SUR LES

CORPS ALGÉBRIQUES

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 NEUCHATEL
POUR OBTENIR LE GRADE DE DOCTEUR ÈS SCIENCES

PAR

JEAN GRIZE

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES

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

UNIVERSITÉ DE NEUCHATEL

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 α qui n'y est pas contenu, ainsi que toutes les grandeurs qui prennent naissance quand on combine α avec les éléments de K à l'aide des opérations fondamentales, on obtient un corps plus général, K', entièrement déterminé par K et α ; 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

$$(1) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots\ldots + a_{n-1} x + a_n = 0.$$

Adjoignons au corps R une racine α 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 Ω 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 $\mathfrak{A} \equiv \mathrm{id}\,\{\alpha\}$, l'ensemble infini des quaternions complexes dont les quatre coordonnées parcourent, indépendamment les unes des autres, les nombres de l'idéal α 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, 3ième 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 ω 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

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

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

Si l'on pose encore

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

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 ω peut s'écrire comme suit :

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

expression dans laquelle les c_λ 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 $\overline{\overline{a}}$. De même, $\sqrt{\overline{\overline{a}}}$ désignera la racine carrée du nombre a débarrasse préalablement de ses facteurs carrés.

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

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

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 φ_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 $\sqrt{\overline{\overline{ABC}}}$ en $-\sqrt{\overline{\overline{ABC}}}$.

φ_2 désignera la permutation qui change $\sqrt{B}$ en $-\sqrt{B}$ et, par suite, $\sqrt{\overline{\overline{AB}}}$ en $-\sqrt{\overline{\overline{AB}}}$, $\sqrt{\overline{\overline{BC}}}$ en $-\sqrt{\overline{\overline{BC}}}$ et $\sqrt{\overline{\overline{ABC}}}$ en $-\sqrt{\overline{\overline{ABC}}}$.

φ_3 désignera la permutation qui change $\sqrt{C}$ en $-\sqrt{C}$ et, par suite, $\sqrt{\overline{\overline{BC}}}$ en $-\sqrt{\overline{\overline{BC}}}$, $\sqrt{\overline{\overline{CA}}}$ en $-\sqrt{\overline{\overline{CA}}}$ et $\sqrt{\overline{\overline{ABC}}}$ en $-\sqrt{\overline{\overline{ABC}}}$.

φ_4 désignera la permutation qui change simultanément $\sqrt{A}$ en $-\sqrt{A}$ et $\sqrt{B}$ en $-\sqrt{B}$ et, par suite, $\sqrt{\overline{\overline{CA}}}$ en $-\sqrt{\overline{\overline{CA}}}$ et $\sqrt{\overline{\overline{BC}}}$ en $-\sqrt{\overline{\overline{BC}}}$.

φ_5 désignera la permutation qui change simultanément $\sqrt{B}$ en $-\sqrt{B}$ et $\sqrt{C}$ en $-\sqrt{C}$ et, par suite, $\sqrt{\overline{\overline{AB}}}$ en $-\sqrt{\overline{\overline{AB}}}$ et $\sqrt{\overline{\overline{CA}}}$ en $-\sqrt{\overline{\overline{CA}}}$.

φ_6 désignera la permutation qui change simultanément $\sqrt{C}$ en $-\sqrt{C}$ et $\sqrt{A}$ en $-\sqrt{A}$ et, par suite, $\sqrt{\overline{\overline{AB}}}$ en $-\sqrt{\overline{\overline{AB}}}$ et $\sqrt{\overline{\overline{BC}}}$ en $-\sqrt{\overline{\overline{BC}}}$.

Enfin φ_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, $\sqrt{\overline{\overline{ABC}}}$ en $-\sqrt{\overline{\overline{ABC}}}$.

Si l'on désigne, en outre, par φ_0 la permutation identique qui ne change aucune des déterminations des sept radicaux $\sqrt{A}$, $\sqrt{B}$,...

..., $\sqrt{\overline{ABC}}$, 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 ω un nombre du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$. Mettons ω 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 ω ci-dessus les sept permutations $\varphi_1, \varphi_2, \ldots, \varphi_7$ du § 4, on obtient les sept nombres

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

qui sont dits les *conjugués* de ω.

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

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

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

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 4e degré *. Ce sont

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

Les indices des sous-corps $K_1, K_2, \ldots, K_7$ ont été choisis de telle manière que la permutation φ_λ, d'indice λ, laisse inchangé précisément le sous-corps K_λ de même indice.

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

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

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 ω du corps K peut s'écrire

$$\omega = m_0 + m_1\sqrt{A_1} + m_2\sqrt{A_2} + m_3\sqrt{A_3} + m_4\sqrt{A_4}$$
$$+ m_5\sqrt{A_1A_2} + m_6\sqrt{A_1A_3} + m_7\sqrt{A_1A_4} + m_8\sqrt{A_2A_3} + m_9\sqrt{A_2A_4} + m_{10}\sqrt{A_3A_4}$$
$$+ m_{11}\sqrt{A_1A_2A_3} + m_{12}\sqrt{A_1A_2A_4} + m_{13}\sqrt{A_1A_3A_4} + m_{14}\sqrt{A_2A_3A_4}$$
$$+ m_{15}\sqrt{A_1A_2A_3A_4}.$$

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. $\qquad A_1 = A_1's\,;\quad A_2 = A_2's\,;\quad A_3 = A_3's\,;\quad A_4 = A_4's,$

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

$(A_1'/A_2'/A_3') = d_4\,;\ (A_1'/A_2'/A_4') = d_3\,;\ (A_1'/A_3'/A_4') = d_2\,;\ (A_2'/A_3'/A_4') = d_1,$

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. $\quad A_1' = A_1''d_2d_3d_4\,;\ A_2' = A_2''d_1d_3d_4\,;\ A_3' = A_3''d_1d_2d_4\,;\ A_4' = A_4''d_1d_2d_3,$

expressions dans lesquelles les nombres A_1'', A_2'', A_3'' et A_4'' sont premiers entre eux trois à trois.

Désignons enfin par δ_1, δ_2, δ_3, δ_4, δ_5, δ_6 les pgcd des nombres A_1'', A_2'', A_3'' et A_4'' pris deux à deux, ce qu'on écrira

$$(A_1''/A_2'') = \delta_1\,;\quad (A_1''/A_3'') = \delta_2\,;\quad (A_1''/A_4'') = \delta_3$$
$$(A_2''/A_3'') = \delta_4\,;\quad (A_2''/A_4'') = \delta_5\,;\quad (A_3''/A_4'') = \delta_6.$$

Les formules précédentes montrent que les nombres δ_λ sont premiers entre eux deux à deux. On peut alors écrire

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

où les a_λ désignent quatre nombres appropriés qui dépendent des A_λ'' et sont premiers entre eux deux à deux.

On voit finalement qu'on peut écrire, en s'appuyant sur les formules 1. 2, 1. 3 et 1. 4,

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

On obtient alors

$$\text{1. 6.}\qquad \begin{aligned} &\overline{A_1A_2} = a_1a_2\delta_3\delta_4\delta_5 d_1 d_2\,; && \overline{A_1A_3} = a_1a_3\delta_2\delta_4\delta_6 d_1 d_3\\ &\overline{A_1A_4} = a_1a_4\delta_2\delta_3\delta_6 d_1 d_4\,; && \overline{A_2A_3} = a_2a_3\delta_1\delta_4\delta_5 d_2 d_3\\ &\overline{A_2A_4} = a_2a_4\delta_1\delta_3\delta_6 d_2 d_4\,; && \overline{A_3A_4} = a_3a_4\delta_1\delta_2\delta_5 d_3 d_4\\ &\overline{A_1A_2A_3} = a_1a_2a_3\delta_4\delta_5\delta_6 d_4 s\,; && \overline{A_1A_2A_4} = a_1a_2a_4\delta_3\delta_5\delta_6 d_3 s\\ &\overline{A_1A_3A_4} = a_1a_3a_4\delta_2\delta_4\delta_5 d_2 s\,; && \overline{A_2A_3A_4} = a_2a_3a_4\delta_1\delta_3\delta_5 d_1 s\\ &\overline{A_1A_2A_3A_4} = a_1a_2a_3a_4 d_1 d_2 d_3 d_4. \end{aligned}$$

Aucun des produits $\overline{A_1A_2},\ldots,\overline{A_1A_2A_3A_4}$ ne contient un facteur carré.

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

$$\begin{aligned} \omega = {} & c_0 + c_1\sqrt{A_1} + c_2\sqrt{A_2} + c_3\sqrt{A_3} + c_4\sqrt{A_4}\\ & + c_5\sqrt{\overline{A_1A_2}} + c_6\sqrt{\overline{A_1A_3}} + c_7\sqrt{\overline{A_1A_4}} + c_8\sqrt{\overline{A_2A_3}} + c_9\sqrt{\overline{A_2A_4}} + c_{10}\sqrt{\overline{A_3A_4}}\\ & + c_{11}\sqrt{\overline{A_1A_2A_3}} + c_{12}\sqrt{\overline{A_1A_2A_4}} + c_{13}\sqrt{\overline{A_1A_3A_4}} + c_{14}\sqrt{\overline{A_2A_3A_4}}\\ & + c_{15}\sqrt{\overline{A_1A_2A_3A_4}}, \end{aligned}$$

expression dans laquelle les nombres qui figurent sous les radicaux ont les valeurs données par les formules 1. 5 et 1. 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 8e degré (v. § 4), que le corps

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

Nous les désignerons par $\varphi_1, \varphi_2, \ldots, \varphi_{15}$ et nous adjoindrons à ces quinze permutations la permutation φ_0 qui transforme le corps K en lui-même.

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

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

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

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

$$\sqrt{A_1}, \sqrt{A_2}, \sqrt{A_3}, \ldots, \sqrt{A_n},$$

où les A_λ sont n entiers ordinaires, positifs ou négatifs et dont aucun ne contient un facteur carré, on définit le corps $K\left(\sqrt{A_1}, \sqrt{A_2}, \ldots, \sqrt{A_n}\right)$ 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 $K\left(\sqrt{A_1}, \ldots, \sqrt{A_n}\right)$ admet 2^n permutations $\varphi_0, \varphi_1, \ldots, \varphi_{m-1}$, où $m \equiv 2^n$.

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

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

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

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

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

CHAPITRE II

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

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

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 ω prend la forme

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 $\varphi_1, \varphi_2, \ldots, \varphi_7$ (v. ch. I. 4) ; on obtient les conjugués de ω, savoir : $\omega^{(1)}, \omega^{(2)}, \ldots, \omega^{(7)}$ (v. ch. I. 5).

Formons les sept nombres :

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 Ω_λ sont entiers dans les sous-corps du 4e degré dont ils font partie.

Désignons par $\sqrt{a}$ et $\sqrt{b}$ deux racines carrées déterminant un corps $K(\sqrt{a}, \sqrt{b})$ du 4e degré, a et b étant deux entiers ordinaires, positifs ou négatifs, ne contenant aucun facteur carré. Tout nombre θ 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 $\sqrt{c} \equiv \sqrt{\overline{ab}}$ et le nombre θ s'écrit

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

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

α) Si x, y, z et t sont quatre nombres entiers ordinaires.

β) 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.

γ) Si les quatre nombres x, y, z et t sont des fractions irréductibles de dénominateur 4.

Dans le cas γ), 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 Ω_λ (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 :

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

1° Si les sept produits $apqs$, $bqrs$, ..., $abcs$ ne sont pas tous congrus à 1 modulo 4, les h_λ, 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 $apqs$, $bqrs$, ..., $abcs$ sont tous congrus à 1 modulo 4, les h_λ sont des entiers de *même parité* (en particulier, si un seul des nombres h_λ est impair, ils sont tous impairs).

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

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

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

où l'on a posé

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

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

2° Si, au contraire, les $m-1$ nombres a_λ sont tous congrus à 1 modulo 4, les entiers h_λ, 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 ω un nombre entier du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$.

Mettons ω 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_λ 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 ω_7 est entier dans le corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$. On le voit en mettant ω_7 sous la forme

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

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

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

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

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

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 ω_4, ω_5 et ω_6 sont entiers dans les corps du 4e 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

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

expression dans laquelle les H_λ 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

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

les trois nombres ω_1, ω_2 et ω_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

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

* Voir Amberg, op. cit., § 2.

est aussi entier dans le corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$; 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

$$\omega - h_7\omega_7 - h'_6\omega_6 - h'_5\omega_5 - h'_4\omega_4 - H'_3\omega_3 - H'_2\omega_2 - H'_1\omega_1 - H_3\omega_3 = 0$$

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_λ sont des entiers ordinaires.

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

$$\omega_0 = 1 ; \quad \omega_1 = \frac{1+\sqrt{apqs}}{2} ; \quad \omega_2 = \frac{1+\sqrt{bqrs}}{2} ; \quad \omega_3 = \frac{1+\sqrt{crps}}{2} ;$$

II. 11.
$$\omega_4 = \frac{1+\sqrt{apqs}+\sqrt{bqrs}+\sqrt{abrp}}{4} ; \quad \omega_5 = \frac{1+\sqrt{bqrs}+\sqrt{crps}+\sqrt{bcpq}}{4} ;$$

$$\omega_6 = \frac{1+\sqrt{crps}+\sqrt{apqs}+\sqrt{caqr}}{4} ;$$

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

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.

1er sous-cas. C est congru à 2 modulo 4.

Si on met A, B et C sous la forme

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

On obtient, tous calculs faits,

II. 12.
$$\begin{cases} apqs \equiv bqrs \equiv abrp \equiv 1 & \pmod 4, \\ crps \equiv bcpq \equiv caqr \equiv abcs \equiv 2 & (\ \text{»}\ ). \end{cases}$$

2e sous-cas. C est congru à 3 modulo 4.

On obtient, dans ce cas,

II. 13.
$$\begin{cases} apqs \equiv bqrs \equiv abrp \equiv 1 & \pmod 4, \\ crps \equiv bcpq \equiv caqr \equiv abcs \equiv 3 & (\ \text{»}\ ). \end{cases}$$

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 :

$$\omega_0 = 1\,; \quad \omega_1 = \frac{1+\sqrt{apqs}}{2}\,; \quad \omega_2 = \frac{1+\sqrt{bqrs}}{2}\,; \quad \omega_3 = \sqrt{crps}\,;$$

$$\omega_4 = \frac{1+\sqrt{apqs}+\sqrt{bqrs}+\sqrt{abrp}}{4}\,; \quad \omega_5 = \frac{1+\sqrt{bqrs}+\sqrt{crps}+\sqrt{bcpq}}{2}\,;$$

II. 14.

$$\omega_6 = \frac{1+\sqrt{crps}+\sqrt{apqs}+\sqrt{caqr}}{2}\,;$$

$$\omega_7 = \frac{1+\sqrt{apqs}+\sqrt{bqrs}+\sqrt{crps}+\sqrt{abrp}+\sqrt{bcpq}+\sqrt{caqr}+\sqrt{abcs}}{4}\,.$$

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 :

$$\begin{aligned} &1^{o}\ B \equiv C \equiv 2 && \pmod 4,\\ &2^{o}\ B \equiv 2\,;\ C \equiv 3 && (\ \text{»}\ ),\\ &3^{o}\ B \equiv C \equiv 3 && (\ \text{»}\ ). \end{aligned}$$

1er 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 :

1re possibilité :

II. 15.
$$\left\{\begin{aligned} &apqs \equiv bcpq \equiv abcs \equiv 1 \pmod 4,\\ &bqrs \equiv crps \equiv abrp \equiv caqr \equiv 2 \pmod 4. \end{aligned}\right.$$

2e possibilité :

II. 16.
$$\left\{\begin{aligned} &apqs \equiv 1 && \pmod 4,\\ &bcpq \equiv abcs \equiv 3 && (\ \text{»}\ ),\\ &bqrs \equiv crps \equiv abrp \equiv caqr \equiv 2 && (\ \text{»}\ ). \end{aligned}\right.$$

2e sous-cas : $A \equiv 1\,;\ B \equiv 2\,;\ C \equiv 3 \pmod 4$.

