéaux devient, en vertu de VI. 27,

$$\text{VI. 28.} \quad h = \frac{\sum_1 \sum_2 \dots \sum_7 \sqrt{D_1} \sqrt{D_2} \dots \sqrt{D_7}}{2^{\sigma+2} \pi^3 l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3)}.$$

Désignons par  $h_1, h_2$  et  $h_3$  les nombres de classes d'idéaux des trois sous-corps quadratiques réels dont les discriminants sont  $D_1, D_2$  et  $D_3$ . On a \*

$$\text{VI. 29.} \quad h_1 = \frac{\sqrt{D_1} \sum_1}{l(\varepsilon_1)}, \quad h_2 = \frac{\sqrt{D_2} \sum_2}{l(\varepsilon_2)}, \quad h_3 = \frac{\sqrt{D_3} \sum_3}{l(\varepsilon_3)}.$$

Si  $h_4, h_5, h_6$  et  $h_7$  désignent respectivement les nombres de classes d'idéaux des quatre sous-corps quadratiques imaginaires dont les discriminants sont  $D_4, D_5, D_6$  et  $D_7$ , on a \*

$$h_\lambda = \frac{u \sqrt{D_\lambda} \sum_\lambda}{2\pi} \quad \text{pour } \lambda = 4, 5, 6, 7.$$

Mais  $u = 2$ , donc

$$\text{VI. 30.} \quad h_\lambda = \frac{\sqrt{D_\lambda} \sum_\lambda}{\pi} \quad \text{pour } \lambda = 4, 5, 6, 7.$$

Si on tient compte des formules VI. 29 et VI. 30, la formule VI.28 devient

$$\text{VI. 31.} \quad h = 2^{-(\sigma+2)} h_1 h_2 h_3 \dots h_7.$$

\* Voir Lejeune Dirichlet, op. cit., p. 608 et suiv.

8. Le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  admet sept unités fondamentales. Supposons, en premier lieu, que nous soyons dans le cas particulier du n° V. 13, et reprenons les formules V. 16, savoir :

$$\begin{aligned}
 \varepsilon_1 &= \pm \lambda_1^{a_1} \\
 \varepsilon_2 &= \pm \lambda_1^{b_1} \lambda_2^{a_2} \\
 \varepsilon_3 &= \pm \lambda_1^{c_1} \lambda_2^{b_2} \lambda_3^{a_3} \\
 &\dots\dots\dots \\
 \varepsilon_7 &= \pm \lambda_1^{g_1} \lambda_2^{f_2} \lambda_3^{e_3} \dots \lambda_7^{a_7}.
 \end{aligned}$$

Le déterminant VI. 7 s'écrit, dans ce cas,

$$\Delta_\varepsilon = \begin{vmatrix} l(\varepsilon_1), & l(\varepsilon_2), & l(\varepsilon_3), & l(\varepsilon_4), & l(\varepsilon_5), & l(\varepsilon_6), & l(\varepsilon_7) \\ l(\varepsilon_1), & l(\varepsilon_2), & l(\varepsilon_3), & -l(\varepsilon_4), & -l(\varepsilon_5), & -l(\varepsilon_6), & -l(\varepsilon_7) \\ -l(\varepsilon_1), & l(\varepsilon_2), & -l(\varepsilon_3), & l(\varepsilon_4), & -l(\varepsilon_5), & l(\varepsilon_6), & -l(\varepsilon_7) \\ l(\varepsilon_1), & -l(\varepsilon_2), & -l(\varepsilon_3), & l(\varepsilon_4), & l(\varepsilon_5), & -l(\varepsilon_6), & -l(\varepsilon_7) \\ -l(\varepsilon_1), & l(\varepsilon_2), & -l(\varepsilon_3), & -l(\varepsilon_4), & l(\varepsilon_5), & -l(\varepsilon_6), & l(\varepsilon_7) \\ -l(\varepsilon_1), & -l(\varepsilon_2), & l(\varepsilon_3), & l(\varepsilon_4), & -l(\varepsilon_5), & -l(\varepsilon_6), & l(\varepsilon_7) \\ l(\varepsilon_1), & -l(\varepsilon_2), & -l(\varepsilon_3), & -l(\varepsilon_4), & -l(\varepsilon_5), & l(\varepsilon_6), & l(\varepsilon_7) \end{vmatrix} = 2^9 l(\varepsilon_1) l(\varepsilon_2) \dots \dots \dots l(\varepsilon_7).$$

Si on désigne par  $\Delta_\lambda$  le déterminant VI.7 relatif aux  $\lambda$ , les formules VI. 32 permettent d'écrire

$$\Delta_\lambda = \frac{\Delta_\varepsilon}{a_1 a_2 \dots a_7}$$

ou, en remplaçant  $\Delta_\varepsilon$  par sa valeur VI. 33 et en rappelant que, dans le cas particulier du n° V. 13, on a  $a_1 a_2 \dots a_7 = 1$ ,

$$\text{VI. 34.} \quad \Delta_\lambda = 2^9 l(\varepsilon_1) l(\varepsilon_2) \dots \dots \dots l(\varepsilon_7).$$

Comme, par hypothèse, le nombre des racines de l'unité contenues dans le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est égal à 2, on a, pour le régulateur  $E$  du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  (v. formule VI. 8),

$$E = \frac{\Delta_\lambda}{u} = 2^8 l(\varepsilon_1) l(\varepsilon_2) \dots \dots \dots l(\varepsilon_7).$$

La formule VI. 16 donnant le nombre de classes devient

$$\text{VI. 35.} \quad h = \frac{\sum_1 \sum_2 \dots \sum_7 \sqrt{D}}{\chi \cdot (2\pi)^{n-\nu} 2^8 l(\varepsilon_1) \dots \dots \dots l(\varepsilon_7)}.$$

Mais on a, dans ce cas,

$$\nu = 8; \quad n = 8; \quad \chi = 2^{2\nu-n-1} = 2^7; \quad n - \nu = 0.$$

L'expression VI. 35 du nombre de classes d'idéaux s'écrit dès lors

$$\text{VI. 36.} \quad h = \frac{\sum_1 \sum_2 \dots \sum_7 \sqrt{D_1} \sqrt{D_2} \dots \sqrt{D_7}}{2^{15} l(\varepsilon_1) l(\varepsilon_2) \dots l(\varepsilon_7)} .$$

Les sept sous-corps quadratiques étant réels on a, si on désigne par  $h_\lambda$  le nombre de classes d'idéaux de l'un quelconque d'entre eux,

$$\text{VI. 37.} \quad h_\lambda = \frac{\sqrt{D_\lambda} \sum_\lambda}{l(\varepsilon_\lambda)} \quad \text{pour } \lambda = 1, 2, \dots, 7 .$$

La formule VI.36 peut donc s'écrire, en vertu de VI.37,

$$\text{VI. 38.} \quad h = 2^{-15} h_1 h_2 \dots h_7 .$$

Reprenons maintenant les formules V. 15 dans lesquelles les  $\mu_\lambda$  représentent des unités fondamentales choisies parmi les unités fondamentales des sous-corps du 4<sup>e</sup> degré  $K_1, K_2, \dots, K_7$ . Les  $\mu_\lambda$  peuvent donc prendre l'une des formes

$$\text{VI. 39.} \quad \varepsilon_1, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_1 \varepsilon_2}, \sqrt{\varepsilon_1 \varepsilon_2 \varepsilon_3} .$$

Mais si, dans les formules VI. 32, l'une des unités  $\varepsilon_\lambda$  est remplacée par l'une des unités VI. 39, on aura, suivant les cas,

$$l(\sqrt{\varepsilon_1}) = \frac{1}{2} l(\varepsilon_1); \quad l(\sqrt{\varepsilon_1 \varepsilon_2}) = \frac{1}{2} l(\varepsilon_1) + \frac{1}{2} l(\varepsilon_2); \quad \text{etc...}$$

Il s'ensuit que le déterminant  $\Delta_\varepsilon$ , donné par la formule VI. 33, se décompose en une somme de deux ou plusieurs déterminants, tous nuls sauf un seul, savoir le déterminant VI. 33 multiplié par une puissance de 2.

On aura donc encore dans ce cas

$$\text{VI. 40.} \quad h = 2^p h_1 h_2 \dots h_7 .$$

Les formules VI.34, VI.38 et VI.40 sont résumées par le théorème suivant :

**THÉORÈME.** *Le nombre de classes d'idéaux du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  est égal au produit des nombres de classes d'idéaux des sous-corps quadratiques multiplié par une puissance de 2.*

## CHAPITRE VII

### Etude des corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ qui contiennent, en plus de $+1$ et $-1$ , d'autres racines de l'unité.

1. Dans tout ce qui précède, nous avons supposé que le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  ne contenait que les deux seules racines de l'unité  $+1$  et  $-1$ . Nous allons examiner maintenant des corps qui contiennent, avec  $+1$  et  $-1$ , encore d'autres racines de l'unité.

Les racines  $n^{\text{ièmes}}$  primitives de l'unité sont racines d'une équation de degré  $\varphi(n)$ ,  $\varphi$  désignant la fonction arithmétique connue sous le nom d'indicateur d'Euler\*. Or, ces racines devant faire partie du corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  qui est de degré 8, elles doivent être racines d'une équation dont le degré est un diviseur de 8, donc racines d'une équation du premier, du second, du quatrième ou du huitième degré. On doit donc avoir, dans tous les cas,

$$\text{VII. 1.} \quad \varphi(n) \leq 8.$$

Cette inégalité entraîne les inégalités suivantes\*\* :

$$\varphi(n) \geq \sqrt{n} \quad \text{si } n \text{ est impair,}$$

$$\varphi(n) \geq \sqrt{\frac{n}{2}} \quad \text{si } n \text{ est pair.}$$

On déduit de ces inégalités

$$\text{VII. 2.} \quad \left\{ \begin{array}{l} n \leq [\varphi(n)]^2 \quad \text{si } n \text{ est impair,} \\ n \leq 2[\varphi(n)]^2 \quad \text{si } n \text{ est pair.} \end{array} \right.$$

\* Voir, par exemple, Henri Weber, *Traité d'Algèbre supérieure*, chap. XII, Paris, 1898.

\*\* Voir J. Amberg, op. cit. § 5.

Les inégalités VII. 2 deviennent, en vertu de VII. 1,

$$\begin{aligned} n &\leq 64 && \text{si } n \text{ est impair,} \\ n &\leq 128 && \text{si } n \text{ est pair.} \end{aligned}$$

Il suffit donc de calculer  $\varphi(n)$  pour les valeurs suivantes de  $n$  :

$$2, 3, 4, 5, \dots, 62, 63, 64 \text{ puis } 66, 68, 70, \dots, 128,$$

et de conserver les valeurs de  $\varphi(n)$  qui sont égales à 1, à 2, à 4 ou à 8. On obtient de cette manière le tableau suivant :

	$n$	$\varphi(n)$
VII. 3.	2 . . . . .	1
	3, 4, 6 . . . . .	2
	5, 8, 10, 12 . . .	4
	15, 16, 20, 24, 30	8

2. On sait que les racines  $n^{\text{ièmes}}$  de l'unité peuvent s'obtenir à l'aide de la formule générale

$$\text{VII. 4. } \sqrt[n]{1} = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \text{ pour } k = 1, 2, 3, \dots, n.$$

Nous donnons ci-après le tableau des racines  $n^{\text{ièmes}}$  pour les valeurs de  $n$  du tableau VII.3. A partir de  $n = 5$ , nous n'indiquons que la seule racine qu'on obtient en faisant  $k = 1$  dans la formule VII. 4.

*Racines carrées* + 1 et - 1

*Racines cubiques* + 1,  $\frac{-1 + \sqrt{-3}}{2}$ ,  $\frac{-1 - \sqrt{-3}}{2}$

*Racines quatrièmes* + 1, - 1, +  $i$ , -  $i$

*Racines cinquièmes*  $\frac{1}{4} [\sqrt{5} - 1 + i \sqrt{10} + 2\sqrt{5}]$

*Racines sixièmes*  $\frac{1 + \sqrt{-3}}{2}$

*Racines huitièmes*  $\frac{\sqrt{2 + \sqrt{-2}}}{2}$

*Racines dixièmes*  $\frac{1}{4} [\sqrt{5} + 1 + i \sqrt{10 - 2\sqrt{5}}]$

Racines douzièmes  $\frac{\sqrt{-1} + \sqrt{-3}}{2}$

Racines quinzièmes  $\frac{1}{8} \left[ \sqrt{5} + 1 + \sqrt{30 - 6\sqrt{5}} + i(\sqrt{3} + \sqrt{15} - \sqrt{10 - 2\sqrt{5}}) \right]$

Racines seizièmes  $\frac{1}{2} \left[ \sqrt{2 + \sqrt{2}} + i\sqrt{2 - \sqrt{2}} \right]$ .

Racines vingtièmes  $\frac{1}{4} \left[ \sqrt{10 + 2\sqrt{5}} + i(\sqrt{5} - 1) \right]$

Racines vingt-quatrièmes  $\frac{1}{2} \left[ \sqrt{2 + \sqrt{3}} + i\sqrt{2 - \sqrt{3}} \right]$

Racines trentièmes  $\frac{1}{8} \left[ \sqrt{30 + 6\sqrt{5}} + \sqrt{5} - 1 + i(\sqrt{10 + 2\sqrt{5}} - \sqrt{3} - \sqrt{15}) \right]$ .