On obtient dans ce cas

II. 17.
$$\left\{\begin{aligned} &apqs \equiv 1 && \pmod 4,\\ &bqrs \equiv abrp \equiv bcpq \equiv abcs \equiv 2 && (\ \text{»}\ ),\\ &crps \equiv caqr \equiv 3 && (\ \text{»}\ ). \end{aligned}\right.$$

3e sous-cas : $A \equiv 1 ;\ B \equiv C \equiv 3$ *(mod 4).*

On obtient dans ce cas

$$\text{II. 18.} \quad \left\{ \begin{array}{ll} apqs \equiv bcpq \equiv abcs \equiv 1 & \text{(mod 4)}, \\ bqrs \equiv crps \equiv abrp \equiv caqr \equiv 3 & (\ \ » \ \ ). \end{array} \right.$$

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 4e 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*, ..., *abcs* est congru à 1 modulo 4. Nous allons rechercher une base des entiers du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ dans ce dernier cas.

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

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

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

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

Le nombre

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

est un nombre entier dans le corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$. On le voit immédiatement en mettant ω_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 $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$.

* Les formules II. 16 donneraient une base analogue.

$$\omega_0 = 1 ;$$

$$\omega_1 = \frac{1+\sqrt{apqs}}{2} ; \qquad \omega_2 = \sqrt{crps} ; \qquad \omega_3 = \sqrt{bqrs} ;$$

II. 20.
$$\omega_4 = \frac{\sqrt{abrp}+\sqrt{bqrs}}{2} ; \qquad \omega_5 = \frac{\sqrt{abrp}+\sqrt{bcpq}}{2} ;$$

$$\omega_6 = \frac{1+\sqrt{apqs}+\sqrt{crps}+\sqrt{caqr}}{2} ;$$

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

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

II. 21. $$apqs,\ bqrs,\ \ldots,\ abcs$$

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 4e 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 8e 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 $K(\sqrt{A_1}, \sqrt{A_2}, \ldots, \sqrt{A_n})$, de degré 2^n, les dénominateurs des « entiers » peuvent prendre l'une des valeurs $1, 2, 2^2, 2^3, \ldots, 2^n$.

CHAPITRE III

Le discriminant et la forme fondamentale du corps $K\left(\sqrt{A_1}, \ldots, \sqrt{A_n}\right)$.

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

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

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

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

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

$$\mu_1, \mu_2, \ldots, \mu_r$$
$$\nu_1, \nu_2, \ldots, \nu_r$$

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

liés entre eux par le système suivant de r équations :

III. 2.
$$\begin{aligned}
\mu_1 &= c_{1,1}\nu_1 + c_{1,2}\nu_2 + \ldots + c_{1,r}\nu_r \\
\mu_2 &= c_{2,1}\nu_1 + c_{2,2}\nu_2 + \ldots + c_{2,r}\nu_r \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\mu_r &= c_{r,1}\nu_1 + c_{r,2}\nu_2 + \ldots + c_{r,r}\nu_r.
\end{aligned}$$

Si l'on désigne alors par D_μ le discriminant relatif aux μ et par D_ν le discriminant relatif aux ν, on a la relation suivante :

III. 3. $$D_\mu = \Delta^2 \cdot D_\nu,$$

Δ étant le déterminant des $c_{k,l}$.

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

3. Nous distinguerons trois cas correspondant aux trois bases des entiers du corps (v. formules II. 11, II. 14 et II. 20).

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

Posons

III. 4. $$\nu_0 \equiv 1\,;\quad \nu_1 \equiv \sqrt{apqs}\,;\quad \nu_2 \equiv \sqrt{bqrs}\,;\quad \nu_3 \equiv \sqrt{crps}\,;\quad \nu_4 \equiv \sqrt{abrp}\,;$$
$$\nu_5 \equiv \sqrt{bcpq}\,;\quad \nu_6 \equiv \sqrt{caqr}\,;\quad \nu_7 \equiv \sqrt{abcs}.$$

Posons encore, en vertu des formules II. 11 :

III. 5.
$$\begin{aligned}
\mu_0 &\equiv 1 \cdot \nu_0 \\
\mu_1 &\equiv \frac{1}{2}\nu^0 + \frac{1}{2}\nu_1 \\
\mu_2 &\equiv \frac{1}{2}\nu_0 + \frac{1}{2}\nu_2 \\
\mu_3 &\equiv \frac{1}{2}\nu_0 + \frac{1}{2}\nu_3 \\
\mu_4 &\equiv \frac{1}{4}\nu_0 + \frac{1}{4}\nu_1 + \frac{1}{4}\nu_2 + \frac{1}{4}\nu_4 \\
\mu_5 &\equiv \frac{1}{4}\nu_0 + \frac{1}{4}\nu_2 + \frac{1}{4}\nu_3 + \frac{1}{4}\nu_5 \\
\mu_6 &\equiv \frac{1}{4}\nu_0 + \frac{1}{4}\nu_1 + \frac{1}{4}\nu_3 + \frac{1}{4}\nu_6 \\
\mu_7 &\equiv \frac{1}{8}\nu_0 + \frac{1}{8}\nu_1 + \frac{1}{8}\nu_2 + \frac{1}{8}\nu_3 + \frac{1}{8}\nu_4 + \frac{1}{8}\nu_5 + \frac{1}{8}\nu_6 + \frac{1}{8}\nu_7
\end{aligned}$$

Si l'on forme le discriminant D_ν relatif aux ν_λ (v. formules III. 1 et III. 4), on obtient

III. 6. $$D_\nu = 16^6\,(abcpqrs)^4.$$

D'autre part, le déterminant Δ des coefficients des ν_λ, dans les égalités III. 5, a pour valeur

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

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

III. 8. $$D = D_\mu = (abcpqrs)^4.$$

2e cas. La base des entiers du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ est donnée por 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 $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$,

III. 9. $$D = 16^2\,(abcpqrs)^4.$$

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

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

III. 10. $$D = 16^3\,(abcpqrs)^4.$$

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

On sait ** que le discriminant du corps quadratique $K\left(\sqrt{m}\right)$ 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.

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

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

III. 11. $$apqs,\ bqrs,\ crps,\ abrp,\ bcpq,\ caqr,\ abcs$$

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

* Le corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ 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

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

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

$$D_1 D_2 \cdot \ldots \cdot D_7 = (abcpqrs)^4.$$

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

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

2e 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 supposerons 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

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

On déduit de là

$$D_1 D_2 \cdot \ldots \cdot D_7 = 16^2\,(abcpqrs)^4.$$

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

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

3e 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 supposerons, 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 $D_2, \ldots, D_7$, on peut écrire

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

On a, par suite,

$$D_1 D_2 \cdot \ldots \cdot D_7 = 16^2 (abcpqrs)^4$$

et, en vertu de la formule III. 10,

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

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

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

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

Posons

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

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

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

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

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

La norme d'un nombre du corps $K(\sqrt{A_1}, \ldots, \sqrt{A_n})$ (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 :

III. 14. $$N(x - \xi) = 0,$$

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

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

d'où

$$(x - \xi) = (a_0 x - u_0)\omega_0 + (a_1 x - u_1)\omega_1 + \ldots + (a_{m-1} x - u_{m-1})\omega_{m-1}$$

$$= \sum_{\lambda=0}^{m-1} (a_\lambda x - u_\lambda)\omega_\lambda .$$

Posons encore

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

L'équation fondamentale III. 14 s'écrit alors

$$N(\rho_0\omega_0 + \rho_1\omega_1 + \ldots + \omega_{1m-1}\omega_{m-1}) = 0$$

ou

III. 15.
$$N\left(V_0 + V_1\sqrt{A_1} + V_2\sqrt{A_2} + \ldots \right.$$
$$\left. \ldots + V_{m-1}\sqrt{\overline{A_1 A_2 \cdot \ldots A_n}}\right) = 0,$$

expression dans laquelle les V_λ sont des fonctions linéaires des ρ_λ.

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

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

ou

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

CHAPITRE IV

Décomposition des nombres rationnels en facteurs idéaux.

1. Envisageons un nombre premier rationnel π.

Pour décomposer l'idéal principal rationnel (π) 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* (π) *et de degré* f*; on peut toujours construire une fonction* $\Pi(x; u_1, u_2, \ldots, u_n)$ *de degré* f *en* x*, irréductible suivant* π *et qui, lorsqu'on y remplace* x *par la forme fondamentale* ξ *(v. ch. III), a les propriétés suivantes: les coefficients des puissances et des produits des* $u_1, u_2, \ldots, u_n$ *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* (π).

II. *Si* (π)*, décomposé en facteurs premiers idéaux, donne*

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

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

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

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

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

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

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

1er *cas.* π est un nombre premier impair.

2e cas. π 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 π EST UN NOMBRE PREMIER IMPAIR.

3. Il faut distinguer deux sous-cas :

Sous-cas α. Aucun des nombres a, b, c, p, q, r, s n'est divisible par π (v. ch. I, 1).

Sous-cas β. L'un des nombres de la suite a, b, c, p, q, r, s est divisible par π *.

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

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

dans laquelle les V_λ 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 $V_0 + V_1\sqrt{apqs} + \ldots + V_7\sqrt{abcs}$ à l'aide des permutations $\varphi_0, \varphi_1, \ldots, \varphi_7$ (v ch. I, 4).

Le dénominateur du premier membre de IV. 1 est une puissance de 2. Cela résulte du fait que les entiers $\omega_0, \omega_1, \ldots, \omega_7$, 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, π 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

$$\text{IV. 2.} \qquad N = FF_1 \ldots F_7$$

expression dans laquelle on a

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

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

En ce qui concerne les sept nombres de la suite

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

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 π ;

* 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 π.

2° ou bien trois nombres de la suite IV. 3 sont résidus quadratiques de π ; en outre, ces trois nombres forment la base de l'un des sous-corps du 4e 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* π. Il existe alors sept nombres $\rho_1, \rho_2, \ldots, \rho_7$ tels que

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

L'égalité IV. 2*a* peut alors s'écrire, modulo π,

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

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

$$\text{IV. 6.} \qquad (\pi) = \mathfrak{p}\mathfrak{p}_1 \ldots \mathfrak{p}_7. \quad \text{(idéaux du 1er degré).}$$

On peut poser en outre

$$\mathfrak{p} = \mathrm{id}\,|\pi, F|$$

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

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

Si on désigne par $D_1, D_2, \ldots, D_7$ les discriminants des sept sous-corps quadratiques de $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$, il résulte des hypothèses faites sur les nombres *apqs*, ..., *abcs* que les sept discriminants D_λ sont résidus quadratiques de π. 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 π, égal à -1 quand x est non résidu et, enfin, égal à zéro quand x est divisible par π.

La formule IV. 6 correspond au cas

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

2° *Trois des nombres de la suite IV. 3 sont résidus quadratiques de* π. Nous savons que les trois nombres de la suite IV. 3 qui sont résidus quadratiques de π déterminent un des sous-corps du 4e 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 ρ_1, ρ_2 et ρ_3 tels que les congruences suivantes sont satisfaites :

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

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

IV. 8. $$N = F F_1 F_2 . \ldots F_7 .$$

F_1 se déduisant de F à l'aide de la permutation φ_1, le produit FF_1 fait partie du sous-corps K_1 (v. ch. I, 6), on peut donc écrire

IV. 9. $$FF_1 = A_0 + A_1\sqrt{bqrs} + A_2\sqrt{crps} + A_3\sqrt{bcpq}$$

expression dans laquelle les A_λ sont des fonctions des quantités V_s qui figurent dans l'expression IV. 5.

Posons

$$FF_1 \equiv F' .$$

Les produits des six facteurs $F_2, \ldots, F_7$ 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

IV. 10. $$N = F' F_1' F_2' F_3' .$$

Dans cette dernière égalité, F' a la valeur IV. 9 et peut s'écrire modulo π 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

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

où $$\mathfrak{p} = \mathrm{id}\,(\pi, F')$$

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

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 $K(\sqrt{bcpq})$, 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* β (v. § 3). *Un et un seul des nombres de la suite* a, b, c, p, q, r, s *est divisible par* π.

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

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

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

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

1° Si les trois nombres *bqrs*, *crps* et *bcpq* sont tous les trois résidus quadratiques de π, il existe trois nombres ρ_1, ρ_2 et ρ_3 tels que

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

Le facteur F s'écrit alors, mod π (v. formule IV, 2*a*),

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

et les facteurs F_2, F_3 et F_5 se déduisent de F à l'aide des permutations φ_λ.

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

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

où $\mathfrak{p} = \mathrm{id}\,\{\pi, F\}$, 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,

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

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

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

où l'on a posé

$$A_0 \equiv V_0^2 - V_2^2 bqrs + V_3^2 crps - V_5^2 bcpq$$
$$A_1 \equiv 2\,(V_0 V_3 - V_2 V_5 bq)$$

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

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

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

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

7. Décomposition d'un nombre premier impair π dans le corps $K(\sqrt{A_1}, \sqrt{A_2}, \ldots, \sqrt{A_n})$.

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

IV. 17.

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

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

8. *1er cas. Aucun des nombres a_λ, $d_k^{(l)}$, s n'est divisible par π.*

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

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

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

1re possibilité. Les 2^n-1 nombres de la suite IV. 18 sont résidus quadratiques de π.

2e possibilité. $2^{n-1}-1$ nombres de la suite IV. 18 sont résidus quadratidiques de π 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 $\overline{A_1A_2 \ldots A_s}$ $(1 \leq s \leq n)$, on peut raisonner sur le nombre $A_1A_2 \ldots A_s$, puisque ces deux nombres sont les mêmes à un facteur carré près.

1° Si les n nombres $A_1, \ldots, A_n$ sont tous résidus quadratiques de π, les 2^n-1 nombres de la suite IV. 18 sont évidemment tous résidus quadratiques de π.

2° Si un et un seul des nombres $A_1, \ldots, A_n$, par exemple A_1, est non-résidu quadratique de π, 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_rA_s, il y a $n-1=\binom{n-1}{1}$ non-résidus,
» » » $A_rA_sA_t$, 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

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

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

parmi les nombres A_r, 2 non-résidus,
» » » A_rA_s, $2(n-2)$ » »
» » » $A_rA_sA_t$, $(n-2)(n-3)$ » »

etc...

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

$$2+2(n-2)+(n-2)(n-3)+\frac{(n-2)(n-3)(n-4)}{3}$$
$$+\frac{(n-2)(n-3)(n-4)(n-5)}{3.4}+\ldots+\frac{(n-2)(n-3)\ldots(n-k)}{3.4\ldots(k-1)}$$
$$+\ldots+\frac{(n-2)(n-3)\ldots3.2.1}{3.4\ldots(n-2)}=2^{n-1}.$$

La démonstration se fait de la même manière lorsque $3, 4, \ldots, n$ nombres de la suite $A_1, A_2, \ldots, A_n$ sont non résidus quadratiques de π. 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 π, l'idéal (π) admet, dans le corps $K(\sqrt{A_1}, \ldots, \sqrt{A_n})$, la décomposition suivante :

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

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

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

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

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

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

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

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. 2e cas. *Un et un seul des nombres a_λ, $d_k^{(l)}$, s est divisible par π.*

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

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

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

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

2° 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 (π) est la suivante :

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

où $\mathfrak{p}, \mathfrak{p}_1, \ldots$ 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).

1er cas. *La base des entiers est donnée par les formules II. 11.*

Dans ce cas, les sept nombres de la suite

IV. 19. *apqs, bqrs, crps, abrp, bcpq, caqr, abcs*

sont congrus à 1 modulo 4.

Le dénominateur commun des nombres $\omega_0, \omega_1, \ldots, \omega_7$ 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 devrons 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 $\rho_1, \ldots, \rho_7$ tels que les congruences suivantes sont satisfaites :

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

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

$$N \equiv F' F_1' F_2' \ldots\ldots F_7',$$

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

$$F' = V_0' + V_1' \sqrt{apqs} + V_2' \sqrt{bqrs} + \ldots\ldots + V_7' \sqrt{abcs},$$

$F_1', \ldots, F_7'$ se déduisant de F' à l'aide des permutations $\varphi_1, \ldots, \varphi_7$.

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

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

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

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

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

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

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

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 $\mathfrak{p}, \ldots, \mathfrak{p}_3$ sont des idéaux du second dégré.

2e CAS : *La base est donnée par les formules 11.14 ou 11.20.* 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 π un nombre premier quelconque et soient d'autre part $D_1, D_2, \ldots, D_7$ les discriminants des sept sous-corps quadratiques du corps $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$. L'idéal (π), dans ce corps K, se décompose conformément au tableau ci-après :

IV. 21.

1. Les sept symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à $+1$. $(\pi) = \mathfrak{p}\,\mathfrak{p}_1 \ldots \mathfrak{p}_7$ (idéaux du 1er degré).

2. Trois symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à $+1$; Quatre » » » » -1 $\Big\}$ $(\pi) = \mathfrak{p}\,\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ (idéaux du 2e degré).

3. Quatre symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à 0 ; Trois » » » » $+1$ $\Big\}$ $(\pi) = \mathfrak{p}^2\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ (idéaux du 1er degré).

4. Quatre symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à 0 ; Deux » » » » -1 ; Un symbole » est égal » $+1$ $\Big\}$ $(\pi) = \mathfrak{p}^2\mathfrak{p}_1^2$ (idéaux du 2e degré).

5. Six symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à 0 ; Un symbole » est égal à $+1$ $\Big\}$ $(\pi) = \mathfrak{p}^4\mathfrak{p}_1$ (idéaux du 1er degré).

6. Six symboles $\left(\frac{D_\lambda}{\pi}\right)$ sont égaux à 0 ; Un symbole » est égal à -1 $\Big\}$ $(\pi) = \mathfrak{p}^4$ (idéal du 2e 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 ε, 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 :

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

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 ± 1 et parmi celles-là il y a une unité fondamentale ε 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 $K = K^{(1)}, K^{(2)}, \ldots, K^{(m)}$ 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 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$, dites unités fondamentales, telles que toute autre unité ε du corps K puisse se mettre sous la forme*

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

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

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

THÉORÈME. — *Le corps $K\left(\sqrt{A_1}, \ldots, \sqrt{A_n}\right)$, 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 $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ 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 $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ 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 4e degré (v. chap. I. 6) est réel. Cela résulte de la façon même dont ces sous-corps sont formés. Nous supposerons, pour fixer les idées, que le sous-corps réel est K_1 dont la base est $\left[1, \sqrt{bqrs}, \sqrt{crps}, \sqrt{bcpq}\right]$ (v. ch. I. 6). Les trois sous-corps quadratiques $K\left(\sqrt{bqrs}\right)$, $K\left(\sqrt{crps}\right)$ et $K\left(\sqrt{bcpq}\right)$ étant réels, ils admettent chacun une et une seule unité fondamentale (v. § 1 de ce chap.). Désignons par ε_1 l'unité fondamentale de $K\left(\sqrt{bqrs}\right)$, par ε_2 celle de $K\left(\sqrt{crps}\right)$ et par ε_3 celle de $K\left(\sqrt{bcpq}\right)$.

* 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 $K_1\left(\sqrt{bqrs},\ \sqrt{crps}\right)$ admet trois unités fondamentales que nous désignerons par η_1, η_2 et η_3. Enfin ζ_1, ζ_2 et ζ_3 seront trois unités fondamentales du corps envisagé $K\left(\sqrt{A},\ \sqrt{B},\ \sqrt{C}\right)$.

5. Problème. — *Connaissant les trois unités fondamentales* ε_1, ε_2 et ε_3 *des sous-corps quadratiques réels* $K\left(\sqrt{bqrs}\right)$, $K\left(\sqrt{crps}\right)$ *et* $K\left(\sqrt{bcpq}\right)$, *ainsi que trois unités fondamentales* η_1, η_2 *et* η_3 *du sous-corps réel* $K_1\left(\sqrt{bqrs},\ \sqrt{crps}\right)$ *du 4e degré, trouver trois unités fondamentales* ζ_1, ζ_2 *et* ζ_3 *du corps* $K\left(\sqrt{A},\ \sqrt{B},\ \sqrt{C}\right)$.

Pour résoudre ce problème, on peut procéder comme suit : Les trois unités η_1, η_2 et η_3, qui sont trois unités fondamentales du sous-corps $K_1\left(\sqrt{bqrs},\ \sqrt{crps}\right)$, peuvent s'exprimer, en fonction des unités fondamentales de K, de la façon suivante :

$$\begin{aligned}\eta_1 &= \pm \zeta_1^{a_1}\,\zeta_2^{a_2}\,\zeta_3^{a_3}\\ \eta_2 &= \pm \zeta_1^{b_1}\,\zeta_2^{b_2}\,\zeta_3^{b_3}\\ \eta_3 &= \pm \zeta_1^{c_1}\,\zeta_2^{c_2}\,\zeta_3^{c_3},\end{aligned}$$

formules qui peuvent s'écrire aussi

$$\text{V. 1.}\qquad \begin{aligned}\eta_1 &= \pm \lambda_1^{a}\\ \eta_2 &= \pm \lambda_1^{b}\lambda_2^{c}\\ \eta_3 &= \pm \lambda_1^{d}\lambda_2^{e}\lambda_3^{f}.\end{aligned}$$

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 ; λ_1, λ_2 et λ_3 sont de nouvelles unités fondamentales de $K\left(\sqrt{A},\ \sqrt{B},\ \sqrt{C}\right)$ et $b, c, \ldots, f$ 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 φ_λ (v. ch. I. 4) choisie convenablement.

Considérons, par exemple, la première des égalités V. 1, et appliquons-lui la permutation φ_1 qui laisse inchangé le sous-corps réel K_1. Cette égalité devient, puisque η_1 fait partie de K_1,

$$\text{V. 2.}\qquad \eta_1 = \pm \lambda_1^{(1)a}$$

où $\lambda_1^{(1)}$ désigne ce que devient λ_1 par l'application de la permutation φ_1.

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

V. 3. $$\eta_1^2 = (\lambda_1 \lambda_1^{(1)})^a.$$

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. $$\lambda_1 \lambda_1^{(1)} = \pm \eta_1^{m_1} \eta_2^{m_2} \eta_3^{m_3}. \qquad (m_\lambda \text{ entiers ordinaires})$$

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

$$\eta_1^2 = \pm \eta_1^{am_1} \eta_2^{am_2} \eta_3^{am_3}$$

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 :

V. 5.

		1re	2e	3e	4e	5e	6e	7e	8e
a	=	1	1	1	2	1	2	2	2
c	=	1	1	2	1	2	1	2	2
f	=	1	2	1	1	2	2	1	2

Nous ferons tout d'abord la remarque suivante :

Si λ_1, λ_2 et λ_3 sont trois unités fondamentales du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$, 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 λ_2 et de λ_3 respectivement. En effet, si

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

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

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

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 λ_1, λ_2 et λ_3 (v. formules V. 1) 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,

$$\eta_1 = \pm \lambda_1$$
$$\eta_2 = \pm \lambda_1^b \lambda_2$$
$$\eta_3 = \pm \lambda_1^d \lambda_2^e \lambda_3$$

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

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

c'est-à-dire

$$\eta_1,\ \eta_2 \quad \text{et} \quad \eta_3.$$

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,

$$\eta_1 = \pm \lambda_1$$
V. 6.
$$\eta_2 = \pm \lambda_1^b \lambda$$
$$\eta_3 = \pm \lambda_1^d \lambda_2^e \lambda_3^2.$$

En vertu de la remarque faite plus haut, les trois unités fondamentales λ_1, λ_2 et λ_3 peuvent être remplacées respectivement par λ_1, $\lambda_1^b \lambda_2$ et λ_3.

Supposons, par exemple, que l'on ait

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

et posons, par suite,

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

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

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

L'unité λ_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 $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ les trois unités λ_1, $\lambda_1^b \lambda_2$ et $\lambda_1^{d_1} \lambda_2^{e_1} \lambda_3$, c'est-à-dire

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

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 :

η_1, η_2 et η_3 désignant trois unités fondamentales du sous-corps réel $K_1\left(\sqrt{bqrs}, \sqrt{crps}\right)$, les unités fondamentales du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ qui en résultent peuvent prendre les formes suivantes :

Valeur du produit acf (formules V. 1.)	Forme des unités fondamentales du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$.		
$acf = 1$	η_r,	η_s,	η_u
$acf = 2$	η_r,	η_s,	$\sqrt{\pm \eta_u}$
	η_r,	η_s,	$\sqrt{\pm \eta_r \eta_u}$ ou $\sqrt{\pm \eta_s \eta_u}$
	η_r,	η_s,	$\sqrt{\pm \eta_r \eta_s \eta_u}$
$acf = 4$	η_r,	$\sqrt{\pm \eta_s}$,	$\sqrt{\pm \eta_u}$
	η_r,	$\sqrt{\pm \eta_s}$,	$\sqrt{\pm \eta_r \eta_u}$
	η_r,	$\sqrt{\pm \eta_s}$,	$\sqrt[4]{\pm \eta_s \eta_u^2}$
	η_r,	$\sqrt{\pm \eta_s}$,	$\sqrt[4]{\pm \eta_r^2 \eta_s \eta_u^2}$
	η_r,	$\sqrt{\pm \eta_r \eta_s}$,	$\sqrt{\pm \eta_r \eta_u}$
	η_r,	$\sqrt{\pm \eta_r \eta_s}$,	$\sqrt[4]{\pm \eta_r \eta_s^2 \eta_u^2}$
	η_r,	$\sqrt{\pm \eta_r \eta_s}$,	$\sqrt[4]{\pm \eta_r \eta_s \eta_u^2}$
$acf = 8$	$\sqrt{\pm \eta_r}$,	$\sqrt{\pm \eta_s}$,	$\sqrt{\pm \eta_u}$
	$\sqrt{\pm \eta_r}$,	$\sqrt{\pm \eta_s}$,	$\sqrt[4]{\pm \eta_s \eta_u^2}$
	$\sqrt{\pm \eta_r}$,	$\sqrt{\pm \eta_s}$,	$\sqrt[4]{\pm \eta_r \eta_s \eta_u^2}$
	$\sqrt{\pm \eta_r}$,	$\sqrt[4]{\pm \eta_r \eta_s^3}$,	$\sqrt[4]{\pm \eta_r \eta_u^2}$
	$\sqrt{\pm \eta_r}$,	$\sqrt[4]{\pm \eta_r \eta_s^2}$,	$\sqrt[8]{\pm \eta_r^3 \eta_2^2 \eta_3}$
	$\sqrt{\pm \eta_r}$,	$\sqrt[4]{\pm \eta_r \eta_s^2}$,	$\sqrt[8]{\pm \eta_r \eta_s^2 \eta_u^4}$

V. 7.

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

Nous nous bornerons à le démontrer pour $\sqrt[4]{\eta_1 \eta_2 \eta_3^2}$.

Posons

$$\lambda \equiv \sqrt[4]{\eta_1 \eta_2 \eta_3^2} \qquad \text{V. 8.}$$

et supposons que λ soit une unité du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$. Appliquons aux deux membres de l'égalité V. 8 la permutation φ_1 qui laisse

inchangé le sous-corps K_1. Les trois unités η_1, η_2 et η_3 faisant partie du sous-corps K_1, elles ne changent pas, et l'égalité V. 8 devient

V. 9. $$\lambda^{(1)} = \sqrt[4]{\eta_1 \eta_2 \eta_3^2}.$$

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

V. 10. $$\lambda\lambda^{(1)} = \eta_3 \sqrt{\eta_1 \eta_2}.$$

Mais $\lambda\lambda^{(1)}$ fait partie du sous-corps K_1 (v. cb. l. 6). Comme η_1, η_2 et η_3 sont trois unités fondamentales de K_1, on peut écrire

V. 11. $$\lambda\lambda^{(1)} = \pm \eta_1^{a_1} \eta_2^{a_2} \eta_3^{a_3},$$

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,

$$\eta_1^{a_1} \eta_2^{a_2} \eta_3^{a_3} = \eta_3 \sqrt{\eta_1 \eta_2}$$

ou $$\eta_1^{2a_1} \eta_2^{2a_2} \eta_3^{2a_3} = \eta_1 \eta_2 \eta_3^2.$$

De cette égalité on tire, en identifiant les exposants,

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

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 $\lambda \equiv \sqrt[4]{\eta_1 \eta_2 \eta_3^2}$ 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 $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$.

V. 12.

Valeur du produit acf	Forme des unités fondamentales.		
1	η_r ,	η_s ,	η_u
$2^1 = 2$	η_r ,	η_s ,	$\sqrt{\pm \eta_u}$
	η_r ,	η_s ,	$\sqrt{\pm \eta_r \eta_u}$
	η_r ,	η_s ,	$\sqrt{\pm \eta_r \eta_s \eta_u}$
$2^2 = 4$	η_r ,	$\sqrt{\pm \eta_s}$,	$\sqrt{\pm \eta_u}$
	η_r ,	$\sqrt{\pm \eta_s}$,	$\sqrt{\pm \eta_r \eta_u}$
	η_r ,	$\sqrt{\pm \eta_r \eta_s}$,	$\sqrt{\pm \eta_r \eta_u}$
$2^3 = 8$	$\sqrt{\pm \eta_r}$,	$\sqrt{\pm \eta_s}$,	$\sqrt{\pm \eta_u}$

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

ε_1	l'unité	fondamentale	du	corps	$K(\sqrt{bqrs})$
ε_2	»	»	»	»	$K(\sqrt{crps})$
ε_3	»	»	»	»	$K(\sqrt{bcpq})$
ε_4	»	»	»	»	$K(\sqrt{apqs})$
ε_5	»	»	»	»	$K(\sqrt{abrp})$
ε_6	»	»	»	»	$K(\sqrt{caqr})$
ε_7	»	»	»	»	$K(\sqrt{abcs})$.