3. Du tableau qui précède, nous tirons les conclusions suivantes :

- 1) Tout corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  contient les racines carrées de l'unité.
- 2) Le corps  $K(\sqrt{-1}, \sqrt{x}, \sqrt{y})$ , qui peut s'écrire plus explicitement, si l'on met en évidence la base du corps,

VII. 5.  $K(1, \sqrt{-1}, \sqrt{x}, \sqrt{y}, \sqrt{-x}, \sqrt{xy}, \sqrt{-y}, \sqrt{-xy})$ ,

où  $x$  et  $y$  sont des entiers ordinaires qui ne renferment aucun facteur carré, contient les racines quatrièmes de l'unité. Si nous supposons  $|x| \neq 2$  et  $\neq 3$ ;  $|y| \neq 2$  et  $\neq 3$ , le corps VII. 5 ne contient aucune racine d'ordre supérieur à 4, car il ne contient ni  $\sqrt{-3}$  ni  $\sqrt{\pm 2}$ , et il ne contient pas non plus les racines cubiques de l'unité.

- 3) Le corps  $K(\sqrt{-3}, \sqrt{x}, \sqrt{y})$ , qui peut s'écrire plus explicitement

VII. 6.  $K(1, \sqrt{-3}, \sqrt{x}, \sqrt{y}, \sqrt{-3x}, \sqrt{xy}, \sqrt{-3y}, \sqrt{-3xy})$ ,

contient les racines 6<sup>ièmes</sup> de l'unité. S'il ne contient pas les racines carrées  $\sqrt{-1}$ ,  $\sqrt{\pm 2}$  et  $\sqrt{+3}$ , il ne peut contenir aucune racine de l'unité d'un ordre supérieur à 6. Pour cela, il suffit de supposer

$$\begin{aligned} x \text{ et } y &\neq 2, \neq 3, \neq -1, \\ x &\neq -y. \end{aligned}$$

- 4) Le corps  $K(\sqrt{-3}, \sqrt{3}, \sqrt{y})$  ou

$$K(1, \sqrt{-3}, \sqrt{3}, \sqrt{y}, \sqrt{-1}, \sqrt{3y}, \sqrt{-3y}, \sqrt{-y}),$$

où l'on suppose  $y \neq 2$ , contient les racines carrées, cubiques, quatrièmes, sixièmes et douzièmes de l'unité, mais il ne contient pas les racines huitièmes.

5) Enfin, le corps  $K(\sqrt{-1}, \sqrt{2}, \sqrt{3})$  ou

VII. 8.  $K(1, \sqrt{2}, \sqrt{3}, \sqrt{-2}, \sqrt{6}, \sqrt{-3}, \sqrt{-6})$

contient à la fois les racines carrées, cubiques, quatrièmes, sixièmes, huitièmes et douzièmes de l'unité.

4. On démontre alors que les racines cinquièmes, dixièmes, quinzièmes, vingtièmes, trentièmes, ainsi que les racines seizeièmes et vingt-quatrièmes ne peuvent pas être contenues dans  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

Les corps algébriques en question ne peuvent contenir que les racines carrées, cubiques, quatrièmes, sixièmes, huitièmes et douzièmes de l'unité.

5. Nous allons étudier maintenant quelques-uns des corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  du § 3 ci-dessus.

En ce qui concerne la base des entiers, le discriminant du corps, la décomposition des idéaux, ces corps spéciaux suivent toutes les règles obtenues dans les chapitres précédents, car nous n'avons fait aucune hypothèse spéciale sur le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Par contre il s'agit d'examiner

- a) si les unités fondamentales ont les mêmes formes qu'au chapitre V ;
- b) si le théorème du chapitre VI sur le nombre de classes d'idéaux est encore valable.

6. Considérons, en premier lieu, le corps VII. 5

$K(1, \sqrt{-1}, \sqrt{x}, \sqrt{y}, \sqrt{-x}, \sqrt{xy}, \sqrt{-y}, \sqrt{-xy})$  où  $|x| \neq 2$  et  $3$  ;  
 $|y| \neq 2$  et  $3$ .

Ce corps contient les racines quatrièmes de l'unité  $+1, -1, +i$  et  $-i$ .

Désignons par  $\rho$  l'une quelconque de ces quatre unités et posons, comme au chapitre V, formule V. 1,

$$\begin{aligned} \eta_1 &= \rho_1 \lambda_1^a \\ \eta_2 &= \rho_2 \lambda_1^b \lambda_2^c \\ \eta_3 &= \rho_3 \lambda_1^d \lambda_2^e \lambda_3^f \end{aligned}$$

VII. 9.

où  $\rho_1, \rho_2$  et  $\rho_3$  représentent des racines quatrièmes de l'unité,  $\eta_1, \eta_2$  et  $\eta_3$  trois unités fondamentales du sous-corps réel du quatrième degré (v. ch. V. 5) ; enfin  $\lambda_1, \lambda_2$  et  $\lambda_3$  sont trois unités fondamentales du corps  $K(\sqrt{-1}, \sqrt{x}, \sqrt{y})$ .

On peut démontrer, comme au chapitre V, que les trois quantités  $a$ ,  $c$  et  $f$ , dans les formules VII. 9, ne peuvent prendre que les valeurs 1 ou 2. Considérons, en effet, par exemple, la première des égalités VII. 9

$$\text{VII. 10.} \quad \gamma_1 = \rho_1 \lambda_1^a.$$

Appliquons à cette dernière égalité la permutation  $\varphi_1$  qui laisse inchangé le sous-corps  $K_1$  et, par suite,  $\gamma_1$

$$\text{VII. 11.} \quad \gamma_1 = \rho_1^{(1)} \lambda_1^{(1)a}.$$

Multiplions membre à membre les deux égalités VII. 10 et VII. 11, il vient

$$\text{VII. 12} \quad \gamma_1^2 = \rho_1 \rho_1^{(1)} (\lambda_1 \lambda_1^{(1)})^a.$$

Or, je dis que le produit  $\rho_1 \rho_1^{(1)} = +1$ . En effet, que  $\rho_1$  soit égal à  $+1$  ou à  $-1$ , la permutation  $\varphi_1$  ne change pas  $\rho_1$ , et dès lors  $\rho_1 \rho_1^{(1)} = \rho_1^2 = +1$ .

Si au contraire  $\rho_1 = +i$  ou  $-i$ ,  $\varphi_1$  change  $\rho_1$  en  $-\rho_1$  et  $\rho_1 \rho_1^{(1)} = -i^2 = +1$ .

L'égalité VII. 12 s'écrit donc  $\gamma_1^2 = (\lambda_1 \lambda_1^{(1)})^a$ , et la démonstration continue comme au chapitre V. On en conclut que les unités fondamentales du corps  $K(\sqrt{-1}, \sqrt{x}, \sqrt{y})$  sont encore données par les formules V. 12.

On a trouvé, pour le nombre de classes, quand le corps  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$  a trois unités fondamentales (v. formule VI. 17),

$$\text{VII. 13.} \quad h = \frac{\sum_1 \sum_2 \dots \sum_7 \sqrt{D}}{2^3 E \pi^4}.$$

Si on se reporte aux définitions données au chapitre VI, on voit que les formules VII. 9 donnent, pour le déterminant VI. 7 relatif aux  $\lambda$ ,

$$\Delta_\lambda = \frac{2^k l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3)}{a c f}$$

où  $k$  est un entier ordinaire et où  $\varepsilon_1$ ,  $\varepsilon_2$  et  $\varepsilon_3$  sont les trois unités fondamentales des trois sous-corps quadratiques réels.

On a dans ce cas

$$E = \frac{\Delta_\lambda}{u}$$

où  $u$  est le nombre des racines de l'unité contenues dans  $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . Comme  $u = 4 = 2^2$  et que  $a c f$  est une puissance de

2, la formule VII. 13 peut s'écrire finalement comme suit :

$$h = \frac{2^l \sum_1 \sum_2 \dots \sum_7 \sqrt{D_1} \dots \sqrt{D_7}}{\pi^4 l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3)}$$

où  $l$  est un entier ordinaire.

Si l'on reprend les valeurs des nombres de classes d'idéaux des sous-corps quadratiques (v. ch. VI. 7), on voit que l'on a encore

$$h = 2^r h_1 h_2 \dots h_7$$

où  $r$  est un entier ordinaire.

7. Prenons, comme deuxième exemple, le corps VII. 6

$$K(1, \sqrt{-3}, \sqrt{x}, \sqrt{y}, \sqrt{-3x}, \sqrt{xy}, \sqrt{-3y}, \sqrt{-3xy}),$$

où  $x$  et  $y \neq -1, \neq 2$  et  $\neq 3$  et où  $x \neq -y$ .

Ce corps contient les racines sixièmes de l'unité. Soit  $\alpha$  l'une d'elles, le corps contient  $\pm 1, \pm \alpha, \pm \alpha^2$ .

Posons de nouveau

$$\begin{aligned} \text{VII. 14.} \quad \tau_1 &= \rho_1 \lambda_1^a \\ \tau_2 &= \rho_2 \lambda_1^b \lambda_2^c \\ \tau_3 &= \rho_3 \lambda_1^d \lambda_2^e \lambda_3^f \end{aligned}$$

où  $\rho_1, \rho_2$  et  $\rho_3$  sont des racines sixièmes de l'unité.

Considérons la première des égalités VII. 14

$$\tau_1 = \rho_1 \lambda_1^a$$

et appliquons aux deux membres la permutation  $\varphi_1$ ; l'égalité ci-dessus devient

$$\tau_1 = \rho_1 \lambda_1^{(1)a}$$

La multiplication membre à membre des deux dernières égalités donne

$$\text{VII. 15.} \quad \tau_1^2 = \rho_1 \rho_1^{(1)} (\lambda_1 \lambda_1^{(1)})^a.$$

$$\text{Or, } \rho_1 = \frac{\pm 1 \pm \sqrt{-3}}{2}; \quad \rho_1^{(1)} = \frac{\pm 1 \mp \sqrt{-3}}{2}; \quad \rho_1 \rho_1^{(1)} = 1.$$

L'égalité VII. 15 devient

$$\tau_1^2 = (\lambda_1 \lambda_1^{(1)})^a.$$

La démonstration et les calculs sont dès lors les mêmes qu'au chapitre V, et les unités sont encore données par le tableau V. 12.

*Nombre de classes.* Le régulateur du corps est  $E = \frac{\Delta_\lambda}{u}$ . Or,  $u = 6$  puisque le corps contient 6 racines de l'unité ; donc  $E = \frac{\Delta_\lambda}{6}$ .

Le nombre de classes (formule VI. 17) s'écrit dans ce cas

$$h = \frac{3 \cdot 2^t \sum_1 \sum_2 \dots \sum_7 \sqrt{D_1} \dots \sqrt{D_7}}{\pi^4 l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3)}$$

où  $t$  est un nombre entier ordinaire.

Si on reprend les valeurs des nombres de classes d'idéaux des sous-corps quadratiques (v. ch. VI) et si on remarque que le nombre de

classes du corps  $K(\sqrt{-3})$  est  $\frac{3 \sum_\lambda \sqrt{D_\lambda}}{\pi}$ , où  $\lambda$  est l'un des nombres 1, ..., 7, on voit que l'on a encore

$$h = 2^s h_1 h_2 \dots h_7.$$

Le théorème sur le nombre de classes (v. ch. VI. 8) est donc encore valable dans les cas spéciaux susmentionnés.

## DEUXIÈME PARTIE

### Etude des quaternions dont les coordonnées sont tirées du corps algébrique $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

#### CHAPITRE PREMIER

##### Définitions, notations ; opérations sur les quaternions complexes.

1. On appelle *quaternion* \* une expression de la forme

$$a \equiv a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3$$

où  $a_0, a_1, a_2$  et  $a_3$  sont des nombres rationnels dits les *coordonnées* du quaternion  $a$ , et où  $i_1, i_2$  et  $i_3$  sont trois symboles définis par les relations suivantes :

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

Quand l'une des coordonnées  $a_\lambda$  est égale à 1, on ne l'écrit pas. Par exemple  $a = a_0 + a_1 i_1 + i_2 + i_3$  désigne le quaternion dont les coordonnées sont  $a_0, a_1, 1, 1$ .

Si, dans l'expression de  $a$ , un terme fait défaut, cela signifie que la coordonnée correspondante est nulle.

*Exemple :*  $a = a_0 + a_2 i_2$

est le quaternion de coordonnées  $a_0, 0, a_2, 0$ .

Si  $a_0 = a_1 = a_2 = a_3 = 0$ , le quaternion est dit *nul*.

\* A. Hurwitz. *Zahlentheorie der Quaternionen*. Berlin, 1919.

A l'exception de la multiplication qui n'est pas commutative, les opérations sur les quaternions suivent les règles de l'algèbre classique.

En ce qui concerne la multiplication et la division, on distingue la multiplication à gauche, la multiplication à droite, la division à gauche et la division à droite.

Les quaternions dont nous venons de rappeler la définition seront appelés, dans la suite de ce travail, *quaternions à coordonnées rationnelles*, ou simplement *quaternions rationnels* \*, par opposition aux quaternions complexes que nous allons définir.

Les quaternions rationnels seront représentés par des lettres latines majuscules  $A, B, C, D, \dots$

2. Nous appellerons *quaternions complexes* des quaternions dont les coordonnées sont tirées d'un corps algébrique autre que le corps des nombres rationnels. Dans la présente étude, nous considérerons l'ensemble des quaternions complexes dont les coordonnées sont tirées du corps algébrique du huitième degré  $K(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps})$ , corps que nous avons étudié dans la première partie de ce travail \*\*. Le corps  $K(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps})$  sera appelé, dans la suite, le *corps primordial* \*\*\*, et nous le représenterons par  $K$ .

Les quaternions complexes à coordonnées tirées du corps primordial  $K$  seront désignés par des lettres grecques majuscules

$$A, B, \Gamma, \Delta, \dots$$

Les coordonnées des quaternions complexes sont donc des nombres du corps primordial  $K$ ; ces coordonnées seront représentées par des lettres grecques minuscules

$$\alpha, \beta, \gamma, \delta, \dots$$

Enfin, les nombres rationnels seront désignés par des lettres latines minuscules  $a, b, c, d, \dots$

Il résulte de la définition des quaternions complexes que l'un quelconque de ces derniers pourra s'écrire

$$(2) \quad A = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3.$$

\* On entend par *quaternions hamiltoniens* les quaternions dont les coordonnées sont des nombres réels. Les quaternions « rationnels » sont donc des quaternions hamiltoniens.

\*\* D'après cela, un « quaternion complexe », au sens que nous donnons à ce mot, peut être quaternion hamiltonien ou non.

\*\*\* Nous dirons parfois aussi, simplement, le corps  $K$ .

Les coordonnées  $\alpha_\lambda$  s'écrivent (v. 1<sup>re</sup> partie, ch. I) comme suit :

$$(3) \quad \left\{ \begin{array}{l} \alpha_\lambda = a_{\lambda,0} + a_{\lambda,1} \sqrt{apqs} + a_{\lambda,2} \sqrt{bqrs} + a_{\lambda,3} \sqrt{crps} + a_{\lambda,4} \sqrt{abrp} \\ \quad + a_{\lambda,5} \sqrt{bcpq} + a_{\lambda,6} \sqrt{caqr} + a_{\lambda,7} \sqrt{abcs} \end{array} \right.$$

pour  $\lambda = 0, 1, 2, 3$ .

3. *Addition et soustraction de deux quaternions complexes.* Soient les deux quaternions complexes

$$(4) \quad \left\{ \begin{array}{l} A = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \\ B = \beta_0 + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3. \end{array} \right.$$

On a

$$A \pm B \equiv \alpha_0 \pm \beta_0 + (\alpha_1 \pm \beta_1) i_1 + (\alpha_2 \pm \beta_2) i_2 + (\alpha_3 \pm \beta_3) i_3.$$

En particulier, le quaternion complexe

$$0 - A = -A = -\alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3$$

sera dit *l'opposé* de A.

On voit que l'addition est commutative et associative.

4. *Produit de deux quaternions complexes.* Soient les deux quaternions complexes (4).

Si on tient compte des relations (1), on obtient

$$AB = \pi_0 + \pi_1 i_1 + \pi_2 i_2 + \pi_3 i_3$$

où l'on a posé

$$(5) \quad \left\{ \begin{array}{l} \pi_0 \equiv \alpha_0 \beta_0 - \alpha_1 \beta_1 - \alpha_2 \beta_2 - \alpha_3 \beta_3 \\ \pi_1 \equiv \alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_3 - \alpha_3 \beta_2 \\ \pi_2 \equiv \alpha_0 \beta_2 - \alpha_1 \beta_3 + \alpha_2 \beta_0 + \alpha_3 \beta_1 \\ \pi_3 \equiv \alpha_0 \beta_3 + \alpha_1 \beta_2 - \alpha_2 \beta_1 + \alpha_3 \beta_0. \end{array} \right.$$

On voit que AB est, en général, différent de BA. On obtient pour ce dernier produit

$$(6) \quad \left\{ \begin{array}{l} BA = \rho_0 + \rho_1 i_1 + \rho_2 i_2 + \rho_3 i_3 \text{ avec} \\ \rho_0 \equiv \alpha_0 \beta_0 - \alpha_1 \beta_1 - \alpha_2 \beta_2 - \alpha_3 \beta_3 \\ \rho_1 \equiv \alpha_1 \beta_0 + \alpha_0 \beta_1 + \alpha_3 \beta_2 - \alpha_2 \beta_3 \\ \rho_2 \equiv \alpha_2 \beta_0 - \alpha_3 \beta_1 + \alpha_0 \beta_2 + \alpha_1 \beta_3 \\ \rho_3 \equiv \alpha_3 \beta_0 + \alpha_2 \beta_1 - \alpha_1 \beta_2 + \alpha_0 \beta_3 \end{array} \right.$$

Si  $AB = BA$  les quaternions A et B sont dits *permutables*.

5. *Conjugués et normes de quaternions complexes.* Soit le quaternion complexe

$$A = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3.$$

En appliquant successivement au quaternion complexe A les permutations  $\varphi_1, \varphi_2, \dots, \varphi_7$  du corps primordial K (voir 1<sup>re</sup> partie ch. I. 4), on obtient les quaternions

$$\begin{aligned} A^{(1)} &= \alpha_0^{(1)} + \alpha_1^{(1)} i_1 + \alpha_2^{(1)} i_2 + \alpha_3^{(1)} i_3 \\ &\dots\dots\dots \\ &\dots\dots\dots \\ A^{(7)} &= \alpha_0^{(7)} + \alpha_1^{(7)} i_1 + \alpha_2^{(7)} i_2 + \alpha_3^{(7)} i_3 \end{aligned}$$

D'autre part, en changeant les signes des trois dernières coordonnées de A, on obtient

$$\bar{A} = \alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3.$$

On constate que

$$\bar{A}A = A\bar{A} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.$$

Appliquons aussi au quaternion  $\bar{A}$  les permutations  $\varphi_1, \varphi_2, \dots, \varphi_7$  du corps primordial K ; on obtient les sept quaternions

$$\begin{aligned} \bar{A}^{(1)} &= \alpha_0^{(1)} - \alpha_1^{(1)} i_1 - \alpha_2^{(1)} i_2 - \alpha_3^{(1)} i_3 \\ &\dots\dots\dots \\ &\dots\dots\dots \\ \bar{A}^{(7)} &= \alpha_0^{(7)} - \alpha_1^{(7)} i_1 - \alpha_2^{(7)} i_2 - \alpha_3^{(7)} i_3. \end{aligned}$$

Formons le produit

$$(7) \quad A\bar{A} A^{(1)}\bar{A}^{(1)} A^{(2)}\bar{A}^{(2)} \dots A^{(7)}\bar{A}^{(7)} \equiv No(A).$$

En vertu de la propriété associative de la multiplication, propriété qui subsiste pour les quaternions, l'égalité (7) peut s'écrire

$$No(A) = (A\bar{A}) (A^{(1)}\bar{A}^{(1)}) \dots (A^{(7)}\bar{A}^{(7)})$$

ou encore

$$(8) \quad \left\{ \begin{aligned} No(A) &= (\alpha_0^{(2)} + \alpha_1^{(2)} + \alpha_2^{(2)} + \alpha_3^{(2)}) (\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \dots \\ &\dots (\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}). \end{aligned} \right.$$

Le second membre de l'égalité (8) est un nombre rationnel. Il sera dit la *norme* du quaternion complexe A ; cette norme sera désignée par  $No(A)$ .

Ecrivons le produit (7) comme suit :

$$No(A) = A (\bar{A}A^{(1)}\bar{A}^{(1)} \dots A^{(7)}\bar{A}^{(7)}).$$

Le quaternion complexe

$$(9) \quad \widehat{A} \equiv \overline{A}A^{(1)}\overline{A}^{(1)} \dots A^{(7)}\overline{A}^{(7)}$$

sera dit le *conjugué* de A. Il peut s'écrire aussi

$$\begin{aligned} \widehat{A} = & (\alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3) (\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \dots \\ & \dots (\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}). \end{aligned}$$

On peut écrire

$$A\widehat{A} = \widehat{A}A = No(A).$$

On voit donc que tout quaternion complexe est permutable avec son conjugué.

DÉFINITION. Le produit d'un quaternion complexe par son conjugué est dit la *norme* du quaternion complexe considéré.

On peut énoncer, en vertu de la formule 8, le théorème suivant :

THÉORÈME. *La norme d'un quaternion complexe est un nombre rationnel.*

THÉORÈME. *La norme d'un produit de quaternions complexes est égale au produit des normes des facteurs.*

Soient, en effet, les deux quaternions complexes

$$\begin{aligned} A &= \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \\ B &= \beta_0 + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3. \end{aligned}$$

Formons le produit

$$\begin{aligned} \widehat{B}A &= (\beta_0 - \beta_1 i_1 - \beta_2 i_2 - \beta_3 i_3) (\beta_0^{(1)2} + \beta_1^{(1)2} + \beta_2^{(1)2} + \beta_3^{(1)2}) \dots (\beta_0^{(7)2} + \beta_1^{(7)2} + \beta_2^{(7)2} + \beta_3^{(7)2}) \\ &\cdot (\alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3) (\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \dots (\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}) \end{aligned}$$

ce qui peut s'écrire encore

$$(10) \quad \left\{ \begin{aligned} \widehat{B}A &= (\beta_0^{(1)2} + \beta_1^{(1)2} + \beta_2^{(1)2} + \beta_3^{(1)2}) \dots (\beta_0^{(7)2} + \beta_1^{(7)2} + \beta_2^{(7)2} + \beta_3^{(7)2}) \\ &\cdot (\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \dots (\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}) \widehat{B}A. \end{aligned} \right.$$

Or, on a

$$\widehat{B}A = \pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3$$

où les  $\pi_\lambda$  ont les valeurs (5).

Si on désigne par  $\pi$  le produit des quatorze premiers facteurs du second membre de (10), l'égalité (10) s'écrit

$$\widehat{B}A = \pi(\pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3).$$

D'autre part, on a

$$\widehat{AB} = (\pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3) (\pi_0^{(1)2} + \pi_1^{(1)2} + \pi_2^{(1)2} + \pi_3^{(1)2}) \\ \dots (\pi_0^{(\tau)2} + \pi_1^{(\tau)2} + \pi_2^{(\tau)2} + \pi_3^{(\tau)2}),$$

ce qui peut s'écrire, tous calculs faits,

$$\widehat{AB} = (\pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3) \pi.$$

On a donc finalement

$$\widehat{AB} = \widehat{BA}$$

La norme d'un produit peut donc s'écrire

$$No(AB) = (AB) (\widehat{AB}) = AB \widehat{B} \widehat{A} = A(B\widehat{B}) \widehat{A} = A \cdot No(B) \cdot \widehat{A} = No(B) \cdot A\widehat{A}$$

d'où

$$No(AB) = No(A) \cdot No(B).$$

Le théorème est ainsi démontré pour deux facteurs ; par le passage de  $n$  à  $n + 1$ , on le démontrerait pour  $n$  facteurs.

6. L'ensemble des quaternions à coordonnées tirées du corps primordial  $K$  forme un *anneau de quaternions*, ou un *domaine numéral*, que nous désignerons par  $\Omega$ . Si  $\Omega$  contient le quaternion  $\Gamma$ , il contient aussi son conjugué  $\widehat{\Gamma}$  tel que  $\Gamma\widehat{\Gamma}$  soit rationnel.

7. *Diviseurs de zéro.* Un quaternion complexe  $A$ , différent de zéro, sera dit *un diviseur de zéro* si sa norme  $No(A)$  est nulle.

La norme de  $A$  s'écrit (formule 8)

$$No(A) = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2) (\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \\ \dots (\alpha_0^{(\tau)2} + \alpha_1^{(\tau)2} + \alpha_2^{(\tau)2} + \alpha_3^{(\tau)2}).$$

Si le corps  $K$  est réel,  $\alpha_0, \alpha_1, \alpha_2$  et  $\alpha_3$  sont réels ; les nombres  $\alpha_0^2, \alpha_1^2, \dots$  sont positifs et on ne peut avoir  $No(A) = 0$  que si l'on a

$$\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0.$$

Autrement dit, si  $No(A) = 0$ , on a aussi  $A = 0$ , et  $A$  n'est pas un diviseur de zéro.