Chacun des sept sous-corps du 4e degré est réel et admet trois unités fondamentales. On sait en outre que, si ε_r, ε_s et ε_u sont les trois unités fondamentales des trois sous-corps quadratiques d'un corps K_ν du 4e degré (v. ch. I. 6), les trois unités fondamentales de K_ν peuvent prendre l'une des sept formes suivantes ** :

V. 13.

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

Enfin, les unités ε_λ contenues dans les différents sous-corps du 4e degré sont données par le tableau suivant :

V. 14.

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

Nous désignerons dans la suite par $\alpha_1, \beta_1, \gamma_1$ un système d'unités fondamentales du sous-corps du 4e 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 fondalentales 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, $\varepsilon_r^{(3)} \equiv \varepsilon_4$; $\varepsilon_u^{(3)} \equiv \varepsilon_1$; $\varepsilon_u^{(3)} \equiv \varepsilon_5$.

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

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

V. 15.
$$\begin{aligned}
\mu_1 &= \pm \lambda_1^{a_1} \\
\mu_2 &= \pm \lambda_1^{b_1} \lambda_2^{a_2} \\
\mu_3 &= \pm \lambda_1^{c_1} \lambda_2^{b_2} \lambda_3^{a_3} \\
\mu_4 &= \pm \lambda_1^{d_1} \lambda_2^{c_2} \lambda_3^{b_3} \lambda_4^{a_4} \\
\mu_5 &= \pm \lambda_1^{e_1} \lambda_2^{d_2} \lambda_3^{c_3} \lambda_4^{b_4} \lambda_5^{a_5} \\
\mu_6 &= \pm \lambda_1^{f_1} \lambda_2^{e_2} \lambda_3^{d_3} \lambda_4^{c_4} \lambda_5^{b_5} \lambda_6^{a_6} \\
\mu_7 &= \pm \lambda_1^{g_1} \lambda_2^{f_2} \lambda_3^{e_3} \lambda_4^{d_4} \lambda_5^{c_5} \lambda_6^{b_6} \lambda_7^{a_7} ,
\end{aligned}$$

où $\lambda_1, \lambda_2, \ldots, \lambda_7$ *forment un système d'unités fondamentales de* $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$, *chacun des sept entiers* $a_1, a_2, \ldots, a_7$ *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 4e degré (v. tableau V. 13), on peut toujours trouver, parmi les dites unités fondamentales, une unité fondamentale μ_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 $\mu_1, \mu_2 \ldots, \mu_{m-1}$ $(m < 7)$, des égalités V. 15, de telle manière que les entiers $a_1, \ldots, a_{m-1}$ ne puissent prendre que les valeurs 1 et 2, il est toujours possible de choisir μ_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

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

R est donc égal à 1 si les sept entiers a_λ sont égaux à 1 ; $R = 2$ si un et un seul des entiers a_λ 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 $a_1, a_2, \ldots, a_7$ 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 4e degré aient des unités fondamentales de la forme (1), tableau V. 13.

Admettons, par exemple, (v. tableau V. 14) que ε_1, ε_2 et ε_3 soient les unités fondamentales de K_1 ; ε_4, ε_2 et ε_6 celles de K_2 ; ε_4, ε_1 et ε_5 celles de K_3 et ε_2, ε_5, ε_7 celles de K_4.

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

V. 16.
$$\begin{aligned}
\varepsilon_1 &= \pm \lambda_1^{a_1} \\
\varepsilon_2 &= \pm \lambda_1^{b_1} \lambda_2^{a_2} \\
\varepsilon_3 &= \pm \lambda_1^{c_1} \lambda_2^{b_2} \lambda_3^{a_3} \\
\varepsilon_4 &= \pm \lambda_1^{d_1} \lambda_2^{c_2} \lambda_3^{b_3} \lambda_4^{a_4} \\
\varepsilon_5 &= \pm \lambda_1^{e_1} \lambda_2^{d_2} \lambda_3^{c_3} \lambda_4^{b_4} \lambda_5^{a_5} \\
\varepsilon_6 &= \pm \lambda_1^{f_1} \lambda_2^{e_2} \lambda_3^{d_3} \lambda_4^{c_4} \lambda_5^{b_5} \lambda_6^{a_6} \\
\varepsilon_7 &= \pm \lambda_1^{g_1} \lambda_2^{f_2} \lambda_3^{e_3} \lambda_4^{d_4} \lambda_5^{c_5} \lambda_6^{b_6} \lambda_7^{a_7}.
\end{aligned}$$

On a alors le

THÉORÈME. — *Dans le cas particulier des formules V. 16, le corps* $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ *n'admet aucune unité de la forme* $\sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \ldots \varepsilon_k^{\alpha_k}}$ $(k \leq 7)$ *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 $\alpha_1, \alpha_2, \ldots, \alpha_k$, dans l'expression $\sqrt[n]{\pm \varepsilon_1^{\alpha_1} \ldots \varepsilon_k^{\alpha_k}}$, est impair. Supposons, pour fixer les idées, que α_1 soit impair et posons $\alpha_1 \equiv 2\alpha_1' + 1$.

Posons encore

V. 17.
$$\theta \equiv \sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \ldots \varepsilon_k^{\alpha_k}}.$$

Si on applique aux deux membres de V. 17 la permutation φ_1 (v. ch. I. 4), les unités ε_1, ε_2 et ε_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

V. 18.
$$\theta' \equiv \sqrt[n]{\pm \varepsilon_1^{\alpha_1} \varepsilon_2^{\alpha_2} \varepsilon_3^{\alpha_3} \varepsilon_4'^{\alpha_4} \ldots}$$

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

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

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, ε_1, ε_2 et ε_3 (v. ch. 1. 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 $\theta = \sqrt[n]{\pm\, \varepsilon_1^{\alpha_1}\, \varepsilon_2^{\alpha_2} \cdots \varepsilon_k^{\alpha_k}}$ ne peut pas être une unité du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ dès que n est supérieur à 2.

14. *Forme des unités fondamentales du corps* $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ *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

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

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

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

3) Dans un système d'unités fondamentales du corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$, système qui comprend 7 unités, nous n'écrirons que les unités ε_λ situées sous un radical. Par exemple, le système $\sqrt{\varepsilon_1}$, $\sqrt{\varepsilon_2}$, ε_3, ε_4, ε_5, ε_6, ε_7 s'écrira comme suit :

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

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

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

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 $\sqrt{\varepsilon_j}$ et cinq unités de la forme ε_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,

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

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

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

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

(7 formes.)

Si $R = 4$

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

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

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

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

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

Nous écrirons, de plus,

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

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

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

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

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

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

où l'on a

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

Les grandeurs

VI. 1. $$l_1(\xi), l_2(\xi), \ldots, l_m(\xi)$$

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

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

VI. 2. $$\xi^{(1)}\xi^{(2)} \ldots \xi^{(m)} = N(\xi).$$

2. *1er cas. Le corps* $K\left(\sqrt{A_1}, \sqrt{A_2}, \ldots, \sqrt{A_n}\right)$ *est réel.*

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

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

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

d'où l'on déduit

VI. 3. $$l_1(\alpha) + l_2(\alpha) + l_3(\alpha) + \ldots + l_m(\alpha) = lN(\alpha),$$

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

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

VI. 4. $$l_1(\lambda) + l_2(\lambda) + l_3(\lambda) + \ldots + l_m(\lambda) = 0.$$

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

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

2e cas. Le corps $K\left(\sqrt{A_1}, \ldots, \sqrt{A_n}\right)$ *est imaginaire.*

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

$$l_1(\alpha) + l_2(\alpha) + \ldots + \underline{l_m(\alpha)} = lN(\alpha).$$

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

VI. 6. $$l_1(\lambda) + l_2(\lambda) + \ldots + \underline{l_m(\lambda)} = 0.$$

Mais le corps $K\left(\sqrt{A_1}, \ldots, \sqrt{A_n}\right)$ 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 $r+1$,

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

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

Le régulateur du corps $K\left(\sqrt{A_1}, \sqrt{A_2}, \ldots, \sqrt{A_n}\right)$.

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

Formons le déterminant

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

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

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

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

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

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

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

Nous utiliserons dans la suite la formule suivante**:

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

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

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 ν, 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, 3e 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 * :

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

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

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

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

Le produit Π 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 (π) que nous écrirons donc (p).

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

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

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

$$\left(\frac{1}{1 - p^{-s}}\right)^8 = (1 - p^{-s})^{-8}$$

$$= (1 - p^{-s})^{-1} \cdot \left[1 - \left(\frac{D_1}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_2}{p}\right) p^{-s}\right]^{-1} \cdot \ldots \cdot \left[1 - \left(\frac{D_7}{p}\right) p^{-s}\right]^{-1}.$$

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

Le facteur sous le symbole Π dans la formule VI. 11 peut s'écrire

$$(1 - p^{-2s})^{-4} = (1 - p^{-s}) \cdot \left[1 - \left(\frac{D_r}{p}\right) p^{-s}\right]^{-1}$$

$$\cdot \left[1 - \left(\frac{D_u}{p}\right) p^{-s}\right]^{-1} \cdot \left[1 - \left(\frac{D_v}{p}\right) p^{-s}\right]^{-1} \cdot \prod_w \left[1 - \left(\frac{D_w}{p}\right) p^{-s}\right]^{-1},$$

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.

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

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

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

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

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.

4e 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 Π dans la formule VI. 11 peut s'écrire

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

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

5e 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 Π dans la formule VI. 11 s'écrit

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

6e 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 Π dans la formule VI. 11 peut se mettre sous la forme

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

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

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

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

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

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

Or, on a

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

La formule VI. 14 devient alors

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

Si on pose, pour simplifier l'écriture,

$$\sum\frac{1}{m}\left(\frac{D_\lambda}{m}\right)\equiv\sum_\lambda \qquad \text{pour } \lambda=1,2,\ldots,7,$$

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

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

* 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

$$\text{VI. 17.} \qquad h = \frac{\sum_1 \sum_2 \cdot \ldots \cdot \sum_7 \sqrt{D}}{2^3 E \pi^4}.$$

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

Reprenons les formules V. 1

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

où λ_1, λ_2 et λ_3 sont trois unités fondamentales de $K(\sqrt{A}, \sqrt{B}, \sqrt{C})$, tandis que η_1, η_2 et η_3 sont trois unités fondamentales du sous-corps réel $K_1(\sqrt{bqrs}, \sqrt{crps})$.

Désignons par Δ_η le déterminant VI. 7 relatif aux η, on a

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

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

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

Le déterminant Δ_η (formule VI.19) peut s'écrire

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

où Δ_λ désigne le déterminant VI. 7 relatif aux λ_r.

Pour calculer Δ_η il faut distinguer six cas différents suivant la forme des unités fondamentales η_1, η_2 et η_3 du sous-corps réel K_1. Ces unités fondamentales sont données par le tableau V.13.

Si on calcule la valeur de Δ_η pour les six cas de ce tableau, on voit que Δ_η a la forme suivante :

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

où ρ, entier ordinaire, est donné par le tableau suivant :

VI. 22

Cas	Unités fondamentales du sous-corps $K_1(\sqrt{bqrs}, \sqrt{rcps})$			Valeur de ρ
1	ε_1,	ε_2,	ε_3	2
2	ε_1,	ε_2,	$\sqrt{\varepsilon_3}$	1
3	ε_1,	ε_2,	$\sqrt{\varepsilon_1\varepsilon_3}$	1
4	ε_1,	ε_2,	$\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}$	1
5	ε_1,	$\sqrt{\varepsilon_2}$,	$\sqrt{\varepsilon_3}$	0
6	ε_1,	$\sqrt{\varepsilon_2}$,	$\sqrt{\varepsilon_1\varepsilon_3}$	0
7	ε_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^μ, où $\mu = 0, 1, 2$ ou 3 (v. tableau V. 12). Par suite, la formule VI. 23 peut s'écrire, si on remplace Δ_η 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 σ, qui dépend à la fois de la forme des unités fondamentales η_1, η_2 et η_3 du sous-corps réel $K_1(\sqrt{bqrs}, \sqrt{crps})$ (v. tableau VI. 22) et de la valeur du produit acf, est donné par le tableau suivant :

VI. 25

	$acf = 1$	$acf = 2$	$acf = 2^2$	$acf = 2^3$
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 ρ correspondant au cas n^{o} du tableau VI.22 et à une valeur donnée du produit *acf*, se trouve à l'intersection de la n^{o} 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

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

où Δ_λ 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 Δ_λ par sa valeur,

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

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

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

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 *

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

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 *

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

Mais $u = 2$, donc

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

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

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

* 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 :

VI. 32.
$$\begin{aligned}
\varepsilon_1 &= \pm \lambda_1^{a_1} \\
\varepsilon_2 &= \pm \lambda_1^{b_1} \lambda_2^{a_2} \\
\varepsilon_3 &= \pm \lambda_1^{c_1} \lambda_2^{b_2} \lambda_3^{a_3} \\
&\cdots\cdots\cdots\cdots\cdots \\
\varepsilon_7 &= \pm \lambda_1^{g_1} \lambda_2^{f_2} \lambda_3^{e_3} \ldots \lambda_7^{a_7}.
\end{aligned}$$

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

VI. 33.
$$\Delta_\varepsilon = \begin{vmatrix}
l(\varepsilon_1), & l(\varepsilon_2), & l(\varepsilon_3), & l(\varepsilon_4), & l(\varepsilon_5), & l(\varepsilon_6), & l(\varepsilon_7) \\
l(\varepsilon_1), & l(\varepsilon_2), & l(\varepsilon_3), & -l(\varepsilon_4), & -l(\varepsilon_5), & -l(\varepsilon_6), & -l(\varepsilon_7) \\
-l(\varepsilon_1), & l(\varepsilon_2), & -l(\varepsilon_3), & l(\varepsilon_4), & -l(\varepsilon_5), & l(\varepsilon_6), & -l(\varepsilon_7) \\
l(\varepsilon_1), & -l(\varepsilon_2), & -l(\varepsilon_3), & l(\varepsilon_4), & l(\varepsilon_5), & -l(\varepsilon_6), & -l(\varepsilon_7) \\
-l(\varepsilon_1), & l(\varepsilon_2), & -l(\varepsilon_3), & -l(\varepsilon_4), & l(\varepsilon_5), & -l(\varepsilon_6), & l(\varepsilon_7) \\
-l(\varepsilon_1), & -l(\varepsilon_2), & l(\varepsilon_3), & l(\varepsilon_4), & -l(\varepsilon_5), & -l(\varepsilon_6), & l(\varepsilon_7) \\
l(\varepsilon_1), & -l(\varepsilon_2), & -l(\varepsilon_3), & -l(\varepsilon_4), & -l(\varepsilon_5), & l(\varepsilon_6), & l(\varepsilon_7)
\end{vmatrix} = 2^9 l(\varepsilon_1) l(\varepsilon_2) \cdot \ldots \cdot l(\varepsilon_7).$$

Si on désigne par Δ_λ le déterminant VI.7 relatif aux λ, les formules VI. 32 permettent d'écrire

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

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

VI. 34.
$$\Delta_\lambda = 2^9 l(\varepsilon_1) l(\varepsilon_2) \cdot \ldots \cdot l(\varepsilon_7).$$

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),

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

La formule VI. 16 donnant le nombre de classes devient

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

Mais on a, dans ce cas,

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

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

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

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

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

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

$$\text{VI. 38.} \qquad h = 2^{-15} h_1\, h_2 \cdot \ldots \cdot h_7 .$$

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

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

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

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

Il s'ensuit que le déterminant Δ_t, 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

$$\text{VI. 40.} \qquad h = 2^\rho\, h_1 h_2 \cdot \ldots \cdot h_7 .$$

Les formules VI.31, VI.38 et VI.40 sont résumées par le théorème suivant :

Théorème. *Le nombre de classes d'idéaux du corps* $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ *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 $\varphi(n)$, φ 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,

VII. 1. $$\varphi(n) \leq 8.$$

Cette inégalité entraîne les inégalités suivantes ** :

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

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

On déduit de ces inégalités

VII. 2. $$\begin{cases} n \leq [\varphi(n)]^2 & \text{si } n \text{ est impair,} \\ n \leq 2[\varphi(n)]^2 & \text{si } n \text{ est pair.} \end{cases}$$

* 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,

$$n \leqq 64 \qquad \text{si } n \text{ est impair,}$$
$$n \leqq 128 \qquad \text{si } n \text{ est pair.}$$

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

2, 3, 4, 5, . . . , 62, 63, 64 puis 66, 68, 70, . . . , 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 :

VII. 3.

n	$\varphi(n)$
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

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

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 $+ 1, \dfrac{-1+\sqrt{-3}}{2}, \dfrac{-1-\sqrt{-3}}{2}$

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

Racines cinquièmes $\dfrac{1}{4}\left[\sqrt{5}-1+i\sqrt{10}+2\sqrt{5}\right]$

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

Racines huitièmes $\dfrac{\sqrt{2}+\sqrt{-2}}{2}$

Racines dixièmes $\dfrac{1}{4}\left[\sqrt{5}+1+i\sqrt{10-2\sqrt{5}}\right]$

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

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

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

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

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

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

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

1) Tout corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ contient les racines carrées de l'unité.