*Il ne peut donc y avoir des diviseurs de zéro que si le corps primordial  $K$  est imaginaire.*

THÉORÈME. *Si  $A$  est un diviseur de zéro, dans le domaine numéral  $\Omega$ , il existe toujours deux quaternions complexes  $B \neq 0$  et  $\Gamma \neq 0$ , tels que l'on ait*

$$AB = 0 \quad \text{et} \\ \Gamma A = 0.$$

*Démonstration.* Formons le produit AB, on a (v. § 4)

$$AB = \pi_0 + \pi_1 i_1 + \pi_2 i_2 + \pi_3 i_3$$

où  $\pi_0, \pi_1, \pi_2$  et  $\pi_3$  ont les valeurs suivantes (v. formules 5) :

$$(10) \quad \left\{ \begin{array}{l} \pi_0 = \alpha_0 \beta_0 - \alpha_1 \beta_1 - \alpha_2 \beta_2 - \alpha_3 \beta_3 \\ \pi_1 = \alpha_1 \beta_0 + \alpha_0 \beta_1 - \alpha_3 \beta_2 + \alpha_2 \beta_3 \\ \pi_2 = \alpha_2 \beta_0 + \alpha_3 \beta_1 + \alpha_0 \beta_2 - \alpha_1 \beta_3 \\ \pi_3 = \alpha_3 \beta_0 - \alpha_2 \beta_1 + \alpha_1 \beta_2 + \alpha_0 \beta_3. \end{array} \right.$$

Si le produit AB est nul, on a  $\pi_0 = \pi_1 = \pi_2 = \pi_3 = 0$ , c'est-à-dire

$$(11) \quad \left\{ \begin{array}{l} \alpha_0 \beta_0 - \alpha_1 \beta_1 - \alpha_2 \beta_2 - \alpha_3 \beta_3 = 0 \\ \alpha_1 \beta_0 + \alpha_0 \beta_1 - \alpha_3 \beta_2 + \alpha_2 \beta_3 = 0 \\ \alpha_2 \beta_0 + \alpha_3 \beta_1 + \alpha_0 \beta_2 - \alpha_1 \beta_3 = 0 \\ \alpha_3 \beta_0 - \alpha_2 \beta_1 + \alpha_1 \beta_2 + \alpha_0 \beta_3 = 0. \end{array} \right.$$

Pour qu'il existe un quaternion  $B \equiv \beta_0 + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3 \neq 0$  et tel que  $AB = 0$ , il faut que le système (11) de quatre équations linéaires à quatre inconnues  $\beta_0, \beta_1, \beta_2$  et  $\beta_3$  admette une solution  $(\beta_0, \beta_1, \beta_2, \beta_3)$  non nulle ; et pour cela le déterminant  $\Delta$  des coefficients des inconnues  $\beta_\lambda$  doit être nul. En d'autres termes, on doit avoir

$$(12) \quad \Delta = \begin{vmatrix} \alpha_0 & -\alpha_1 & -\alpha_2 & -\alpha_3 \\ \alpha_1 & +\alpha_0 & -\alpha_3 & +\alpha_2 \\ \alpha_2 & +\alpha_3 & +\alpha_0 & -\alpha_1 \\ \alpha_3 & -\alpha_2 & +\alpha_1 & +\alpha_0 \end{vmatrix} = 0.$$

Or, le déterminant (12) a la valeur suivante :

$$(13) \quad \Delta = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)^2.$$

Comme, par hypothèse, A est un diviseur de zéro, sa norme est nulle, donc

$$(14) \quad \left\{ \begin{array}{l} No(A) = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2) (\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \dots \\ \dots (\alpha_0^{(r)2} + \alpha_1^{(r)2} + \alpha_2^{(r)2} + \alpha_3^{(r)2}) = 0. \end{array} \right.$$

L'un au moins des facteurs du second membre de  $No(A)$  doit être nul. Supposons que l'on ait  $\alpha_0^{(r)2} + \alpha_1^{(r)2} + \alpha_2^{(r)2} + \alpha_3^{(r)2} = 0$  et posons  $\theta \equiv \alpha_0^{(r)2} + \alpha_1^{(r)2} + \alpha_2^{(r)2} + \alpha_3^{(r)2}$ .

On peut écrire, puisque  $\theta$  fait partie du corps primordial  $K$  (voir 1<sup>re</sup> partie ch. I. 1),

$$\theta = a_0 + a_1 \sqrt{apqs} + a_2 \sqrt{bqrs} + \dots + a_7 \sqrt{abcs}.$$

Puisque  $\theta$  est nul, on a  $a_0 = a_1 = a_2 = \dots = a_7 = 0$  et, par suite, les autres facteurs de  $No(A)$ , facteurs qui sont les conjugués de  $\theta$  dans le corps  $K$ , sont nuls aussi.

Réciproquement, si l'un quelconque des facteurs du second membre de l'égalité (14) est nul, c'est que l'on a

$$a_0 = a_1 = \dots a_7 = 0. \quad \text{Par suite } \theta = 0 \text{ et tous}$$

les conjugués de  $\theta$  sont nuls.

*Conclusion.* Si la norme  $No(A) = 0$ , on a  $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$  et, par suite,  $\Delta = 0$ . Réciproquement, si  $\Delta = 0$ , on a  $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$  et, par suite,  $No(A) = 0$ .

Donc, si  $A$  est un diviseur de zéro, il existe un quaternion complexe  $B \neq 0$  tel que l'on ait  $AB = 0$ .

Si nous posons maintenant

$$\Gamma \equiv \gamma_0 + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3$$

et que nous formions le produit  $\Gamma A$ , on a

$$\Gamma A = \rho_0 + \rho_1 i_1 + \rho_2 i_2 + \rho_3 i_3, \quad \text{où l'on a posé (v. formules 6)}$$

$$(I) \quad \left\{ \begin{array}{l} \rho_0 = \alpha_0 \gamma_0 - \alpha_1 \gamma_1 - \alpha_2 \gamma_2 - \alpha_3 \gamma_3 \\ \rho_1 = \alpha_1 \gamma_0 + \alpha_0 \gamma_1 + \alpha_3 \gamma_2 - \alpha_2 \gamma_3 \\ \rho_2 = \alpha_2 \gamma_0 - \alpha_3 \gamma_1 + \alpha_0 \gamma_2 + \alpha_1 \gamma_3 \\ \rho_3 = \alpha_3 \gamma_0 + \alpha_2 \gamma_1 - \alpha_1 \gamma_2 + \alpha_0 \gamma_3 \end{array} \right.$$

Pour que  $\Gamma A = 0$ , il faut  $\rho_0 = \rho_1 = \rho_2 = \rho_3 = 0$ . Pour qu'il existe un quaternion  $\Gamma \neq 0$ , mais tel que l'on ait simultanément  $\rho_0 = \rho_1 = \rho_2 = \rho_3 = 0$ , il faut que soit nul le déterminant des coefficients  $\alpha_\lambda$ , dans les quatre équations linéaires à quatre inconnues obtenues en égalant à zéro chacune des quatre égalités (I) ci-dessus. Or, ce déterminant n'est autre que  $\Delta = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)^2$ . On voit, comme dans le cas du produit  $AB$ , que quand  $A$  est un diviseur de zéro, le quaternion  $\Gamma$  existe tel que  $\Gamma A = 0$ .

8. *Réciproque d'un quaternion complexe.* Désignons par  $A$  un quaternion complexe non nul du domaine numéral  $\Omega$ . Si  $A$  n'est pas diviseur de zéro, nous appellerons *réciproque* de  $A$  le quaternion  $\frac{1}{No(A)} \widehat{A}$ , et nous écrirons  $\frac{1}{No(A)} \widehat{A} \equiv A^{-1}$ . On voit que l'on a  $\Lambda A^{-1} = A^{-1} \Lambda = 1$ .

9. *Division des quaternions complexes.* Soit  $A$  un quaternion complexe non nul et qui ne soit pas diviseur de zéro. Si l'on a

$$\Lambda A = B,$$

$\Lambda$  est dit le *quotient à droite* du quaternion B par le quaternion A. On a

$$\Lambda = BA^{-1}.$$

Si, au contraire, on a la relation

$$A\Theta = B,$$

$\Theta$  est dit le *quotient à gauche* du quaternion B par le quaternion A et

$$\Theta = A^{-1}B.$$

On voit que les quotients à gauche et à droite sont en général différents.

10. *Permutations du domaine numéral*  $\Omega$ . Adjoignons au quaternion complexe A du domaine  $\Omega$ , d'après une règle quelconque, un quaternion  $f(A)$ ; la substitution

$$[A, f(A)],$$

résultat du remplacement de A par  $f(A)$ , s'appelle une *permutation* du domaine  $\Omega$  si, par l'emploi de cette substitution, toute égalité entre quaternions reste vérifiée et si, en outre, les quaternions  $f(A)$  ne sont pas tous nuls.

On voit immédiatement que l'on a le théorème suivant :

THÉORÈME. *Les huit permutations  $\varphi_0, \varphi_1, \dots, \varphi_7$  du corps primordial K (v. ch. I. 4, première partie) sont également des permutations du domaine numéral  $\Omega$ .*

11. Nous avons encore à introduire les définitions suivantes :

I. Etant donné le quaternion complexe

$$(16) \quad A \equiv \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3,$$

à coordonnées tirées du corps primordial K, nous appellerons *conjugué relatif* de A, et nous désignerons par  $\bar{A}$ , le quaternion complexe

$$(17) \quad \bar{A} \equiv \alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3.$$

II. Nous appellerons *norme relative* de A, et nous désignerons par  $n(A)$ , la quantité

$$(18) \quad n(A) \equiv A\bar{A} = \bar{A}A = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.$$

La norme relative d'un quaternion complexe est un nombre du corps primordial K. Nous la désignerons aussi par la lettre grecque minuscule correspondante comme suit :

$$n(A) \equiv \alpha, \quad n(B) \equiv \beta, \quad \text{etc....}$$

LE QUATERNION COMPLEXE ENTIER.

Un quaternion rationnel est dit entier \* quand il peut être mis sous la forme suivante :

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

où  $a_0, a_1, a_2$  et  $a_3$  sont des entiers ordinaires, et où l'on a posé

$$(21) \quad \rho \equiv \frac{1 + i_1 + i_2 + i_3}{2}.$$

Désignons par

$$\omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6, \omega_7$$

une base des entiers du corps primordial  $K$  (v. I<sup>re</sup> partie, chap. II). Tout quaternion complexe à coordonnées tirées du corps primordial  $K$  pourra dès lors se mettre sous la forme suivante :

$$(22) \quad A = A_0 \omega_0 + A_1 \omega_1 + A_2 \omega_2 + \dots + A_7 \omega_7$$

où les  $A_\lambda$  sont des quaternions rationnels.

*Définition.* Le quaternion complexe (22) sera dit un *quaternion complexe entier*, si les sept quaternions rationnels  $A_0, \dots, A_7$  sont des quaternions rationnels entiers.

Le quaternion complexe (22), supposé entier, peut s'écrire, en vertu de la définition précédente,

$$A = (a_0^{(0)} \rho + a_1^{(0)} i_1 + a_2^{(0)} i_2 + a_3^{(0)} i_3) \omega_0 + (a_0^{(1)} \rho + a_1^{(1)} i_1 + a_2^{(1)} i_2 + a_3^{(1)} i_3) \omega_1 + \dots \\ \dots + (a_0^{(7)} \rho + a_1^{(7)} i_1 + a_2^{(7)} i_2 + a_3^{(7)} i_3) \omega_7,$$

ce qui peut s'écrire

$$(23) \quad A = \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \quad \text{où l'on a posé}$$

$$(24) \quad \begin{cases} \alpha_0 \equiv a_0^{(0)} \omega_0 + a_0^{(1)} \omega_1 + \dots + a_0^{(7)} \omega_7 \\ \alpha_1 \equiv a_1^{(0)} \omega_0 + a_1^{(1)} \omega_1 + \dots + a_1^{(7)} \omega_7 \\ \alpha_2 \equiv a_2^{(0)} \omega_0 + a_2^{(1)} \omega_1 + \dots + a_2^{(7)} \omega_7 \\ \alpha_3 \equiv a_3^{(0)} \omega_0 + a_3^{(1)} \omega_1 + \dots + a_3^{(7)} \omega_7. \end{cases}$$

On voit que les quatre nombres  $\alpha_0, \alpha_1, \alpha_2$  et  $\alpha_3$  sont des entiers dans le corps primordial  $K$ .

Soit  $A$  le quaternion (22) et désignons, comme plus haut, par  $\bar{A}$  le conjugué relatif de  $A$ . On vérifie que l'on a

$$(25) \quad \bar{A} = \alpha_0 \rho - (\alpha_0 + \alpha_1) i_1 - (\alpha_0 + \alpha_2) i_2 - (\alpha_0 + \alpha_3) i_3.$$

On a, pour la norme relative de  $A$ ,

$$(26) \quad n(A) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_0 (\alpha_1 + \alpha_2 + \alpha_3).$$

\* Voir A. Hurwitz, *Zahlentheorie der Quaternionen*.

## CHAPITRE II

### Les idéaux dans le domaine numéral $\Omega$ .

12. Soit  $\mathfrak{a}$  un idéal du corps primordial  $K (\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps})$ . Nous appellerons *idéal du domaine numéral  $\Omega$* , et nous représenterons par  $\mathfrak{A} \equiv \text{id } |\mathfrak{a}|$ , l'ensemble infini de quaternions complexes entiers

$$(27) \quad A = \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$$

dont les quatre coordonnées  $\alpha_0, \alpha_1, \alpha_2$  et  $\alpha_3$  parcourent, indépendamment les unes des autres, tous les nombres de l'idéal  $\mathfrak{a}$ . \*

Dans l'expression (27),  $\rho$  est égal à

$$\frac{1 + i_1 + i_2 + i_3}{2}.$$

13. L'idéal  $\mathfrak{A} \equiv \text{id } |\mathfrak{a}|$  du domaine numéral  $\Omega$  sera dit un *idéal principal*, si  $\mathfrak{a}$  est un idéal principal ( $\alpha$ ) dans le corps primordial  $K$ . Nous écrirons, dans ce cas,

$$(28) \quad \mathfrak{A} \equiv \text{id } |(\alpha)|.$$

Il résulte de la définition de l'idéal principal dans le domaine numéral  $\Omega$ , que tous les quaternions de l'idéal (28) sont de la forme

$$A = \alpha (\xi_0 \rho + \xi_1 i_1 + \xi_2 i_2 + \xi_3 i_3)$$

où  $\xi_0, \xi_1, \xi_2$  et  $\xi_3$  sont des nombres entiers du corps primordial  $K$ .

*Exemple :*  $\mathfrak{A} \equiv \text{id } |(2)|$  contient tous les quaternions entiers dont les quatre coordonnées sont des multiples de 2 dans le corps primordial  $K$ . En d'autres termes,  $\xi_\lambda$  ( $\lambda = 0, 1, 2, 3$ ) désignant des nombres entiers quelconques du corps primordial  $K$ , tous les quaternions de l'idéal  $\mathfrak{A} \equiv \text{id } |(2)|$  du domaine numéral  $\Omega$  ont la forme

$$2 \xi_0 \rho + 2 \xi_1 i_1 + 2 \xi_2 i_2 + 2 \xi_3 i_3 \quad \text{ou} \quad 2 (\xi_0 \rho + \xi_1 i_1 + \xi_2 i_2 + \xi_3 i_3).$$

\* Voir Boris Seitz : *Sur l'arithmomie des nombres de Weierstrass généralisés et de quelques systèmes de polytettarions complexes*. Thèse, page 20, définition de « l'idéal diagonal ».

Il suit de là que tous les quaternions de l'idéal  $\mathfrak{A} \equiv \text{id } \{(\alpha)\}$  sont, dans le domaine numéral  $\Omega$ , des multiples de  $\alpha$ . Nous écrirons aussi l'idéal  $\mathfrak{A}$  dans ce cas

$$(28) \quad \mathfrak{A} = (\alpha).$$

Remarquons qu'un quaternion complexe entier quelconque  $A = \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$  détermine toujours un idéal du domaine numéral  $\Omega$ , savoir :

$$(29) \quad \mathfrak{A} \equiv \text{id } \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3)\}.$$

C'est l'ensemble de tous les quaternions dont les quatre coordonnées font partie de l'idéal  $\mathfrak{a} \equiv (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$  du corps  $K$ . Si trois des coordonnées de  $A$  sont nulles, par exemple  $\alpha_0, \alpha_2$  et  $\alpha_3$ , le quaternion  $A$  devient  $A = \alpha_1 i_1$  et l'idéal  $\mathfrak{A}$  s'écrit  $\mathfrak{A} \equiv \text{id } \{(\alpha_1)\}$  ou  $\mathfrak{A} \equiv (\alpha_1)$ . Dans la suite de ce travail, nous représenterons par  $(A)$  l'idéal (29) déterminé par le quaternion  $A$ . \*

14. *Définition.* Quand un quaternion  $A$  fait partie de l'idéal  $\mathfrak{A}$ , nous dirons que  $A$  est congru à zéro modulo  $\mathfrak{A}$  et nous écrirons

$$A \equiv 0 \text{ mod } \mathfrak{A}. **$$

15. *Produit de deux idéaux de quaternions complexes.* Soient  $\mathfrak{A}$  et  $\mathfrak{B}$  deux idéaux du domaine numéral  $\Omega$  et posons

$$\mathfrak{A} \equiv \text{id } \{a\} \quad \text{et} \quad \mathfrak{B} \equiv \text{id } \{b\}.$$

Nous appellerons *produit* de ces deux idéaux l'idéal

$$\mathfrak{C} \equiv \text{id } \{c\}$$

comprenant tous les quaternions, et ceux-là seulement, dont les quatre coordonnées appartiennent à l'idéal  $c \equiv a b$ , du corps  $K$ . On voit que la multiplication des idéaux, ainsi définie dans le domaine numéral  $\Omega$ , est *commutative* et *associative*.

\* Soit un quaternion rationnel entier  $A \equiv a_0 \rho + a_1 i_1 + a_2 i_2 + a_3 i_3$ . Considéré comme un quaternion du domaine  $\Omega$ ,  $A$  détermine un idéal  $\mathfrak{A} \equiv \text{id } \{a_0, a_1, a_2, a_3\}$ . L'idéal  $(a_0, a_1, a_2, a_3)$  du corps primordial  $K$  est, dans ce corps, un idéal principal  $(d)$  où  $d$  est le *pgcd* des nombres  $a_0, a_1, a_2$  et  $a_3$  pris dans leur ensemble.

\*\* Dans la théorie classique des idéaux, si un nombre  $\alpha$  fait partie d'un idéal  $\mathfrak{a}$ , on écrit

$$\alpha \equiv 0 \text{ mod } \mathfrak{a}.$$

En écrivant

$$A \equiv 0 \text{ mod } \mathfrak{A},$$

nous généralisons la définition admise dans la théorie classique des idéaux.

16. *Divisibilité.* L'idéal  $\mathfrak{A} \equiv \text{id } \{a\}$  sera dit *divisible par l'idéal*  $\mathfrak{B} \equiv \text{id } \{b\}$  s'il existe un idéal  $\mathfrak{C} \equiv \text{id } \{c\}$  tel que l'on ait

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

On a alors, dans le corps primordial  $K$ ,

$$a = cb.$$

PROPRIÉTÉS DES IDÉAUX.

17. THÉORÈME. *La somme et la différence de deux nombres A et B de l'idéal  $\mathfrak{A} \equiv \text{id } \{a\}$  font partie de cet idéal  $\mathfrak{A}$ .*

En effet, posons

$$A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \quad B \equiv \beta_0 \rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3.$$

Puisque, par hypothèse, A et B sont tous deux contenus dans  $\mathfrak{A}$ , on a

$$(30) \quad \alpha_r \equiv 0 \pmod{a} \quad \text{et} \quad \beta_r \equiv 0 \pmod{a} \quad \text{pour} \quad r = 0, 1, 2, 3.$$

Or, on a

$$A \pm B = (\alpha_0 \pm \beta_0) \rho + (\alpha_1 \pm \beta_1) i_1 + (\alpha_2 \pm \beta_2) i_2 + (\alpha_3 \pm \beta_3) i_3$$

et l'on sait, par la théorie des idéaux de corps algébriques, que les congruences (30) entraînent

$$\alpha_r \pm \beta_r \equiv 0 \pmod{a}; \quad \text{par suite}$$

$$A \pm B \equiv 0 \pmod{\mathfrak{A}}. \quad \text{c. q. f. d.}$$

18. THÉORÈME. *Si un quaternion complexe entier  $A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$  du domaine  $\Omega$  fait partie de l'idéal  $\mathfrak{A}$ , les produits à droite, AB, et les produits à gauche, BA, de A par un quaternion entier quelconque B de  $\Omega$ , sont également contenus dans l'idéal  $\mathfrak{A}$ .*

En effet,  $A \equiv 0 \pmod{\mathfrak{A}}$  entraîne  $\alpha_r \equiv 0 \pmod{a}$ , pour  $r = 0, 1, 2, 3$ . Or, les coordonnées des produits AB et BA sont des combinaisons linéaires, à coefficients entiers, des coordonnées  $\alpha_0, \alpha_1, \alpha_2$  et  $\alpha_3$  avec les coordonnées de B (v. § 4, ch. I). Ces combinaisons linéaires sont donc des nombres de a et par suite AB et BA font partie de l'idéal  $\mathfrak{A}$ .

19. THÉORÈME. *Soit  $\mathfrak{A} \equiv \text{id } \{a\}$  un idéal du domaine  $\Omega$ . Si cet idéal contient le quaternion entier A, il contient aussi le conjugué relatif  $\bar{A}$  et la norme relative  $n(A)$  de A.*

*Démonstration.* Soit  $A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$  un nombre de l'idéal  $\mathfrak{A}$ ; on a dès lors

$$\begin{aligned} A &\equiv 0 \pmod{\mathfrak{A}} && \text{et on en déduit} \\ \alpha_r &\equiv 0 \pmod{a}, && \text{pour } r = 0, 1, 2, 3. \end{aligned}$$

L'idéal  $\mathfrak{a}$  contient aussi les nombres

$$\alpha_0; \quad -(\alpha_0 + \alpha_1); \quad -(\alpha_0 + \alpha_2); \quad -(\alpha_0 + \alpha_3),$$

qui sont précisément les coordonnées de  $\bar{A}$  (v. § 11). Ce dernier quaternion fait donc partie de l'idéal  $\mathfrak{A}$ ; en vertu de la définition de la norme relative (§ 11) et du théorème 18,  $n(A) = A\bar{A}$  fait également partie de l'idéal  $\mathfrak{A}$ .

20. THÉORÈME. *Tout idéal du domaine  $\Omega$  admet une BASE, c'est-à-dire que l'on peut toujours trouver dans l'idéal huit nombres  $\Gamma_1, \Gamma_2, \dots, \Gamma_8$  tels que tout autre nombre de l'idéal considéré puisse se mettre sous la forme*

$$X_1\Gamma_1 + X_2\Gamma_2 + \dots + X_8\Gamma_8,$$

où les  $X_r$  désignent des quaternions rationnels entiers. En outre si  $\mathfrak{A} \equiv \text{id } \mathfrak{a}$ , et si l'on désigne par  $\gamma_1, \gamma_2, \dots, \gamma_8$  une base de l'idéal  $\mathfrak{a}$  du corps  $K$ , on pourra poser

$$\Gamma_1 \equiv \gamma_1; \quad \Gamma_2 \equiv \gamma_2; \quad \dots; \quad \Gamma_8 \equiv \gamma_8.$$

*Démonstration.* Soit de nouveau

$$A \equiv \alpha_0\rho + \alpha_1i_1 + \alpha_2i_2 + \alpha_3i_3$$

un nombre de l'idéal  $\mathfrak{A} \equiv \text{id } \mathfrak{a}$ ; on peut donc écrire, en vertu des hypothèses faites,

$$\alpha_r = x_1^{(r)}\gamma_1 + x_2^{(r)}\gamma_2 + \dots + x_8^{(r)}\gamma_8 \quad \text{pour } r = 0, 1, 2, 3,$$

les  $x_\lambda^{(k)}$  étant des nombres entiers ordinaires. Dès lors, on a

$$A = (x_1^{(0)}\gamma_1 + \dots + x_8^{(0)}\gamma_8)\rho + (x_1^{(1)}\gamma_1 + \dots + x_8^{(1)}\gamma_8)i_1 + \dots + (x_1^{(3)}\gamma_1 + x_2^{(3)}\gamma_2 + \dots + x_8^{(3)}\gamma_8)i_3,$$

ou encore

$$(31) \quad A = (x_1^{(0)}\rho + x_1^{(1)}i_1 + x_1^{(2)}i_2 + x_1^{(3)}i_3)\gamma_1 + \dots + (x_8^{(0)}\rho + x_8^{(1)}i_1 + x_8^{(2)}i_2 + x_8^{(3)}i_3)\gamma_8.$$

Tout nombre de l'idéal  $\mathfrak{A}$  peut donc se mettre sous la forme (31) et, d'autre part, tout nombre de la forme (31) fait partie de l'idéal  $\mathfrak{A}$ .

Les quaternions qui figurent dans les parenthèses au second membre de l'égalité (31) sont des quaternions à coordonnées  $x_\lambda^{(k)}$  rationnelles entières; par suite le théorème est démontré.

21. THÉORÈME. *Si  $\mathfrak{A} \equiv \text{id } \mathfrak{a}$  est divisible par  $\mathfrak{B} \equiv \text{id } \mathfrak{b}$ , tout quaternion  $A$  de  $\mathfrak{A}$  fait partie de  $\mathfrak{B}$ .*

Comme dans la démonstration du théorème (19) on a, dans le corps  $K$ , les congruences suivantes :

$$\alpha_r \equiv 0 \pmod{\mathfrak{a}} \quad \text{pour } r = 0, 1, 2, 3.$$

D'autre part,  $\mathfrak{A}$  étant divisible par  $\mathfrak{B}$  on a, dans le corps  $K$ ,

$$a \equiv 0 \pmod{b}.$$

Dès lors, tout nombre de  $a$  fait partie de  $b$ . On en conclut que  $\alpha_r \equiv 0 \pmod{b}$  et, par suite, que  $A \equiv 0 \pmod{\mathfrak{B}}$ , ce qui démontre le théorème.

22. THÉORÈME. *Etant donné un idéal  $\mathfrak{A}$  du domaine  $\Omega$ , il existe dans  $\Omega$  un idéal  $\mathfrak{B}$  tel que le produit  $\mathfrak{A}\mathfrak{B}$  soit un idéal principal.*

Pour le démontrer, posons

$$\mathfrak{A} \equiv \text{id } |a|.$$

On sait trouver dans le corps  $K$  un idéal  $a^{-1}$  tel que  $aa^{-1} = (a)$ .