2) Le corps $K\left(\sqrt{-1}, \sqrt{x}, \sqrt{y}\right)$, qui peut s'écrire plus explicitement, si l'on met en évidence la base du corps,

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

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

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

contient les racines $6^{\text{ièmes}}$ 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

$$x \text{ et } y \neq 2, \neq 3, \neq -1,$$
$$x \neq -y.$$

VII. 7. 4) Le corps $K\left(\sqrt{-3}, \sqrt{3}, \sqrt{y}\right)$ ou

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

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 seizièmes 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

$$K(1, \sqrt{-1}, \sqrt{x}, \sqrt{y}, \sqrt{-x}, \sqrt{xy}, \sqrt{-y}, \sqrt{-xy}) \text{ où } |x| \neq 2 \text{ et } 3 ; \quad |y| \neq 2 \text{ et } 3.$$

Ce corps contient les racines quatrièmes de l'unité $+1$, -1, $+i$ et $-i$.

Désignons par ρ l'une quelconque de ces quatre unités et posons, comme au chapitre V, formule V. 1,

VII. 9.
$$\begin{aligned} \eta_1 &= \rho_1 \lambda_1^a \\ \eta_2 &= \rho_2 \lambda_1^b \lambda_2^c \\ \eta_3 &= \rho_3 \lambda_1^d \lambda_2^e \lambda_3^f \end{aligned}$$

où ρ_1, ρ_2 et ρ_3 représentent des racines quatrièmes de l'unité, η_1, η_2 et η_3 trois unités fondamentales du sous-corps réel du quatrième degré (v. ch. V. 5) ; enfin λ_1, λ_2 et λ_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

VII. 10. $$\eta_1 = \rho_1 \lambda_1^a .$$

Appliquons à cette dernière égalité la permutation φ_1 qui laisse inchangé le sous-corps K_1 et, par suite, η_1

VII. 11. $$\eta_1 = \rho_1^{(1)} \lambda_1^{(1)a}.$$

Multiplions membre à membre les deux égalités VII. 10 et VII. 11, il vient

VII. 12 $$\eta_1^2 = \rho_1 \rho_1^{(1)} \left(\lambda_1 \lambda_1^{(1)}\right)^a.$$

Or, je dis que le produit $\rho_1 \rho_1^{(1)} = +1$. En effet, que ρ_1 soit égal à $+1$ ou à -1, la permutation φ_1 ne change pas ρ_1, et dès lors $\rho_1 \rho_1^{(1)} = \rho_1^2 = +1$.

Si au contraire $\rho_1 = +i$ ou $-i$, φ_1 change ρ_1 en $-\rho_1$ et $\rho_1 \rho_1^{(1)} = -i^2 = +1$.

L'égalité VII. 12 s'écrit donc $\eta_1^2 = \left(\lambda_1 \lambda_1^{(1)}\right)^a$, et la démonstration continue comme au chapitre V. On en conclut que les unités fondamentales du corps $K\left(\sqrt{-1}, \sqrt{x}, \sqrt{y}\right)$ sont encore données par les formules V. 12.

On a trouvé, pour le nombre de classes, quand le corps $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$ a trois unités fondamentales (v. formule VI. 17),

VII. 13. $$h = \frac{\sum_1 \sum_2 \ldots \sum_7 \sqrt{D}}{2^3 E \pi^4} .$$

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 λ_i,

$$\Delta_\lambda = \frac{2^k l(\varepsilon_1) l(\varepsilon_2) l(\varepsilon_3)}{a c f}$$

où k est un entier ordinaire et où ε_1, ε_2 et ε_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 $K\left(\sqrt{A}, \sqrt{B}, \sqrt{C}\right)$. Comme $u = 4 = 2^2$ et que acf est une puissance de

2, la formule VII. 13 peut s'écrire finalement comme suit :

$$h = \frac{2^l \sum_1 \sum_2 . \ \ldots \ . \sum_7 \sqrt{D_1} . \ \ldots \ . \sqrt{D_7}}{\pi^4 \, l(\varepsilon_1) \, l(\varepsilon_2) \, l(\varepsilon_3)}$$

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

$$h = 2^r \, h_1 \, h_2 . \ \ldots \ h_7$$

où r est un entier ordinaire.

7. Prenons, comme deuxième exemple, le corps VII. 6

$$K\left(1, \sqrt{-3}, \sqrt{x}, \sqrt{y}, \sqrt{-3x}, \sqrt{xy}, \sqrt{-3y}, \sqrt{-3xy}\right),$$

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 α l'une d'elles, le corps contient ± 1, $\pm \alpha$, $\pm \alpha^2$.

Posons de nouveau

VII. 14.
$$\begin{aligned} \eta_1 &= \rho_1 \lambda_1^a \\ \eta_2 &= \rho_2 \lambda_1^b \lambda_2^c \\ \eta_3 &= \rho_3 \lambda_1^d \lambda_2^e \lambda_3^f \end{aligned}$$

où ρ_1, ρ_2 et ρ_3 sont des racines sixièmes de l'unité.

Considérons la première des égalités VII. 14

$$\eta_1 = \rho_1 \lambda_1^a$$

et appliquons aux deux membres la permutation φ_1 ; l'égalité ci-dessus devient

$$\eta_1 = \rho_1 \lambda_1^{(1)a}.$$

La multiplication membre à membre des deux dernières égalités donne

VII. 15.
$$\eta_1^2 = \rho_1 \rho_1^{(1)} \left(\lambda_1 \lambda_1^{(1)}\right)^a.$$

Or, $\rho_1 = \dfrac{\pm 1 \pm \sqrt{-3}}{2}$; $\rho_1^{(1)} = \dfrac{\pm 1 \mp \sqrt{-3}}{2}$; $\rho_1 \rho_1^{(1)} = 1$.

L'égalité VII. 15 devient

$$\eta_1^2 = \left(\lambda_1 \lambda_1^{(1)}\right)^a.$$

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

$$h = \frac{3 \cdot 2^t \sum_1 \sum_2 \ldots \sum_7 \sqrt{D_1} \ldots \sqrt{D_7}}{\pi^4 \, l(\varepsilon_1) \, l(\varepsilon_2) \, l(\varepsilon_3)}$$

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 λ est l'un des nombres $1, \ldots, 7$, on voit que l'on a encore

$$h = 2^s h_1 \, h_2 \ldots h_7.$$

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 :

$$(1) \qquad \begin{cases} i_1^2 = i_2^2 = i_3^2 = -1 \\ i_1 i_2 = -i_2 i_1 = i_3 \\ i_2 i_3 = -i_3 i_2 = i_1 \\ i_3 i_1 = -i_1 i_3 = i_2. \end{cases}$$

Quand l'une des coordonnées a_λ 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 : $\qquad a = a_0 + a_2 i_2$

est le quaternion de coordonnées a_0, o, a_2 o.

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,...

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 $K\left(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps}\right)$, corps que nous avons étudié dans la première partie de ce travail **. Le corps $K\left(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps}\right)$ sera appelé, dans la suite, le *corps primordial* ***, et nous le représenterons par K.

Les qnaternions complexes à coordonnées tirées du corps primordial K seront désignés par des lettres grecques majuscules

$$\mathrm{A},\ \mathrm{B},\ \Gamma,\ \Delta,\ \ldots$$

Les coordonnées des quaternions complexes sont donc des nombres du corps primordial K ; ces coordonnées seront représentées par des lettres grecques minuscules

$$\alpha,\ \beta,\ \gamma,\ \delta,\ \ldots$$

Enfin, les nombres rationnels seront désignés par des lettres latines minuscules a, b, c, d, ...

Il résulte de la définition des quaternions complexes que l'un quelconque de ces derniers pourra s'écrire

$$\mathrm{A} = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3. \tag{2}$$

* 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 α_λ s'écrivent (v. 1re partie, ch. I) comme suit :

$$(3)\quad \left\{ \begin{array}{l} \alpha_\lambda = a_{\lambda,0} + a_{\lambda,1}\sqrt{apqs} + a_{\lambda,2}\sqrt{bqrs} + a_{\lambda,3}\sqrt{crps} + a_{\lambda,4}\sqrt{abrp} \\ \qquad + a_{\lambda,5}\sqrt{bcpq} + a_{\lambda,6}\sqrt{caqr} + a_{\lambda,7}\sqrt{abcs} \end{array} \right.$$

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

$$BA = \rho_0 + \rho_1 i_1 + \rho_2 i_2 + \rho_3 i_3 \quad \text{avec}$$

$$(6)\quad \left\{ \begin{array}{l} \rho_0 \equiv \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 \\ \rho_1 \equiv \alpha_1\beta_0 + \alpha_0\beta_1 + \alpha_3\beta_2 - \alpha_2\beta_3 \\ \rho_2 \equiv \alpha_2\beta_0 - \alpha_3\beta_1 + \alpha_0\beta_2 + \alpha_1\beta_3 \\ \rho_3 \equiv \alpha_3\beta_0 + \alpha_2\beta_1 - \alpha_1\beta_2 + \alpha_0\beta_3 \end{array} \right.$$

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 $\varphi_1, \varphi_2, \ldots, \varphi_7$ du corps primordial K (voir 1re partie ch. I. 4), on obtient les quaternions

$$\begin{aligned} A^{(1)} &= \alpha_0^{(1)} + \alpha_1^{(1)} i_1 + \alpha_2^{(1)} i_2 + \alpha_3^{(1)} i_3 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ A^{(7)} &= \alpha_0^{(7)} + \alpha_1^{(7)} i_1 + \alpha_2^{(7)} i_2 + \alpha_3^{(7)} i_3 \end{aligned}$$

D'autre part, en changeant les signes des trois dernières coordonnées de A, on obtient

$$\overline{A} = \alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3.$$

On constate que

$$\overline{A}A = A\overline{A} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.$$

Appliquons aussi au quaternion $\overline{A}$ les permutations $\varphi_1, \varphi_2, \ldots, \varphi_7$ du corps primordial K ; on obtient les sept quaternions

$$\begin{aligned} \overline{A}^{(1)} &= \alpha_0^{(1)} - \alpha_1^{(1)} i_1 - \alpha_2^{(1)} i_2 - \alpha_3^{(1)} i_3 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \overline{A}^{(7)} &= \alpha_0^{(7)} - \alpha_1^{(7)} i_1 - \alpha_2^{(7)} i_2 - \alpha_3^{(7)} i_3. \end{aligned}$$

Formons le produit

$$A\overline{A}\, A^{(1)}\overline{A}^{(1)}\, A^{(2)}\overline{A}^{(2)}. \ \ldots\ A^{(7)}\overline{A}^{(7)} \equiv No(A). \tag{7}$$

En vertu de la propriété associative de la multiplication, propriété qui subsiste pour les quaternions, l'égalité (7) peut s'écrire

$$No(A) = (A\overline{A})(A^{(1)}\overline{A}^{(1)}). \ \ldots\ . (A^{(7)}\overline{A}^{(7)})$$

ou encore

$$\left\{ \begin{aligned} No(A) = &\left(\alpha_0^{(2)} + \alpha_1^{(2)} + \alpha_2^{(2)} + \alpha_3^{(2)}\right)\left(\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}\right)\ldots \\ &\ldots\left(\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}\right). \end{aligned} \right. \tag{8}$$

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 :

$$No(A) = A\left(\overline{A}A^{(1)}\overline{A}^{(1)} \ldots A^{(7)}\overline{A}^{(7)}\right).$$

Le quaternion complexe

$$\widehat{\overline{\mathrm{A}}} \equiv \overline{\mathrm{A}}\overline{\mathrm{A}}^{(1)}\overline{\mathrm{A}}^{(1)}. \ \ldots \ \mathrm{A}^{(7)}\overline{\mathrm{A}}^{(7)} \tag{9}$$

sera dit le *conjugué* de A. Il peut s'écrire aussi

$$\widehat{\overline{\mathrm{A}}} = \left(\alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3\right)\left(\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}\right)\ldots$$
$$\ldots\left(\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}\right).$$

On peut écrire

$$\mathrm{A}\widehat{\overline{\mathrm{A}}} = \widehat{\overline{\mathrm{A}}}\mathrm{A} = No(\mathrm{A}).$$

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

$$\mathrm{A} = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3,$$
$$\mathrm{B} = \beta_0 + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3.$$

Formons le produit

$$\widehat{\overline{\mathrm{B}}}\widehat{\overline{\mathrm{A}}} = \left(\beta_0 - \beta_1 i_1 - \beta_2 i_2 - \beta_3 i_3\right)\left(\beta_0^{(1)2} + \beta_1^{(1)2} + \beta_2^{(1)2} + \beta_3^{(1)2}\right) \ \ldots \ \left(\beta_0^{(7)2} + \beta_1^{(7)2} + \beta_2^{(7)2} + \beta_3^{(7)2}\right)$$
$$\cdot\left(\alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3\right)\left(\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}\right) \ \ldots \ \left(\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}\right)$$

ce qui peut s'écrire encore

$$\begin{cases} \widehat{\overline{\mathrm{B}}}\widehat{\overline{\mathrm{A}}} = \left(\beta_0^{(1)2} + \beta_1^{(1)2} + \beta_2^{(1)2} + \beta_3^{(1)2}\right)\ldots\left(\beta_0^{(7)2} + \beta_1^{(7)2} + \beta_2^{(7)2} + \beta_3^{(7)2}\right) \\ \cdot\left(\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}\right)\ldots\left(\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}\right)\overline{\mathrm{B}}\,\overline{\mathrm{A}}. \end{cases} \tag{10}$$

Or, on a

$$\overline{\mathrm{B}}\,\overline{\mathrm{A}} = \pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3$$

où les π_λ ont les valeurs(5).