Posons donc  $\mathfrak{B} \equiv \text{id } |a^{-1}|$ , et l'on aura  $\mathfrak{A}\mathfrak{B} = \text{id } |(a)|$ .

Nous écrirons par analogie

$$\mathfrak{A}^{-1} \equiv \text{id } |a^{-1}|$$

et l'idéal  $\mathfrak{A}^{-1}$  sera dit *le réciproque* de l'idéal  $\mathfrak{A}$ .

23. THÉORÈME. *Un quaternion complexe entier  $\Gamma \equiv \gamma_0\rho + \gamma_1i_1 + \gamma_2i_2 + \gamma_3i_3$  ne peut être contenu que dans un nombre fini d'idéaux du domaine numéral  $\Omega$ .*

Supposons que l'idéal  $\mathfrak{A} \equiv \text{id } |a|$  contienne la norme relative de  $\Gamma$ , soit  $n(\Gamma) = \gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_0(\gamma_1 + \gamma_2 + \gamma_3)$ . On sait\* que ce nombre  $n(\Gamma)$  n'est contenu que dans un nombre fini d'idéaux du corps primordial  $K$ . Or, tout idéal contenant  $\Gamma$  contient aussi  $n(\Gamma)$  (v. th. 19); le nombre des idéaux du domaine  $\Omega$  contenant  $\Gamma$  est dès lors au plus égal à celui des idéaux du corps  $K$  contenant  $n(\Gamma)$ ; ce nombre est donc limité.

#### LA DÉCOMPOSITION MULTIPLICATIVE DES IDÉAUX DE QUATERNIONS COMPLEXES.

24. THÉORÈME. *Un idéal du domaine numéral  $\Omega$  n'est divisible que par un nombre fini d'idéaux du même domaine.*

En effet, soit  $\mathfrak{A} \equiv \text{id } |a|$  un idéal du domaine  $\Omega$  et  $\mathfrak{B} \equiv \text{id } |b|$  un diviseur de  $\mathfrak{A}$ . Désignons par  $A$  un nombre de  $\mathfrak{A}$ ; d'après le théorème (21) on a  $A \equiv 0 \pmod{\mathfrak{B}}$ . Or,  $A$  ne pouvant être contenu que dans un nombre fini d'idéaux, le nombre des diviseurs  $\mathfrak{B}$  de  $\mathfrak{A}$  est limité.

25. THÉORÈME. *Soient  $\mathfrak{A}$ ,  $\mathfrak{B}$  et  $\mathfrak{C}$  trois idéaux du domaine numéral  $\Omega$ ; l'égalité*

$$\mathfrak{A}\mathfrak{B} = \mathfrak{A}\mathfrak{C} \text{ entraîne } \mathfrak{B} = \mathfrak{C}.$$

\* Voir D. Hilbert, op. cit., chap. II.

On le voit en multipliant à gauche par  $\mathfrak{A}^{-1}$ , ce qui donne

$$\mathfrak{A}^{-1}\mathfrak{A}\mathfrak{B} = \mathfrak{A}^{-1}\mathfrak{A}\mathfrak{C},$$

puis en posant

$$\mathfrak{A}^{-1}\mathfrak{A} \equiv \text{id} \mid (\alpha) \mid = (\alpha).$$

On déduit de là

$$(\alpha)\mathfrak{B} = (\alpha)\mathfrak{C}.$$

Les définitions des § 12 et 13 permettent de passer aux coordonnées, c'est-à-dire de ne plus opérer que sur des idéaux du corps algébrique  $K$ , et l'on sait \* que, dans ce domaine,  $a\mathfrak{b} = a\mathfrak{c}$  entraîne  $\mathfrak{b} = \mathfrak{c}$ .

26. THÉORÈME. Si tous les nombres d'un idéal  $\mathfrak{A} \equiv \text{id} \mid a \mid$  sont congrus à zéro modulo un idéal  $\mathfrak{B} \equiv \text{id} \mid b \mid$ , l'idéal  $\mathfrak{A}$  est divisible par l'idéal  $\mathfrak{B}$ .

Soit de nouveau

$$A \equiv \alpha_0\rho + \alpha_1i_1 + \alpha_2i_2 + \alpha_3i_3$$

un quaternion de l'idéal  $\mathfrak{A}$ , quaternion arbitrairement choisi mais fixe. De l'hypothèse, combinée avec les définitions précédentes, on conclut

$$\alpha_r \equiv 0 \pmod{b}, \quad \text{pour } r = 0, 1, 2, 3.$$

On en déduit

$$\begin{aligned} a &\equiv 0 \pmod{b} && \text{et, par suite,} \\ \mathfrak{A} &\equiv 0 \pmod{\mathfrak{B}}. \end{aligned}$$

27. Soient  $\mathfrak{A}$  et  $\mathfrak{B}$  deux idéaux du domaine numéral  $\Omega$ . Désignons par  $\mathfrak{D}$  un idéal contenant tous les nombres de  $\mathfrak{A}$ , tous ceux de  $\mathfrak{B}$  ainsi que toutes les combinaisons linéaires de ces nombres faites à l'aide de quaternions complexes entiers de  $\Omega$ . Il résulte du théorème 26 que les idéaux  $\mathfrak{A}$  et  $\mathfrak{B}$  sont tous deux divisibles par l'idéal  $\mathfrak{D}$ .

Considérons d'autre part un idéal du domaine  $\Omega$  qui, en plus des nombres de  $\mathfrak{A}$ , de ceux de  $\mathfrak{B}$  et de leurs combinaisons linéaires, contienne encore d'autres nombres. Ce nouvel idéal est un diviseur de  $\mathfrak{D}$ . Dès lors, par analogie avec l'arithmétique ordinaire, nous posons la définition suivante :

*Définition.* L'idéal  $\mathfrak{D}$  est le plus grand commun diviseur des idéaux  $\mathfrak{A}$  et  $\mathfrak{B}$  ; nous le désignerons par la notation  $(\mathfrak{A}/\mathfrak{B})$ .

28. Si  $\mathfrak{D} \equiv \text{id} \mid d \mid$  est le plus grand commun diviseur des deux idéaux  $\mathfrak{A} \equiv \text{id} \mid a \mid$  et  $\mathfrak{B} \equiv \text{id} \mid b \mid$ , l'idéal  $\mathfrak{d}$  est, dans le corps  $K$ , le plus grand commun diviseur des idéaux  $a$  et  $b$ . En effet, dans le domaine  $\Omega$ ,  $\mathfrak{D}$  contient tous les nombres de  $\mathfrak{A}$  et tous ceux de  $\mathfrak{B}$ , on en conclut que, dans le corps primordial  $K$ , l'idéal  $\mathfrak{d}$  contient tous les nombres de  $a$  et tous ceux de  $b$ .

\* Voir D. Hilbert, op. cit., chap. II.

29. *Définitions.* I. L'idéal unité dans le domaine  $\Omega$  des quaternions complexes est l'idéal  $U \equiv \text{id } \{1\} \equiv (1)$ . Cet idéal contient le nombre 1 et, par suite, tous les quaternions entiers de  $\Omega$ .

II. Un idéal  $\mathfrak{P} \equiv \text{id } \{p\}$  de  $\Omega$  est dit un « idéal premier » si, dans toutes les décompositions possibles de  $\mathfrak{P}$  en un produit de deux facteurs idéaux, l'un d'eux est toujours l'idéal unité. Il résulte des définitions posées que l'idéal  $p$  est premier dans le corps primordial  $K$ .

30. THÉORÈME. *Si le produit  $\mathfrak{A}\mathfrak{B}$  de deux idéaux du domaine  $\Omega$  est divisible par un idéal premier  $\mathfrak{P}$ , l'un au moins des facteurs est divisible par  $\mathfrak{P}$ .*

*Démonstration.* Prenons

$$\mathfrak{A} \equiv \text{id } \{a\}; \quad \mathfrak{B} \equiv \text{id } \{b\}; \quad \mathfrak{P} \equiv \text{id } \{p\}.$$

Dans le corps  $K$ ,  $p$  est un idéal premier. Il ressort des définitions posées que si  $\mathfrak{A}\mathfrak{B}$ , dans le domaine  $\Omega$ , est divisible par  $\mathfrak{P}$ ,  $ab$  doit être divisible par  $p$  dans le corps  $K$ ; et l'on sait par la théorie classique des corps algébriques que, dans ce cas,  $a$  ou  $b$  est divisible par  $p$ . On a donc l'une des trois alternatives suivantes :

$$\begin{array}{lll} a \equiv 0 \pmod{p}, & \text{ce qui entraîne} & \mathfrak{A} \equiv 0 \pmod{\mathfrak{P}}; \\ b \equiv 0 \pmod{p}, & \text{ce qui entraîne} & \mathfrak{B} \equiv 0 \pmod{\mathfrak{P}}; \\ a \equiv 0 \pmod{p} \text{ et } b \equiv 0 \pmod{p}, & \text{ce qui entraîne} & \mathfrak{A} \equiv 0 \pmod{\mathfrak{P}} \text{ et } \mathfrak{B} \equiv 0 \pmod{\mathfrak{P}}. \end{array}$$

31. THÉORÈME FONDAMENTAL. *Tout idéal  $\mathfrak{A}$  du domaine numéral  $\Omega$  peut être décomposé, et cela d'une seule manière, en un produit d'un nombre fini d'idéaux premiers du domaine  $\Omega$ .*

*Démonstration.* Tout d'abord, dans une décomposition multiplicative de l'idéal  $\mathfrak{A}$ , le nombre des facteurs est limité, en vertu du théorème 24. Supposons que l'on ait obtenu les deux décompositions suivantes en produits d'idéaux tous premiers :

$$\begin{aligned} \mathfrak{A} &= \mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_r; \\ \mathfrak{A} &= \mathfrak{Q}_1 \mathfrak{Q}_2 \dots \mathfrak{Q}_s. \end{aligned}$$

L'idéal  $\mathfrak{A}$  est donc divisible par l'idéal premier  $\mathfrak{Q}_1$ ; en vertu du théorème 30, l'un des idéaux  $\mathfrak{P}_k$ , par exemple  $\mathfrak{P}_1$ , sera divisible par  $\mathfrak{Q}_1$ . Mais  $\mathfrak{P}_1$  étant un idéal premier, on doit avoir  $\mathfrak{P}_1 = \mathfrak{Q}_1$ ; il reste alors

$$\mathfrak{P}_2 \mathfrak{P}_3 \dots \mathfrak{P}_r = \mathfrak{Q}_2 \mathfrak{Q}_3 \dots \mathfrak{Q}_s.$$

En répétant le raisonnement ci-dessus, on voit que chacun des idéaux  $\mathfrak{Q}_r$  se trouve parmi les idéaux  $\mathfrak{P}_k$  et vice-versa.

Le théorème est donc démontré.

### CHAPITRE III

#### Les congruences suivant un idéal du domaine numéral $\Omega$ .

32. Des définitions posées plus haut, il résulte que

1. tout entier du domaine  $\Omega$  est congru à lui-même suivant un idéal quelconque, puisque tout idéal contient le nombre zéro ;
2. la congruence  $A \equiv B \pmod{\mathfrak{A}}$  entraîne  $B \equiv A \pmod{\mathfrak{A}}$  ;
3. deux entiers congrus à un même troisième mod  $\mathfrak{A}$  sont congrus entre eux mod  $\mathfrak{A}$ .

Ces trois propriétés permettent de répartir tous les quaternions complexes entiers du domaine  $\Omega$  en classes modulo  $\mathfrak{A}$ , en mettant dans une même classe tous les nombres congrus à un même idéal et, par suite, congrus entre eux. De cette façon, tout entier du domaine  $\Omega$  se trouve faire partie d'une classe et d'une seule, suivant le module  $\mathfrak{A}$  ; on peut prendre, pour représenter une classe, un nombre quelconque de cette classe. Si l'on choisit un seul nombre dans chaque classe, on obtient un système complet de restes suivant le module  $\mathfrak{A}$ .

*Définition.* Le nombre des quaternions d'un système complet de restes modulo  $\mathfrak{A}$  est dit la *norme* de l'idéal  $\mathfrak{A}$ . On la représente par  $N_0(\mathfrak{A})$ .

33. THÉORÈME. Pour que deux quaternions complexes entiers du domaine numéral  $\Omega$ , par exemple

$$A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \quad \text{et} \quad B \equiv \beta_0 \rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3,$$

soient congrus suivant un idéal  $\mathfrak{A} \equiv id \mid a \mid$ , il faut et il suffit que l'on ait, dans le corps primordial  $K$ , les congruences suivantes :

$$\alpha_\lambda \equiv \beta_\lambda \pmod{a} \quad \text{pour} \quad \lambda = 0, 1, 2, 3.$$

*Démonstration.* 1) La condition est nécessaire, car pour que l'on ait  $A \equiv B \pmod{\mathfrak{A}}$ , il faut que  $A - B \equiv 0 \pmod{\mathfrak{A}}$ .

Or,  $A - B = (\alpha_0 - \beta_0) \rho + (\alpha_1 - \beta_1) i_1 + (\alpha_2 - \beta_2) i_2 + (\alpha_3 - \beta_3) i_3$ .