Si on désigne par π le produit des quatorze premiers facteurs du second membre de (10), l'égalité (10) s'écrit

$$\widehat{\overline{\mathrm{B}}}\widehat{\overline{\mathrm{A}}} = \pi(\pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3).$$

D'autre part, on a

$$\widehat{AB} = (\pi_0 - \pi_1 i_1 - \pi_2 i_2 - \pi_3 i_3)(\pi_0^{(1)2} + \pi_1^{(1)2} + \pi_2^{(1)2} + \pi_3^{(1)2}) \cdot \ldots \cdot (\pi_0^{(7)2} + \pi_1^{(7)2} + \pi_2^{(7)2} + \pi_3^{(7)2}),$$

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

$$\widehat{AB} = \widehat{B}\,\widehat{A}$$

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 Ω. Si Ω contient le quaternion Γ, 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)

$$No(A) = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}) \cdot \ldots \cdot (\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}).$$

Si le corps K est réel, α_0, α_1, α_2 et α_3 sont réels ; les nombres α_0^2, α_1^2, ... 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* Ω, *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 π_0, π_1, π_2 et π_3 ont les valeurs suivantes (v. formules 5) :

$$(10)\quad \begin{cases} \pi_0 = \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 \\ \pi_1 = \alpha_1\beta_0 + \alpha_0\beta_1 - \alpha_3\beta_2 + \alpha_2\beta_3 \\ \pi_2 = \alpha_2\beta_0 + \alpha_3\beta_1 + \alpha_0\beta_2 - \alpha_1\beta_3 \\ \pi_3 = \alpha_3\beta_0 - \alpha_2\beta_1 + \alpha_1\beta_2 + \alpha_0\beta_3. \end{cases}$$

Si le produit AB est nul, on a $\pi_0 = \pi_1 = \pi_2 = \pi_3 = 0$, c'est-à-dire

$$(11)\quad \begin{cases} \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 = 0 \\ \alpha_1\beta_0 + \alpha_0\beta_1 - \alpha_3\beta_2 + \alpha_2\beta_3 = 0 \\ \alpha_2\beta_0 + \alpha_3\beta_1 + \alpha_0\beta_2 - \alpha_1\beta_3 = 0 \\ \alpha_3\beta_0 - \alpha_2\beta_1 + \alpha_1\beta_2 + \alpha_0\beta_3 = 0. \end{cases}$$

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 β_0, β_1, β_2 et β_3 admette une solution $(\beta_0, \beta_1, \beta_2, \beta_3)$ non nulle ; et pour cela le déterminant Δ des coefficients des inconnues β_λ 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 :

$$(13)\quad \Delta = \left(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2\right)^2.$$

Comme, par hypothèse, A est un diviseur de zéro, sa norme est nulle, donc

$$(14)\quad \begin{cases} No(A) = \left(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2\right)\left(\alpha_0^{(1)2} + \alpha_1^{(1)2} + \alpha_2^{(1)2} + \alpha_3^{(1)2}\right)\ldots \\ \qquad \ldots\left(\alpha_0^{(7)2} + \alpha_1^{(7)2} + \alpha_2^{(7)2} + \alpha_3^{(7)2}\right) = 0. \end{cases}$$

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 θ fait partie du corps primordial K (voir 1re partie ch. I. 1),

$$\theta = a_0 + a_1\sqrt{apqs} + a_2\sqrt{bqrs} + \ldots + a_7\sqrt{abcs}.$$

Puisque θ est nul, on a $a_0 = a_1 = a_2 = \ldots = a_7 = 0$ et, par suite, les autres facteurs de No (A), facteurs qui sont les conjugués de θ 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

$$a_0 = a_1 = \ldots a_7 = 0.$$ Par suite $\theta = 0$ et tous les conjugués de θ 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 ΓA, on a

$$\Gamma A = \rho_0 + \rho_1 i_1 + \rho_2 i_2 + \rho_3 i_3, \quad \text{où l'on a posé (v. formules 6)}$$

$$(I) \qquad \begin{cases} \rho_0 = \alpha_0\gamma_0 - \alpha_1\gamma_1 - \alpha_2\gamma_2 - \alpha_3\gamma_3 \\ \rho_1 = \alpha_1\gamma_0 + \alpha_0\gamma_1 + \alpha_3\gamma_2 - \alpha_2\gamma_3 \\ \rho_2 = \alpha_2\gamma_0 - \alpha_3\gamma_1 + \alpha_0\gamma_2 + \alpha_1\gamma_3 \\ \rho_3 = \alpha_3\gamma_0 + \alpha_2\gamma_1 - \alpha_1\gamma_2 + \alpha_0\gamma_3 \end{cases}$$

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 α_λ, 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 $\Delta = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)^4$. On voit, comme dans le cas du produit AB, que quand A est un diviseur de zéro, le quaternion Γ existe tel que $\Gamma A = 0$.

8. *Réciproque d'un quaternion complexe.* Désignons par A un quaternion complexe non nul du domaine numéral Ω. Si A n'est pas diviseur de zéro, nous appellerons *réciproque* de A le quaternion $\frac{1}{No(A)}\,\hat{A}$, et nous écrirons $\frac{1}{No(A)}\,\hat{A} \equiv A^{-1}$. On voit que l'on a $AA^{-1} = A^{-1}A = 1$.

9. *Division des quaternions complexes.* Soit A un quaternion complexe non nul et qui ne soit pas diviseur de zéro. Si l'on a

$$\Lambda A = B,$$

Λ 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

$$A\Theta = B,$$

Θ 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* Ω. Adjoignons au quaternion complexe A du domaine Ω, 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 Ω 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* $\varphi_0, \varphi_1, \ldots, \varphi_7$ *du corps primordial K (v. ch. I. 4, première partie) sont également des permutations du domaine numéral* Ω.

11. Nous avons encore à introduire les définitions suivantes :

I. Etant donné le quaternion complexe

$$A \equiv \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \tag{16}$$

à coordonnées tirées du corps primordial K, nous appellerons *conjugué relatif* de A, et nous désignerons par $\overline{A}$, le quaternion complexe

$$\overline{A} \equiv \alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3. \tag{17}$$

II. Nous appellerons *norme relative* de A, et nous désignerons par $n(A)$, la quantité

$$n(A) \equiv A\overline{A} = \overline{A}A = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2. \tag{18}$$

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

$$\rho \equiv \frac{1 + i_1 + i_2 + i_3}{2}. \tag{21}$$

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^re^ partie, chap. II). Tout quaternion complexe à coordonnées tirées du corps primordial K pourra dès lors se mettre sous la forme suivante :

$$\mathrm{A} = A_0\omega_0 + A_1\omega_1 + A_2\omega_2 + \ldots + A_7\omega_7 \tag{22}$$

où les A_λ sont des quaternions rationnels.

Définition. Le quaternion complexe (22) sera dit un *quaternion complexe entier*, si les sept quaternions rationnels $A_0, \ldots, A_7$ sont des quaternions rationnels entiers.

Le quaternion complexe (22), supposé entier, peut s'écrire, en vertu de la définition précédente,

$$\mathrm{A} = \left(a_0^{(0)}\rho + a_1^{(0)}i_1 + a_2^{(0)}i_2 + a_3^{(0)}i_3\right)\omega_0 + \left(a_0^{(1)}\rho + a_1^{(1)}i_1 + a_2^{(1)}i_2 + a_2^{(1)}i_3\right)\omega_1 + \ldots$$
$$\ldots + \left(a_0^{(7)}\rho + a_1^{(7)}i_1 + a_2^{(7)}i_2 + a_3^{(7)}i_3\right)\omega_7,$$

ce qui peut s'écrire

$$\mathrm{A} = \alpha_0\rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \quad \text{où l'on a posé} \tag{23}$$

$$\begin{cases} \alpha_0 \equiv a_0^{(0)}\omega_0 + a_0^{(1)}\omega_1 + \ldots + a_0^{(7)}\omega_7 \\ \alpha_1 \equiv a_1^{(0)}\omega_0 + a_1^{(1)}\omega_1 + \ldots + a_1^{(7)}\omega_7 \\ \alpha_2 \equiv a_2^{(0)}\omega_0 + a_2^{(1)}\omega_1 + \ldots + a_2^{(7)}\omega_7 \\ \alpha_3 \equiv a_3^{(0)}\omega_0 + a_3^{(1)}\omega_1 + \ldots + a_3^{(7)}\omega_7. \end{cases} \tag{24}$$

On voit que les quatre nombres α_0, α_1, α_2 et α_3 sont des entiers dans le corps primordial K.

Soit A le quaternion (22) et désignons, comme plus haut, par $\overline{A}$ le conjugué relatif de A. On vérifie que l'on a

$$\overline{\mathrm{A}} = \alpha_0\rho - (\alpha_0 + \alpha_1)i_1 - (\alpha_0 + \alpha_2)i_2 - (\alpha_0 + \alpha_3)i_3. \tag{25}$$

On a, pour la norme relative de A,

$$n(\mathrm{A}) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_0(\alpha_1 + \alpha_2 + \alpha_3). \tag{26}$$

* Voir A. Hurwitz, *Zahlentheorie der Quaternionen*.

CHAPITRE II

Les idéaux dans le domaine numéral Ω.

12. Soit $\mathfrak{a}$ un idéal du corps primordial $K\left(\sqrt{apqs}, \sqrt{bqrs}, \sqrt{crps}\right)$. Nous appellerons *idéal du domaine numéral* Ω, et nous représenterons par $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$, l'ensemble infini de quaternions complexes entiers

$$\mathrm{A} = \alpha_0 \rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \tag{27}$$

dont les quatre coordonnées α_0, α_1, α_2 et α_3 parcourent, indépendamment les unes des autres, tous les nombres de l'idéal $\mathfrak{a}$. *

Dans l'expression (27), ρ est égal à

$$\frac{1 + i_1 + i_2 + i_3}{2}.$$

13. L'idéal $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$ du domaine numéral Ω sera dit un *idéal principal*, si $\mathfrak{a}$ est un idéal principal (α) dans le corps primordial K. Nous écrirons, dans ce cas,

$$\mathfrak{A} \equiv \mathrm{id}\,|(\alpha)|. \tag{28}$$

Il résulte de la définition de l'idéal principal dans le domaine numéral Ω, que tous les quaternions de l'idéal (28) sont de la forme

$$\mathrm{A} = \alpha\left(\xi_0 \rho + \xi_1 i_1 + \xi_2 i_2 + \xi_3 i_3\right)$$

où ξ_0, ξ_1, ξ_2 et ξ_3 sont des nombres entiers du corps primordial K.

Exemple : $\mathfrak{A} \equiv \mathrm{id}\,|(2)|$ contient tous les quaternions entiers dont les quatre coordonnées sont des multiples de 2 dans le corps primordial K. En d'autres termes, ξ_λ $(\lambda = 0, 1, 2, 3)$ désignant des nombres entiers quelconques du corps primordial K, tous les quaternions de l'idéal $\mathfrak{A} \equiv \mathrm{id}\,|(2)|$ du domaine numéral Ω ont la forme

$$2\xi_0 \rho + 2\xi_1 i_1 + 2\xi_2 i_2 + 2\xi_3 i_3 \quad \text{ou} \quad 2\left(\xi_0 \rho + \xi_1 i_1 + \xi_2 i_2 + \xi_3 i_3\right).$$

* Voir Boris Seitz : *Sur l'arithnomie 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 $\mathfrak{A} \equiv \mathrm{id}\,|(\alpha)|$ sont, dans le domaine numéral Ω, des multiples de α. Nous écrirons aussi l'idéal $\mathfrak{A}$ dans ce cas

(28) $$\mathfrak{A} = (\alpha).$$

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 Ω, savoir :

(29) $$\mathfrak{A} \equiv \mathrm{id}\,|(\alpha_0, \alpha_1, \alpha_2, \alpha_3)|.$$

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 α_0, α_2 et α_3, le quaternion A devient $A = \alpha_1 i_1$ et l'idéal $\mathfrak{A}$ s'écrit $\mathfrak{A} \equiv \mathrm{id}\,|(\alpha_1)|$ 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

$$A \equiv 0 \bmod \mathfrak{A}. **$$

15. *Produit de deux idéaux de quaternions complexes.* Soient $\mathfrak{A}$ et $\mathfrak{B}$ deux idéaux du domaine numéral Ω et posons

$$\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}| \quad \text{et} \quad \mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{b}|.$$

Nous appellerons *produit* de ces deux idéaux l'idéal

$$\mathfrak{C} \equiv \mathrm{id}\,|\mathfrak{c}|$$

comprenant tous les quaternions, et ceux-là seulement, dont les quatre coordonnées appartiennent à l'idéal $\mathfrak{c} \equiv \mathfrak{a}\,\mathfrak{b}$, du corps K. On voit que la multiplication des idéaux, ainsi définie dans le domaine numéral Ω, 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 Ω, A détermine un idéal $\mathfrak{A} \equiv \mathrm{id}\,|(a_0, a_1, a_2, a_3)|$. 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 α fait partie d'un idéal $\mathfrak{a}$, on écrit

$$\alpha \equiv 0 \bmod \mathfrak{a}.$$

En écrivant

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

nous généralisons la définition admise dans la théorie classique des idéaux.

16. *Divisibilité.* L'idéal $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$ sera dit *divisible par l'idéal* $\mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{b}|$ s'il existe un idéal $\mathfrak{C} \equiv \mathrm{id}\,|\mathfrak{c}|$ tel que l'on ait

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

On a alors, dans le corps primordial K,

$$\mathfrak{a} = \mathfrak{c}\,\mathfrak{b}.$$

Propriétés des idéaux.

17. Théorème. *La somme et la différence de deux nombres* A *et* B *de l'idéal* $\mathfrak{A} \equiv id\,|\mathfrak{a}|$ *font partie de cet idéal* $\mathfrak{A}$.

En effet, posons

$$A \equiv \alpha_0\rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \qquad B \equiv \beta_0\rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3.$$

Puisque, par hypothèse, A et B sont tous deux contenus dans $\mathfrak{A}$, on a

$$\alpha_r \equiv 0 \bmod \mathfrak{a} \quad \text{et} \quad \beta_r \equiv 0 \bmod \mathfrak{a} \quad \text{pour} \quad r = 0, 1, 2, 3. \tag{30}$$

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

$$\alpha_r \pm \beta_r \equiv 0 \bmod \mathfrak{a}\,; \quad \text{par suite}$$
$$A \pm B \equiv 0 \bmod \mathfrak{A}. \qquad \text{c. q. f. d.}$$

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* Ω *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* Ω, *sont également contenus dans l'idéal* $\mathfrak{A}$.

En effet, $A \equiv 0 \bmod \mathfrak{A}$ entraîne $\alpha_r \equiv 0 \bmod \mathfrak{a}$, pour $r = 0, 1, 2, 3$. Or, les coordonnées des produits AB et BA sont des combinaisons linéaires, à coefficients entiers, des coordonnées α_0, α_1, α_2 et α_3 avec les coordonnées de B (v. § 4, ch. I). Ces combinaisons linéaires sont donc des nombres de $\mathfrak{a}$ et par suite AB et BA font partie de l'idéal $\mathfrak{A}$.

19. Théorème. *Soit* $\mathfrak{A} \equiv id\,|\mathfrak{a}|$ *un idéal du domaine* Ω. *Si cet idéal contient le quaternion entier* A, *il contient aussi le conjugué relatif* $\overline{A}$ *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

$$A \equiv 0 \bmod \mathfrak{A} \qquad \text{et on en déduit}$$
$$\alpha_r \equiv 0 \bmod \mathfrak{a}, \qquad \text{pour } r = 0, 1, 2, 3.$$

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 $\overline{\mathrm{A}}$ (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, $n(\mathrm{A}) = \mathrm{A}\overline{\mathrm{A}}$ fait également partie de l'idéal $\mathfrak{A}$.