Il faut donc que l'on ait

$$\alpha_r \equiv \beta_r \pmod{a} \quad \text{pour } r = 0, 1, 2, 3.$$

2) La condition est suffisante car, si  $\alpha_r \equiv \beta_r \pmod{a}$  pour  $r = 0, 1, 2, 3$ , l'idéal  $a$  contient  $\alpha_r - \beta_r$  pour  $r = 0, 1, 2, 3$ , et on a

$$(\alpha_0 - \beta_0) \rho + (\alpha_1 - \beta_1) i_1 + (\alpha_2 - \beta_2) i_2 + (\alpha_3 - \beta_3) i_3 \equiv 0 \pmod{\mathfrak{A}}.$$

Or, le premier membre n'est autre que  $A - B$ , et le théorème est démontré.

34. THÉORÈME. Soit donné, dans le domaine  $\Omega$ , un idéal  $\mathfrak{A} \equiv \text{id } |a|$ ; désignons par  $n_k(a)$  la norme de l'idéal  $a$  dans le corps  $K$ , c'est-à-dire le nombre des éléments d'un système complet de restes modulo  $a$  dans le corps  $K$ ; je dis qu'un système complet de restes modulo  $\mathfrak{A}$ , dans le domaine  $\Omega$ , comprend  $[n_k(a)]^4$  nombres. C'est la norme  $No(\mathfrak{A})$  de l'idéal de quaternions complexes  $\mathfrak{A}$ , et nous écrirons  $No(\mathfrak{A}) = [n_k(a)]^4$ .

Démonstration. Soit  $A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$  un quaternion complexe entier du domaine  $\Omega$ ; faisons parcourir aux coordonnées  $\alpha_r$ , indépendamment les unes des autres, les  $n_k(a)$  nombres d'un système complet de restes modulo  $a$ . On obtient ainsi  $[n_k(a)]^4$  quaternions. On voit tout de suite qu'ils sont incongrus entre eux mod  $\mathfrak{A}$  où  $\mathfrak{A} \equiv \text{id } |a|$  et, de plus, que tout autre quaternion entier de  $\Omega$  est congru, modulo  $\mathfrak{A}$ , à l'un de ces  $[n_k(a)]^4$  quaternions.

35. THÉORÈME. Soit  $n(p) = p^e$  la norme de l'idéal premier  $\mathfrak{p}$  dans le corps  $K$ ; on a, dans le domaine  $\Omega$ ,  $No(\mathfrak{p}) = p^{4e}$ .

Cela résulte du théorème 34.

36. THÉORÈME. Si  $A \equiv B \pmod{\mathfrak{A}}$  et  $\Gamma \equiv \Delta \pmod{\mathfrak{A}}$ , on a aussi

$$(32) \quad A \pm \Gamma \equiv B \pm \Delta \pmod{\mathfrak{A}}.$$

Pour le démontrer, posons

$$\begin{aligned} \mathfrak{A} \equiv \text{id } |a|, \quad A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \quad B \equiv \beta_0 \rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3, \\ \Gamma \equiv \gamma_0 \rho + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3, \quad \Delta \equiv \delta_0 \rho + \delta_1 i_1 + \delta_2 i_2 + \delta_3 i_3. \end{aligned}$$

De  $A \equiv B \pmod{\mathfrak{A}}$ , on déduit

$$(33) \quad \alpha_r \equiv \beta_r \pmod{a}, \quad \text{pour } r = 0, 1, 2, 3.$$

De  $\Gamma \equiv \Delta \pmod{\mathfrak{A}}$ , on déduit

$$(34) \quad \gamma_r \equiv \delta_r \pmod{a}, \quad \text{pour } r = 0, 1, 2, 3.$$

Les congruences (33) et (34) donnent, en vertu des propriétés connues des congruences dans les corps algébriques,

$$\alpha_r \pm \gamma_r \equiv \beta_r \pm \delta_r \pmod{\mathfrak{a}},$$

d'où résultent les congruences (32).

37. THÉORÈME. *Il est permis de multiplier à droite et à gauche, par un quaternion entier quelconque du domaine  $\Omega$ , les deux membres d'une congruence suivant un idéal de  $\Omega$ .*

Car, si  $A \equiv B \pmod{\mathfrak{A}}$ , on a  $A - B \equiv 0 \pmod{\mathfrak{A}}$  et, en vertu du théorème 18, les quaternions

$M(A - B)$  et  $(A - B)M$ , où  $M$  représente un quaternion entier de  $\Omega$ , sont congrus à zéro modulo  $\mathfrak{A}$ , quel que soit l'entier  $M$ . Il en résulte bien

$$MA \equiv MB \text{ et } AM \equiv BM \pmod{\mathfrak{A}}.$$

38. THÉORÈME. *Il est permis de multiplier membre à membre, à droite et à gauche, un nombre fini quelconque de congruences suivant un même idéal du domaine  $\Omega$ .*

Soient les deux congruences

$$(35) \quad A \equiv B \pmod{\mathfrak{A}} \text{ et } \Gamma \equiv \Delta \pmod{\mathfrak{A}}.$$

Ecrivons explicitement les quaternions qui figurent dans les congruences (35) :

$$\begin{aligned} A &\equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 = \frac{1}{2} \left[ \alpha_0 + (\alpha_0 + 2\alpha_1) i_1 + (\alpha_0 + 2\alpha_2) i_2 + (\alpha_0 + 2\alpha_3) i_3 \right]; \\ B &\equiv \beta_0 \rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3 = \frac{1}{2} \left[ \beta_0 + (\beta_0 + 2\beta_1) i_1 + (\beta_0 + 2\beta_2) i_2 + (\beta_0 + 2\beta_3) i_3 \right]; \\ \Gamma &\equiv \gamma_0 \rho + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3 = \frac{1}{2} \left[ \gamma_0 + (\gamma_0 + 2\gamma_1) i_1 + (\gamma_0 + 2\gamma_2) i_2 + (\gamma_0 + 2\gamma_3) i_3 \right]; \\ \Delta &\equiv \delta_0 \rho + \delta_1 i_1 + \delta_2 i_2 + \delta_3 i_3 = \frac{1}{2} \left[ \delta_0 + (\delta_0 + 2\delta_1) i_1 + (\delta_0 + 2\delta_2) i_2 + (\delta_0 + 2\delta_3) i_3 \right]. \end{aligned}$$

Effectuons les produits  $A\Gamma$  et  $B\Delta$  en appliquant les formules (5). On obtient, tous calculs faits,

$$\begin{aligned} A\Gamma &= (\alpha_0 \gamma_0 - \alpha_0 \gamma_1 - \alpha_0 \gamma_2 - \alpha_0 \gamma_3 - \alpha_1 \gamma_0 - 2\alpha_1 \gamma_1 - \alpha_2 \gamma_0 - 2\alpha_2 \gamma_2 - \alpha_3 \gamma_0 - 2\alpha_3 \gamma_3) \rho \\ &\quad + (\alpha_0 \gamma_0 + \alpha_0 \gamma_1 + \alpha_0 \gamma_3 + \alpha_1 \gamma_0 + \alpha_1 \gamma_1 + \alpha_2 \gamma_0 + \alpha_2 \gamma_2 + \alpha_2 \gamma_3 - \alpha_3 \gamma_2 + \alpha_3 \gamma_3) i_1 \\ &\quad + (\alpha_0 \gamma_0 + \alpha_0 \gamma_1 + \alpha_0 \gamma_2 + \alpha_1 \gamma_1 - \alpha_1 \gamma_3 + \alpha_2 \gamma_0 + \alpha_2 \gamma_2 + \alpha_3 \gamma_0 + \alpha_3 \gamma_1 + \alpha_3 \gamma_3) i_2 \\ &\quad + (\alpha_0 \gamma_0 + \alpha_0 \gamma_2 + \alpha_0 \gamma_3 + \alpha_1 \gamma_0 + \alpha_1 \gamma_1 + \alpha_1 \gamma_2 - \alpha_2 \gamma_1 + \alpha_2 \gamma_2 + \alpha_3 \gamma_0 + \alpha_3 \gamma_3) i_3 \end{aligned}$$

et de même

$$\begin{aligned} B\Delta = & (\beta_0\delta_0 - \beta_0\delta_1 - \beta_0\delta_2 - \beta_0\delta_3 - \beta_1\delta_0 - 2\beta_1\delta_1 - \beta_2\delta_0 - 2\beta_2\delta_2 - \beta_3\delta_0 - 2\beta_3\delta_3) \rho \\ & + (\beta_0\delta_0 + \beta_0\delta_1 + \beta_0\delta_2 + \beta_1\delta_0 + \beta_1\delta_1 + \beta_2\delta_0 + \beta_2\delta_2 + \beta_2\delta_3 - \beta_3\delta_2 + \beta_3\delta_3) i_1 \\ & + (\beta_0\delta_0 + \beta_0\delta_1 + \beta_0\delta_2 + \beta_1\delta_1 - \beta_1\delta_3 + \beta_2\delta_0 + \beta_2\delta_2 + \beta_3\delta_0 + \beta_3\delta_1 + \beta_3\delta_3) i_2 \\ & + (\beta_0\delta_0 + \beta_0\delta_2 + \beta_0\delta_3 + \beta_1\delta_0 + \beta_1\delta_1 + \beta_1\delta_2 - \beta_2\delta_1 + \beta_2\delta_2 + \beta_3\delta_0 + \beta_3\delta_3) i_3. \end{aligned}$$

Or, on peut écrire, en vertu des congruences (35),

$$\begin{aligned} \alpha_r &\equiv \beta_r \pmod{a} \quad \text{pour } r = 0, 1, 2, 3; \\ \gamma_s &\equiv \delta_s \pmod{a} \quad \text{pour } s = 0, 1, 2, 3. \end{aligned}$$

Il en résulte, en vertu des propriétés connues des congruences dans les corps algébriques,

$$(36) \quad \alpha_r \gamma_s \equiv \beta_r \delta_s \pmod{a} \quad \text{pour } r \text{ et } s = 0, 1, 2, 3.$$

Si on forme alors la différence  $A\Gamma - B\Delta$ , on voit que l'on a, en vertu des congruences (36),

$$A\Gamma - B\Delta \equiv 0 \pmod{\mathfrak{A}}$$

d'où

$$A\Gamma \equiv B\Delta \pmod{\mathfrak{A}}.$$

Le théorème, ainsi démontré pour le cas de deux congruences, peut être étendu à un nombre quelconque de congruences.

39. THÉORÈME. *Quand deux quaternions complexes entiers sont congrus entre eux suivant un idéal  $\mathfrak{A}$ , leurs conjugués relatifs et leurs normes relatives le sont également suivant le même idéal.*

En formules : La congruence

$$(37) \quad A \equiv B \pmod{\mathfrak{A}}$$

entraîne ces deux autres congruences

$$(38) \quad \bar{A} \equiv \bar{B} \pmod{\mathfrak{A}};$$

$$(39) \quad n(A) \equiv n(B) \pmod{\mathfrak{A}}.$$

Pour le démontrer, on pose

$$\mathfrak{A} \equiv \text{id} \mid a \mid.$$

Il suffit alors d'écrire explicitement

$$A \equiv \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \quad B \equiv \beta_0 \rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3,$$

de se rappeler les définitions des § 12 et 14, pour déduire de l'hypothèse (37) la congruence (38). En multipliant alors (37) et (38) membre à membre, on obtient (39), puisque  $A$  et  $\bar{A}$  sont permutables entre eux.

40. THÉORÈME. Soit, dans le domaine numéral  $\Omega$ , la congruence  $A \equiv B \pmod{\mathfrak{A}}$ . Si  $\Gamma$  est un diviseur (à droite ou à gauche) commun aux deux quaternions complexes entiers  $A$  et  $B$ , il est permis de diviser (à droite ou à gauche) les deux membres de la congruence donnée par  $\Gamma$ , à condition que, dans le domaine  $\Omega$ , l'idéal principal  $\text{id } \{n(\Gamma)\}$  soit premier avec  $\mathfrak{A}$ .