20. Théorème. *Tout idéal du domaine Ω admet une* BASE, *c'est-à-dire que l'on peut toujours trouver dans l'idéal huit nombres $\Gamma_1, \Gamma_2, \ldots, \Gamma_8$ tels que tout autre nombre de l'idéal considéré puisse se mettre sous la forme*

$$X_1\Gamma_1 + X_2\Gamma_2 + \ldots + X_8\Gamma_8,$$

où les X_r désignent des quaternions rationnels entiers. En outre si $\mathfrak{A} \equiv id\{\mathfrak{a}\}$, et si l'on désigne par $\gamma_1, \gamma_2, \ldots, \gamma_8$ une base de l'idéal $\mathfrak{a}$ du corps K, on pourra poser

$$\Gamma_1 \equiv \gamma_1\,; \quad \Gamma_2 = \gamma_2\,; \quad \ldots\,; \quad \Gamma_8 = \gamma_8\,.$$

Démonstration. Soit de nouveau

$$\mathrm{A} \equiv \alpha_0\rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$$

un nombre de l'idéal $\mathfrak{A} \equiv \mathrm{id}\{\mathfrak{a}\}$; on peut donc écrire, en vertu des hypothèses faites,

$$\alpha_r = x_1^{(r)}\gamma_1 + x_2^{(r)}\gamma_2 + \ldots + x_8^{(r)}\gamma_8 \quad \text{pour} \quad r = 0, 1, 2, 3,$$

les $x_\lambda^{(k)}$ étant des nombres entiers ordinaires. Dès lors, on a

$$\mathrm{A} = \left(x_1^{(0)}\gamma_1+\ldots+x_8^{(0)}\gamma_8\right)\rho+\left(x_1^{(1)}\gamma_1+\ldots+x_8^{(1)}\gamma_8\right)i_1+\ldots+\left(x_1^{(3)}\gamma_1+x_2^{(3)}\gamma_2+\ldots+x_8^{(3)}\gamma_8\right)i_3,$$

ou encore

$$\mathrm{A} = \left(x_1^{(0)}\rho+x_1^{(1)}i_1+x_1^{(2)}i_2+x_1^{(3)}i_3\right)\gamma_1+\ldots+\left(x_8^{(0)}\rho+x_8^{(1)}i_1+x_8^{(2)}i_2+x_8^{(3)}i_3\right)\gamma_8. \tag{31}$$

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 $\mathfrak{A} \equiv id\{\mathfrak{a}\}$ est divisible par $\mathfrak{B} \equiv id\{\mathfrak{b}\}$, 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 :

$$\alpha_r \equiv 0 \mod \mathfrak{a} \quad \text{pour} \quad r = 0, 1, 2, 3.$$

D'autre part, $\mathfrak{A}$ étant divisible par $\mathfrak{B}$ on a, dans le corps K,

$$a \equiv 0 \bmod \mathfrak{b}.$$

Dès lors, tout nombre de $\mathfrak{a}$ fait partie de $\mathfrak{b}$. On en conclut que $\alpha_r \equiv 0 \bmod \mathfrak{b}$ et, par suite, que $A \equiv 0 \bmod \mathfrak{B}$, ce qui démontre le théorème.

22. Théorème. *Etant donné un idéal $\mathfrak{A}$ du domaine Ω, il existe dans Ω un idéal $\mathfrak{B}$ tel que le produit $\mathfrak{AB}$ soit un idéal principal.*

Pour le démontrer, posons

$$\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|.$$

On sait trouver dans le corps K un idéal $\mathfrak{a}^{-1}$ tel que $\mathfrak{a}\mathfrak{a}^{-1} = (\alpha)$. Posons donc $\mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{a}^{-1}|$, et l'on aura $\mathfrak{AB} = \mathrm{id}\,|(\alpha)|$.

Nous écrirons par analogie

$$\mathfrak{A}^{-1} \equiv \mathrm{id}\,|\mathfrak{a}^{-1}|$$

et l'idéal $\mathfrak{A}^{-1}$ sera dit *le réciproque* de l'idéal $\mathfrak{A}$.

23. Théorème. *Un quaternion complexe entier $\Gamma \equiv \gamma_0\rho + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3$ ne peut être contenu que dans un nombre fini d'idéaux du domaine numéral Ω.*

Supposons que l'idéal $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$ contienne la norme relative de Γ, 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 Γ contient aussi $n(\Gamma)$ (v. th. 19) ; le nombre des idéaux du domaine Ω contenant Γ 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 Ω n'est divisible que par un nombre fini d'idéaux du même domaine.*

En effet, soit $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$ un idéal du domaine Ω et $\mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{b}|$ un diviseur de $\mathfrak{A}$. Désignons par A un nombre de $\mathfrak{A}$; d'après le théorème (21) on a $A \equiv 0 \bmod \mathfrak{B}$. 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 Ω ; l'égalité*

$$\mathfrak{AB} = \mathfrak{AC} \quad \textit{entraîne} \quad \mathfrak{B} = \mathfrak{C}.$$

* 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

$$\mathfrak{A}^{-1}\mathfrak{A} \equiv \mathrm{id}\,|(\alpha)| = (\alpha).$$

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, $ab = ac$ entraîne $b = c$.

26. Théorème. *Si tous les nombres d'un idéal* $\mathfrak{A} \equiv id\,|\mathfrak{a}|$ *sont congrus à zéro modulo un idéal* $\mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{b}|$, *l'idéal* $\mathfrak{A}$ *est divisible par l'idéal* $\mathfrak{B}$.

Soit de nouveau

$$A \equiv \alpha_0\rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$$

un quaternion de l'idéal $\mathfrak{A}$, quaternion arbitrairement choisi mais fixe. De l'hypothèse, combinée avec les définitions précédentes, on conclut

$$\alpha_r \equiv 0 \bmod \mathfrak{b}, \quad \text{pour} \quad r = 0, 1, 2, 3.$$

On en déduit

$$\mathfrak{a} \equiv 0 \bmod \mathfrak{b} \quad \text{et, par suite,}$$

$$\mathfrak{A} \equiv 0 \bmod \mathfrak{B}.$$

27. Soient $\mathfrak{A}$ et $\mathfrak{B}$ deux idéaux du domaine numéral Ω. 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 Ω. 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 Ω 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* $\mathfrak{D} \equiv id\,|\mathfrak{d}|$ *est le plus grand commun diviseur des deux idéaux* $\mathfrak{A} \equiv id\,|\mathfrak{a}|$ *et* $\mathfrak{B} \equiv id\,|\mathfrak{b}|$, *l'idéal* $\mathfrak{d}$ *est, dans le corps* K, *le plus grand commun diviseur des idéaux* $\mathfrak{a}$ *et* $\mathfrak{b}$. En effet, dans le domaine Ω, $\mathfrak{D}$ 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 $\mathfrak{a}$ et tous ceux de $\mathfrak{b}$.

* Voir D. Hilbert, op. cit., chap. II.

29. *Définitions.* I. L'idéal unité dans le domaine Ω des quaternions complexes est l'idéal $\mathfrak{U} \equiv \mathrm{id}\,|(1)| \equiv (1)$. Cet idéal contient le nombre 1 et, par suite, tous les quaternions entiers de Ω.

II. Un idéal $\mathfrak{P} \equiv \mathrm{id}\,|\mathfrak{p}|$ de Ω 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 $\mathfrak{p}$ est premier dans le corps primordial K.

30. Théorème. *Si le produit $\mathfrak{AB}$ de deux idéaux du domaine Ω est divisible par un idéal premier $\mathfrak{P}$, l'un au moins des facteurs est divisible par $\mathfrak{P}$.*

Démonstration. Prenons

$$\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|\,; \qquad \mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{b}|\,; \qquad \mathfrak{P} \equiv \mathrm{id}\,|\mathfrak{p}|\,.$$

Dans le corps K, $\mathfrak{p}$ est un idéal premier. Il ressort des définitions posées que si $\mathfrak{AB}$, dans le domaine Ω, est divisible par $\mathfrak{P}$, $\mathfrak{ab}$ doit être divisible par $\mathfrak{p}$ dans le corps K ; et l'on sait par la théorie classique des corps algébriques que, dans ce cas, $\mathfrak{a}$ ou $\mathfrak{b}$ est divisible par $\mathfrak{p}$. On a donc l'une des trois alternatives suivantes :

$\mathfrak{a} \equiv 0 \bmod \mathfrak{p}$,	ce qui entraîne	$\mathfrak{A} \equiv 0 \bmod \mathfrak{P}$;
$\mathfrak{b} \equiv 0 \bmod \mathfrak{p}$,	ce qui entraîne	$\mathfrak{B} \equiv 0 \bmod \mathfrak{P}$;
$\mathfrak{a} \equiv 0 \bmod \mathfrak{p}$ et $\mathfrak{b} \equiv 0 \bmod \mathfrak{p}$,	ce qui entraîne	$\mathfrak{A} \equiv 0$ $\mathfrak{B} \equiv 0 \bmod \mathfrak{P}$.

31. Théorème fondamental. *Tout idéal $\mathfrak{A}$ du domaine numéral Ω peut être décomposé, et cela d'une seule manière, en un produit d'un nombre fini d'idéaux premiers du domaine Ω.*

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 :

$$\mathfrak{A} = \mathfrak{P}_1 \mathfrak{P}_2 . \ \ldots \ . \mathfrak{P}_r\,;$$
$$\mathfrak{A} = \mathfrak{Q}_1 \mathfrak{Q}_2 . \ \ldots \ . \mathfrak{Q}_s .$$

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

$$\mathfrak{P}_2 \mathfrak{P}_3 . \ \ldots \ \mathfrak{P}_r = \mathfrak{Q}_2 \mathfrak{Q}_3 . \ \ldots \ \mathfrak{Q}_s .$$

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 Ω.

32. Des définitions posées plus haut, il résulte que

1. tout entier du domaine Ω est congru à lui-même suivant un idéal quelconque, puisque tout idéal contient le nombre zéro ;
2. la congruence $A \equiv B \bmod \mathfrak{A}$ entraîne $B \equiv A \bmod \mathfrak{A}$;
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 Ω 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 Ω 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 *No* ($\mathfrak{A}$).

33. Théorème. *Pour que deux quaternions complexes entiers du domaine numéral* Ω, *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 $\mathfrak{A} \equiv id\{a\}$, *il faut et il suffit que l'on ait, dans le corps primordial* K, *les congruences suivantes* :

$$\alpha_\lambda \equiv \beta_\lambda \bmod a \quad \text{pour} \quad \lambda = 0, 1, 2, 3.$$

Démonstration. 1) La condition est nécessaire, car pour que l'on ait $A \equiv B \bmod \mathfrak{A}$, il faut que $A - B \equiv 0 \bmod \mathfrak{A}$.

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

$$\alpha_r \equiv \beta_r \bmod \mathfrak{a} \quad \text{pour} \quad r = 0, 1, 2, 3.$$

2) La condition est suffisante car, si $\alpha_r \equiv \beta_r \bmod \mathfrak{a}$ pour $r = 0, 1, 2, 3$, l'idéal $\mathfrak{a}$ contient $\alpha_r - \beta_r$ pour $r = 0, 1, 2, 3$, et on a

$$(\alpha_0 - \beta_0)\rho + (\alpha_1 - \beta_1) i_1 + (\alpha_2 - \beta_2) i_2 + (\alpha_3 - \beta_3) i_3 \equiv 0 \bmod \mathfrak{A}.$$

Or, le premier membre n'est autre que A — B, et le théorème est démontré.

34. Théorème. *Soit donné, dans le domaine* Ω, *un idéal* $\mathfrak{A} \equiv id\,|\mathfrak{a}|$; *désignons par* $n_k(\mathfrak{a})$ *la norme de l'idéal* $\mathfrak{a}$ *dans le corps* K, *c'est-à-dire le nombre des éléments d'un système complet de restes modulo* $\mathfrak{a}$ *dans le corps* K ; *je dis qu'un système complet de restes modulo* $\mathfrak{A}$, *dans le domaine* Ω, *comprend* $[n_k(\mathfrak{a})]^4$ *nombres.* C'est la norme $No(\mathfrak{A})$ de l'idéal de quaternions complexes $\mathfrak{A}$, et nous écrirons $No(\mathfrak{A}) = [n_k(\mathfrak{a})]^4$.

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 Ω ; faisons parcourir aux coordonnées α_r, indépendamment les unes des autres, les $n_k(\mathfrak{a})$ nombres d'un système complet de restes modulo $\mathfrak{a}$. On obtient ainsi $[n_k(\mathfrak{a})]^4$ quaternions. On voit tout de suite qu'ils sont incongrus entre eux mod $\mathfrak{A}$ où $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$ et, de plus, que tout autre quaternion entier de Ω est congru, modulo $\mathfrak{A}$, à l'un de ces $[n_k(\mathfrak{a})]^4$ quaternions.

35. Théorème. *Soit* $n(\mathfrak{p}) = p^e$ *la norme de l'idéal premier* $\mathfrak{p}$ *dans le corps* K ; *on a, dans le domaine* Ω, $No(\mathfrak{P}) = p^{4e}$.

Cela résulte du théorème 34.

36. Théorème. *Si* $A \equiv B$ *mod* $\mathfrak{A}$ *et* $\Gamma \equiv \Delta$ *mod* $\mathfrak{A}$, *on a aussi*

$$A \pm \Gamma \equiv B \pm \Delta \quad \textit{mod}\ \mathfrak{A}. \tag{32}$$

Pour le démontrer, posons

$$\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|, \quad A \equiv \alpha_0\rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3, \quad B \equiv \beta_0\rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3.$$
$$\Gamma \equiv \gamma_0\rho + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3, \quad \Delta \equiv \delta_0\rho + \delta_1 i_1 + \delta_2 i_2 + \delta_3 i_3.$$

De $A \equiv B \bmod \mathfrak{A}$, on déduit

$$\alpha_r \equiv \beta_r \bmod \mathfrak{a}, \text{ pour } r = 0, 1, 2, 3. \tag{33}$$

De $\Gamma \equiv \Delta \bmod \mathfrak{A}$, on déduit

$$\gamma_r \equiv \delta_r \bmod \mathfrak{a}, \text{ pour } r = 0, 1, 2, 3. \tag{34}$$

Les congruences (33) et (34) donnent, en vertu des propriétés connues des congruences dans les corps algébriques,

$$\alpha_r \pm \gamma_r \equiv \beta_r \pm \delta_r \bmod a,$$

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* Ω, *les deux membres d'une congruence suivant un idéal de* Ω.

Car, si $A \equiv B \bmod \mathfrak{A}$, on a $A - B \equiv 0 \bmod \mathfrak{A}$ et, en vertu du théorème 18, les quaternions

$M(A - B)$ et $(A - B)M$, où M représente un quaternion entier de Ω, sont congrus à zéro modulo $\mathfrak{A}$, quel que soit l'entier M. Il en résulte bien

$$MA \equiv MB \text{ et } AM \equiv BM \bmod \mathfrak{A}.$$

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* Ω.