Démonstration. Soit  $\mathfrak{A} \equiv \text{id } \{a\}$ . Supposons que  $\Gamma$  soit un diviseur commun à droite de  $A$  et  $B$  et posons

$$A = A^* \Gamma, \quad B = B^* \Gamma.$$

La congruence de l'énoncé peut s'écrire dès lors

$$(40) \quad \begin{aligned} A^* \Gamma &\equiv B^* \Gamma \pmod{\mathfrak{A}} && \text{ou} \\ (A^* - B^*) \Gamma &\equiv 0 \pmod{\mathfrak{A}}. \end{aligned}$$

Multiplions les deux membres de cette dernière congruence (v. th. 38) par  $\bar{\Gamma}$ ; on obtient

$$(A^* - B^*) n(\Gamma) \equiv 0 \pmod{\mathfrak{A}}$$

où  $n(\Gamma)$  désigne la norme relative de  $\Gamma$  (v. § 11);  $n(\Gamma)$  étant un nombre du corps primordial  $K$ , posons encore

$$n(\Gamma) \equiv \gamma.$$

La congruence (40) s'écrit alors comme suit :

$$(41) \quad (A^* - B^*) \gamma \equiv 0 \pmod{\mathfrak{A}}.$$

Désignons par  $\alpha_0, \alpha_1, \alpha_2$  et  $\alpha_3$  les coordonnées du quaternion  $A^* - B^*$ . La congruence (41) signifie (v. § 12 et 14) que les quatre nombres  $\alpha_0 \gamma, \alpha_1 \gamma, \alpha_2 \gamma$  et  $\alpha_3 \gamma$ , qui sont des nombres du corps  $K$ , sont divisibles tous les quatre par l'idéal  $\mathfrak{a}$  de ce corps. Si donc l'idéal  $(\gamma)$  est premier avec  $\mathfrak{a}$ , c'est-à-dire si, dans le domaine  $\Omega$ , l'idéal  $\text{id } \{(\gamma)\} = \text{id } \{n(\Gamma)\}$  est premier avec l'idéal  $\mathfrak{A} \equiv \text{id } \{a\}$ , les nombres  $\alpha_0, \alpha_1, \alpha_2$  et  $\alpha_3$  font partie de  $\mathfrak{a}$ . Il en résulte que le quaternion  $A^* - B^*$  est congru à zéro modulo  $\mathfrak{A}$ . On peut donc diviser par  $\gamma = n(\Gamma)$  les deux membres de la congruence (41), et la congruence (40) devient donc

$$A^* - B^* \equiv 0 \pmod{\mathfrak{A}}$$

ou

$$A^* \equiv B^* \pmod{\mathfrak{A}}.$$

c. q. f. d.

41. THÉORÈME. Si les quaternions complexes entiers  $\Gamma_1, \Gamma_2, \dots, \Gamma_r$ , dont le nombre est  $r \equiv N_0(\mathfrak{A})$ , forment dans le domaine  $\Omega$  un système complet de restes modulo  $\mathfrak{A}$ ; si de plus  $A$  est un quaternion complexe entier du domaine  $\Omega$  tel que  $\text{id } \{n(A)\}$  soit premier avec  $\mathfrak{A}$ , les quaternions

$$(42) \quad \Gamma_1 A, \Gamma_2 A, \dots, \Gamma_r A$$

forment également un système complet de restes modulo  $\mathfrak{A}$ . Il en est de même des quaternions

$$(43) \quad A\Gamma_1, A\Gamma_2, \dots, A\Gamma_r.$$

*Démonstration.* Tout d'abord, les quaternions (42) sont en nombre égal aux quaternions  $\Gamma_r$ , qui forment un système complet de restes suivant  $\mathfrak{A}$ . Il suffit donc de démontrer que deux quelconques des quaternions (42), ou (43), sont incongrus entre eux modulo  $\mathfrak{A}$ .

Or, si l'on avait par exemple,

$$\Gamma_a A \equiv \Gamma_b A \pmod{\mathfrak{A}},$$

ou

$$(\Gamma_a - \Gamma_b) A \equiv 0 \pmod{\mathfrak{A}},$$

où  $\Gamma_a A$  et  $\Gamma_b A$  sont deux quaternions de la suite (42), il s'en suivrait, en vertu du théorème (§ 40) et puisque  $\text{id } |n(A)|$  est premier avec  $\mathfrak{A}$ ,

$$\Gamma_a - \Gamma_b \equiv 0 \pmod{\mathfrak{A}},$$

ce qui serait contraire à l'hypothèse puisque  $\Gamma_a$  et  $\Gamma_b$  font partie d'un même système complet de restes modulo  $\mathfrak{A}$ .

42. THÉORÈME. *La norme d'un produit de deux idéaux de quaternions complexes est égale au produit des normes des facteurs.*

En formule  $No(\mathfrak{A}\mathfrak{B}) = No(\mathfrak{A}) \cdot No(\mathfrak{B})$ .

Posons  $\mathfrak{A} \equiv \text{id } |a|$ ,  $\mathfrak{B} \equiv \text{id } |b|$ .

Appliquons le théorème 34, on obtient

$$No(\mathfrak{A}\mathfrak{B}) = [n_k(ab)]^4 = [n_k(a)]^4 [n_k(b)]^4 = No(\mathfrak{A}) \cdot No(\mathfrak{B})$$

COROLLAIRE. *La norme d'un produit d'un nombre quelconque d'idéaux de quaternions complexes est égale au produit des normes des facteurs.*

#### LE THÉORÈME DE FERMAT GÉNÉRALISÉ.

43. *Définition.* Nous appellerons « *indicateur* » de l'idéal  $\mathfrak{A}$  le nombre de ceux des éléments d'un système complet de restes suivant  $\mathfrak{A}$ , dont les normes relatives, considérées comme des idéaux principaux\*, sont premières avec  $\mathfrak{A}$ ; nous désignerons l'indicateur de  $\mathfrak{A}$  par  $\Phi(\mathfrak{A})$ . C'est une généralisation de la notion d'indicateur, notion introduite par Euler.

THÉORÈME. *Si A est un quaternion complexe entier dans le domaine numéral  $\Omega$ , quaternion dont la norme relative  $n(A)$  est première avec l'idéal  $\mathfrak{A} \equiv \text{id } |a|$ , on a la relation*

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

\* Dans le domaine numéral  $\Omega$ .

*Démonstration.* Considérons, dans le domaine  $\Omega$ , les éléments d'un système complet de restes modulo  $\mathfrak{A}$ , et soient  $B_1, B_2, \dots, B_t$ , où  $t \equiv \Phi(\mathfrak{A})$ , ceux d'entre eux dont la norme relative est première avec  $\mathfrak{A}$ . Déterminons les quaternions complexes entiers

$$\Lambda_1, \Lambda_2, \dots, \Lambda_t$$

tels que

$$(44) \quad \left. \begin{array}{l} A B_1 \equiv \Lambda_1 \\ A B_2 \equiv \Lambda_2 \\ \dots\dots\dots \\ A B_t \equiv \Lambda_t \end{array} \right\} \text{mod } \mathfrak{A}$$

où  $A$  est le quaternion dont parle l'énoncé. Les  $\Lambda_r$  sont incongrus entre eux modulo  $\mathfrak{A}$ , car  $\Lambda_k \equiv \Lambda_r \text{ mod } \mathfrak{A}$ , où  $\Lambda_k$  et  $\Lambda_r$  sont deux des quaternions  $\Lambda_1, \dots, \Lambda_t$ , entraînerait  $B_k \equiv B_r \text{ mod } \mathfrak{A}$  (en vertu des congruences (44) et du théorème § 40).

Je dis que les idéaux

$$\text{id } \{\lambda_1\}, \dots, \text{id } \{\lambda_t\}$$

sont premiers avec l'idéal  $\mathfrak{A}$ .

Posons, puisque la norme relative d'un quaternion complexe est un nombre du corps primordial  $K$  (v. § 11),

$$n(\Lambda_1) \equiv \lambda_1, \quad n(\Lambda_2) \equiv \lambda_2, \quad \dots, \quad n(\Lambda_t) \equiv \lambda_t.$$

Il s'agit donc de démontrer que les idéaux

$$\text{id } \{\lambda_k\}, \text{ pour } k = 1, 2, \dots, t$$

sont premiers avec l'idéal

$$\mathfrak{A} \equiv \text{id } \{a\}.$$

Supposons que les deux idéaux  $\text{id } \{\lambda_k\}$  où  $k$  est l'un des indices 1, 2,  $\dots, t$ , et  $\mathfrak{A} \equiv \text{id } \{a\}$  aient un facteur premier commun  $\mathfrak{P}$ ; on peut écrire

$$\text{id } \{\lambda_k\} = \mathfrak{B} \mathfrak{P} \quad \text{et} \quad \mathfrak{A} = \mathfrak{A}^* \mathfrak{P}.$$

Posons encore

$$\mathfrak{B} \equiv \text{id } \{b\}, \quad \mathfrak{P} \equiv \text{id } \{p\}, \quad \mathfrak{A}^* \equiv \text{id } \{a^*\}.$$

On a donc

$$\text{id } \{\lambda_k\} = \text{id } \{b\} \text{id } \{p\}.$$

Or, en vertu de la définition du produit de deux idéaux, on déduit de la relation précédente l'égalité suivante dans le corps primordial  $K$ :

$$(45) \quad (\lambda_k) = \mathfrak{b} \mathfrak{p}.$$

Mais  $\lambda_k$  est la norme relative de  $\Lambda_k = A B_k$ . On a donc (v. § 11)

$$\lambda_k = \Lambda_k \overline{\Lambda_k} = A B_k \cdot \overline{A B_k} = A B_k \overline{B_k} \overline{A} = n(A) n(B_k).$$

Posons

$$n(A) \equiv \alpha, \quad n(B_k) \equiv \beta_k.$$

L'égalité (45) s'écrit alors

$$(46) \quad (\lambda_k) = (\alpha)(\beta_k) = \mathfrak{b} \mathfrak{p}.$$

Mais, par hypothèse, l'idéal  $\text{id } \{n(A)\}$  ou  $\text{id } \{\alpha\}$  est premier avec l'idéal  $\mathfrak{A} \equiv \text{id } \{a\}$ . Il en résulte que, dans le corps  $K$ , l'idéal  $(\alpha)$  est premier avec l'idéal  $a$ ;  $(\alpha)$  n'est donc pas divisible par l'idéal premier  $\mathfrak{p}$  qui divise  $a$ . L'égalité (46) montre que l'idéal  $(\beta_k)$  devrait être divisible par  $\mathfrak{p}$ . Mais, si c'était le cas, l'idéal  $\text{id } \{(\beta_k)\}$  ou  $\text{id } \{n(B_k)\}$  serait divisible par  $\text{id } \{\mathfrak{p}\} = \mathfrak{P}$ . Or, c'est impossible puisque les  $B_k$  sont, par hypothèse, premiers avec  $\mathfrak{A}$  et par suite avec  $\mathfrak{P}$ .

Il résulte de ce qui précède que les idéaux

$$\text{id } \{n(\Lambda_k)\} \quad \text{pour } k = 1, 2, \dots, t$$

sont premiers avec  $\mathfrak{A}$  et que les quaternions

$$\Lambda_1, \Lambda_2, \dots, \Lambda_t$$

sont congrus, modulo  $\mathfrak{A}$ , aux quaternions de la suite

$$B_1, B_2, \dots, B_t,$$

l'ordre de succession des indices dans les deux suites ci-dessus pouvant différer.

Des congruences (44) on tire, en passant aux normes relatives et en appliquant les théorèmes § 19 et § 38,

$$n(AB_1) \cdot n(AB_2) \cdot \dots \cdot n(AB_t) \equiv n(\Lambda_1) \cdot n(\Lambda_2) \cdot \dots \cdot n(\Lambda_t) \pmod{\mathfrak{A}}$$

ou, puisque  $n(AB_k) = n(A) \cdot n(B_k)$ ,

$$(47) \quad [n(A)]^t \cdot n(B_1) \cdot \dots \cdot n(B_t) \equiv n(\Lambda_1) \cdot \dots \cdot n(\Lambda_t) \pmod{\mathfrak{A}}.$$

Mais l'ensemble des  $\Lambda_k$  coïncidant avec l'ensemble des  $B_k$  et, d'autre part, les idéaux

$$\text{id } \{n(B_k)\} \quad \text{et} \quad \text{id } \{n(\Lambda_k)\} \quad \text{pour } k = 1, 2, \dots, t$$

étant premiers avec  $\mathfrak{A}$ , on déduit de la congruence (47)

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

ou

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

C'est le théorème de Fermat généralisé au domaine  $\Omega$  des quaternions complexes.

## TABLE DES MATIÈRES

---

INTRODUCTION . . . . .	Page 7
------------------------	-----------

### PREMIÈRE PARTIE

#### Les corps dont les nombres s'expriment rationnellement à l'aide de racines carrées.

CHAPITRE I. — Le corps $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$ de degré $2^n$ ; cas particulier du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ de degré 8	11
CHAPITRE II. — Les entiers du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . . . . .	17
CHAPITRE III. — Le discriminant et la forme fondamentale du corps $K(\sqrt{A_1}, \sqrt{A_2}, \dots, \sqrt{A_n})$ . . . . .	25
CHAPITRE IV. — La décomposition des nombres rationnels en fac- teurs idéaux . . . . .	31
CHAPITRE V. — Les unités du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ . . . . .	41
CHAPITRE VI. — Le nombre de classes . . . . .	52
CHAPITRE VII. — Les corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ qui contiennent, en plus de $+1$ et $-1$ , d'autres racines de l'unité . . . . .	64

### DEUXIÈME PARTIE

#### Les quaternions dont les coordonnées sont tirées du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$ .

CHAPITRE I. — Définitions, notations ; opérations sur les quaternions complexes. Le domaine numéral $\Omega$ . . . . .	71
CHAPITRE II. — Les idéaux dans le domaine numéral $\Omega$ . . . . .	81
CHAPITRE III. — Les congruences suivant un idéal du domaine $\Omega$ . . . . . Le théorème de Fermat généralisé. . . . .	88 93

---



**UNAM**

**FECHA DE DEVOLUCIÓN**

El lector se obliga a devolver este libro antes  
del vencimiento de préstamo señalado por el  
último sello



UNIVERSIDAD NACIONAL  
AUTÓNOMA DE  
MÉXICO