Soient les deux congruences

$$A \equiv B \bmod \mathfrak{A} \quad \text{et} \quad \Gamma \equiv \Delta \bmod \mathfrak{A}. \tag{35}$$

Ecrivons explicitement les quaternions qui figurent dans les congruences (35) :

$$A \equiv \alpha_0\rho + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 = \frac{1}{2}\left[\alpha_0 + (\alpha_0 + 2\alpha_1)i_1 + (\alpha_0 + 2\alpha_2)i_2 + (\alpha_0 + 2\alpha_3)i_3\right];$$

$$B \equiv \beta_0\rho + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3 = \frac{1}{2}\left[\beta_0 + (\beta_0 + 2\beta_1)i_1 + (\beta_0 + 2\beta_2)i_2 + (\beta_0 + 2\beta_3)i_3\right];$$

$$\Gamma \equiv \gamma_0\rho + \gamma_1 i_1 + \gamma_2 i_2 + \gamma_3 i_3 = \frac{1}{2}\left[\gamma_0 + (\gamma_0 + 2\gamma_1)i_1 + (\gamma_0 + 2\gamma_2)i_2 + (\gamma_0 + 2\gamma_3)i_3\right];$$

$$\Delta \equiv \delta_0\rho + \delta_1 i_1 + \delta_2 i_2 + \delta_3 i_3 = \frac{1}{2}\left[\delta_0 + (\delta_0 + 2\delta_1)i_1 + (\delta_0 + 2\delta_2)i_2) + (\delta_0 + 2\delta_3)i_3\right].$$

Effectuons les produits $A\Gamma$ et $B\Delta$ en appliquant les formules (5). On obtient, tous calculs faits,

$$\begin{aligned} A\Gamma = {} & (\alpha_0\gamma_0 - \alpha_0\gamma_1 - \alpha_0\gamma_2 - \alpha_0\gamma_3 - \alpha_1\gamma_0 - 2\alpha_1\gamma_1 - \alpha_2\gamma_0 - 2\alpha_2\gamma_2 - \alpha_3\gamma_0 - 2\alpha_3\gamma_3)\rho \\ & + (\alpha_0\gamma_0 + \alpha_0\gamma_1 + \alpha_0\gamma_3 + \alpha_1\gamma_0 + \alpha_1\gamma_1 + \alpha_2\gamma_0 + \alpha_2\gamma_2 + \alpha_2\gamma_3 - \alpha_3\gamma_2 + \alpha_3\gamma_3)\, i_1 \\ & + (\alpha_0\gamma_0 + \alpha_0\gamma_1 + \alpha_0\gamma_2 + \alpha_1\gamma_1 - \alpha_1\gamma_3 + \alpha_2\gamma_0 + \alpha_2\gamma_2 + \alpha_3\gamma_0 + \alpha_3\gamma_1 + \alpha_3\gamma_3)\, i_2 \\ & + (\alpha_0\gamma_0 + \alpha_0\gamma_2 + \alpha_0\gamma_3 + \alpha_1\gamma_0 + \alpha_1\gamma_1 + \alpha_1\gamma_2 - \alpha_2\gamma_1 + \alpha_2\gamma_2 + \alpha_3\gamma_0 + \alpha_3\gamma_3)\, i_3 \end{aligned}$$

et de même

$$\begin{aligned}B\Delta = {} & (\beta_0\delta_0 - \beta_0\delta_1 - \beta_0\delta_2 - \beta_0\delta_3 - \beta_1\delta_0 - 2\beta_1\delta_1 - \beta_2\delta_0 - 2\beta_2\delta_2 - \beta_3\delta_0 - 2\beta_3\delta_3)\,\rho \\ & + (\beta_0\delta_0 + \beta_0\delta_1 + \beta_0\delta_3 + \beta_1\delta_0 + \beta_1\delta_1 + \beta_2\delta_0 + \beta_2\delta_2 + \beta_2\delta_3 - \beta_3\delta_2 + \beta_3\delta_3)\,i_1 \\ & + (\beta_0\delta_0 + \beta_0\delta_1 + \beta_0\delta_2 + \beta_1\delta_1 - \beta_1\delta_3 + \beta_2\delta_0 + \beta_2\delta_2 + \beta_3\delta_0 + \beta_3\delta_1 + \beta_3\delta_3)\,i_2 \\ & + (\beta_0\delta_0 + \beta_0\delta_2 + \beta_0\delta_3 + \beta_1\delta_0 + \beta_1\delta_1 + \beta_1\delta_2 - \beta_2\delta_1 + \beta_2\delta_2 + \beta_3\delta_0 + \beta_3\delta_3)\,i_3.\end{aligned}$$

Or, on peut écrire, en vertu des congruences (35),

$$\alpha_r \equiv \beta_r \bmod \mathfrak{a} \quad \text{pour} \quad r = 0, 1, 2, 3 ;$$
$$\gamma_s \equiv \delta_s \bmod \mathfrak{a} \quad \text{pour} \quad s = 0, 1, 2, 3.$$

Il en résulte, en vertu des propriétés connues des congruences dans les corps algébriques,

$$\alpha_r\gamma_s \equiv \beta_r\delta_s \bmod \mathfrak{a} \quad \text{pour} \quad r \text{ et } s = 0, 1, 2, 3. \tag{36}$$

Si on forme alors la différence $A\Gamma - B\Delta$, on voit que l'on a, en vertu des congruences (36),

$$A\Gamma - B\Delta \equiv 0 \bmod \mathfrak{A}$$

d'où

$$A\Gamma \equiv B\Delta \bmod \mathfrak{A}.$$

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

$$A \equiv B \bmod \mathfrak{A} \tag{37}$$

entraîne ces deux autres congruences

$$\overline{A} \equiv \overline{B} \bmod \mathfrak{A} ; \tag{38}$$

$$n(A) \equiv n(B) \bmod \mathfrak{A}. \tag{39}$$

Pour le démontrer, on pose

$$\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|.$$

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 $\overline{A}$ sont permutables entre eux.

40. Théorème. *Soit, dans le domaine numéral* Ω, *la congruence* $A \equiv B \bmod \mathfrak{A}$. *Si* Γ *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* Γ, *à condition que, dans le domaine* Ω, *l'idéal principal* $id\,|n(\Gamma)|$ *soit premier avec* $\mathfrak{A}$.

Démonstration. Soit $\mathfrak{A} \equiv id\,|\mathfrak{a}|$. Supposons que Γ soit un diviseur commun à droite de A et B et posons

$$A = A^*\Gamma, \qquad B = B^*\Gamma.$$

La congruence de l'énoncé peut s'écrire dès lors

$$A^*\Gamma \equiv B^*\Gamma \bmod \mathfrak{A} \qquad \text{ou}$$

$$(A^* - B^*)\Gamma \equiv 0 \bmod \mathfrak{A}. \tag{40}$$

Multiplions les deux membres de cette dernière congruence (v. th. 38) par $\overline{\Gamma}$; on obtient

$$(A^* - B^*)\,n(\Gamma) \equiv 0 \bmod \mathfrak{A}$$

où $n(\Gamma)$ désigne la norme relative de Γ (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 :

$$(A^* - B^*)\gamma \equiv 0 \bmod \mathfrak{A}. \tag{41}$$

Désignons par α_0, α_1, α_2 et α_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 (γ) est premier avec $\mathfrak{a}$, c'est-à-dire si, dans le domaine Ω, l'idéal $id\,|(\gamma)| = id\,|n(\Gamma)|$ est premier avec l'idéal $\mathfrak{A} \equiv id\,|\mathfrak{a}|$, les nombres α_0, α_1, α_2 et α_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

$$A^* - B^* \equiv 0 \bmod \mathfrak{A}$$

ou

$$A^* \equiv B^* \bmod \mathfrak{A}. \qquad \text{c. q. f. d.}$$

41. Théorème. *Si les quaternions complexes entiers* $\Gamma_1, \Gamma_2, \ldots, \Gamma_r$, *dont le nombre est* $r \equiv No\,(\mathfrak{A})$, *forment dans le domaine* Ω *un système complet de restes modulo* $\mathfrak{A}$; *si de plus* A *est un quaternion complexe entier du domaine* Ω *tel que* $id\,|n\,(A)|$ *soit premier avec* $\mathfrak{A}$, *les quaternions*

$$\Gamma_1 A, \Gamma_2 A, \ldots, \Gamma_r A \tag{42}$$

forment également un système complet de restes modulo $\mathfrak{A}$. *Il en est de même des quaternions*

$$\text{(43)} \qquad A\Gamma_1,\ A\Gamma_2,\ \ldots,\ A\Gamma_r\ .$$

Démonstration. Tout d'abord, les quaternions (42) sont en nombre égal aux quaternions Γ_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,

$$\Gamma_a A \equiv \Gamma_b A \bmod \mathfrak{A},$$

ou

$$(\Gamma_a - \Gamma_b) A \equiv 0 \bmod \mathfrak{A},$$

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 id $|n(A)|$ est premier avec $\mathfrak{A}$,

$$\Gamma_a - \Gamma_b \equiv 0 \bmod \mathfrak{A},$$

ce qui serait contraire à l'hypothèse puisque Γ_a et Γ_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 $\qquad No(\mathfrak{A}\mathfrak{B}) = No(\mathfrak{A}).\ No(\mathfrak{B}).$

Posons $\qquad \mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|, \quad \mathfrak{B} \equiv \mathrm{id}\,|\mathfrak{b}|.$

Appliquons le théorème 34, on obtient

$$No(\mathfrak{A}\mathfrak{B}) = [n_k(\mathfrak{a}\mathfrak{b})]^4 = [n_k(\mathfrak{a})]^4\,[n_k(\mathfrak{b})]^4 = No(\mathfrak{A}).\,No(\mathfrak{B})$$

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* Ω, *quaternion dont la norme relative* $n(A)$ *est première avec l'idéal* $\mathfrak{A} \equiv id\,|\mathfrak{a}|$, *on a la relation*

$$[n(A)]^{\Phi(\mathfrak{A})} \equiv 1 \bmod \mathfrak{A}.$$

* Dans le domainel numéra Ω.

Démonstration. Considérons, dans le domaine Ω, les éléments d'un système complet de restes modulo $\mathfrak{A}$, et soient $B_1, B_2, \ldots, B_t$, où $t \equiv \Phi(\mathfrak{A})$, ceux d'entre eux dont la norme relative est première avec $\mathfrak{A}$. Déterminons les quaternions complexes entiers

$$\Lambda_1, \Lambda_2, \ldots, \Lambda_t$$

tels que

$$(44) \qquad \left.\begin{array}{l} A\,B_1 \equiv \Lambda_1 \\ A\,B_2 \equiv \Lambda_2 \\ \ldots\ldots\ldots \\ A\,B_t \equiv \Lambda_t \end{array}\right\} \bmod \mathfrak{A}$$

où A est le quaternion dont parle l'énoncé. Les Λ_r sont incongrus entre eux modulo $\mathfrak{A}$, car $\Lambda_k \equiv \Lambda_r \bmod \mathfrak{A}$, où Λ_k et Λ_r sont deux des quaternions $\Lambda_1, \ldots, \Lambda_t$, entraînerait $B_k \equiv B_r \bmod \mathfrak{A}$ (en vertu des congruences (44) et du théorème § 40).

Je dis que les idéaux

$$\mathrm{id}\,\{n(\Lambda_1)\}, \ldots, \mathrm{id}\,\{n(\Lambda_t)\}$$

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),

$$n(\Lambda_1) \equiv \lambda_1, \quad n(\Lambda_2) \equiv \lambda_2, \quad \ldots, \quad n(\Lambda_t) \equiv \lambda_t.$$

Il s'agit donc de démontrer que les idéaux

$$\mathrm{id}\,\{(\lambda_k)\}, \text{ pour } k = 1, 2, \ldots, t$$

sont premiers avec l'idéal

$$\mathfrak{A} \equiv \mathrm{id}\,\{a\}.$$

Supposons que les deux idéaux $\mathrm{id}\,\{(\lambda_k)\}$ où k est l'un des indices 1, 2, $\ldots, t$, et $\mathfrak{A} \equiv \mathrm{id}\,\{a\}$ aient un facteur premier commun $\mathfrak{P}$; on peut écrire

$$\mathrm{id}\,\{(\lambda_k)\} = \mathfrak{B}\,\mathfrak{P} \quad \text{et} \quad \mathfrak{A} = \mathfrak{A}^*\,\mathfrak{P}.$$

Posons encore

$$\mathfrak{B} \equiv \mathrm{id}\,\{b\}, \quad \mathfrak{P} \equiv \mathrm{id}\,\{p\}, \quad \mathfrak{A}^* \equiv \mathrm{id}\,\{a^*\}.$$

On a donc

$$\mathrm{id}\,\{(\lambda_k)\} = \mathrm{id}\,\{b\}\ \mathrm{id}\,\{p\}.$$

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 :

$$(45) \qquad (\lambda_k) = b\,p.$$

Mais λ_k est la norme relative de $\Lambda_k = A\,B_k$. On a donc (v. § 11)

$$\lambda_k = \Lambda_k \overline{\Lambda_k} = AB_k \cdot \overline{AB_k} = AB_k \overline{B_k}\,\overline{A_k} = n(A)\,n(B_k).$$

Posons $\qquad n(A) \equiv \alpha, \qquad n(B_k) \equiv \beta_k.$

L'égalité (45) s'écrit alors

$$(\lambda_k) = (\alpha)(\beta_k) = \mathfrak{b}\mathfrak{p}. \tag{46}$$

Mais, par hypothèse, l'idéal id $|n(A)|$ ou id $|(\alpha)|$ est premier avec l'idéal $\mathfrak{A} \equiv \mathrm{id}\,|\mathfrak{a}|$. Il en résulte que, dans le corps K, l'idéal (α) est premier avec l'idéal $\mathfrak{a}$; (α) n'est donc pas divisible par l'idéal premier $\mathfrak{p}$ qui divise $\mathfrak{a}$. L'égalité (46) montre que l'idéal (β_k) devrait être divisible par $\mathfrak{p}$. Mais, si c'était le cas, l'idéal id $|(\beta_k)|$ ou id $|n(B_k)|$ serait divisible par 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

$$\mathrm{id}\,|n(\Lambda_k)| \quad \text{pour } k = 1, 2, \ldots, t$$

sont premiers avec $\mathfrak{A}$ et que les quaternions

$$\Lambda_1, \Lambda_2, \ldots, \Lambda_t$$

sont congrus, modulo $\mathfrak{A}$, aux quaternions de la suite

$$B_1, B_2, \ldots, B_t,$$

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,

$$n(AB_1) \cdot n(AB_2) \cdot \ldots n(AB_t) \equiv n(\Lambda_1) \cdot n(\Lambda_2) \cdot \ldots n(\Lambda_t) \bmod \mathfrak{A}$$

ou, puisque $n(AB_k) = n(A) \cdot n(B_k)$,

$$[n(A)]^t \cdot n(B_1) \cdot \ldots n(B_t) \equiv n(\Lambda_1) \cdot \ldots n(\Lambda_t) \bmod \mathfrak{A}. \tag{47}$$

Mais l'ensemble des Λ_k coïncidant avec l'ensemble des B_k et, d'autre part, les idéaux

$$\mathrm{id}\,|n(B_k)| \text{ et id } |n(\Lambda_k)| \text{ pour } k = 1, 2, \ldots, t$$

étant premiers avec $\mathfrak{A}$, on déduit de la congruence (47)

$$[n(A)]^t \equiv 1 \bmod \mathfrak{A}$$

ou

$$[n(A)]^{\Phi(\mathfrak{A})} \equiv 1 \bmod \mathfrak{A}.$$

C'est le théorème de Fermat généralisé au domaine Ω des quaternions complexes.

TABLE DES MATIÈRES