JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

E.-E. KUMMER

Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers

Journal de mathématiques pures et appliquées 1re série, tome 16 (1851), p. 377-498.
<http://www.numdam.org/item?id=JMPA_1851_1_16__377_0>

MÉMOIRE

Sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers;

PAR M. E.-E. KUMMER,
Professeur de Mathématiques à l'Université de Breslau, en Silésie.

Dans l'état actuel de la science, on entend généralement par nombre complexe une fonction entière, à coefficients entiers, des racines irrationnelles d'une ou de plusieurs équations algébriques dont les coefficients sont également des nombres entiers. Le produit de tous les nombres complexes qu'on déduit d'un d'entre eux en changeant les racines des équations qu'il contient, étant une fonction symétrique de ces racines, sera toujours délivré de toute irrationnalité. Ce produit, qu'on appelle la *norme* du nombre complexe, sera donc un nombre entier; et, par conséquent, tout nombre complexe sera facteur irrationnel d'un nombre entier. De même, si l'on prend les coefficients du nombre complexe pour des indéterminés, la norme représentera une forme homogène d'un certain degré, du genre de celles qui sont décomposables en facteurs linéaires. La théorie des nombres complexes revient, au fond, à la théorie de ces formes, et, à cet égard, elle fait partie d'une des plus belles branches de l'Arithmétique supérieure. C'est sous ce point de vue que M. Lejeune-Dirichlet a fait des recherches très-générales sur les formes de degrés quelconques qui dépendent des normes des nombres complexes. Il a jeté les fondements de cette théorie en découvrant les propriétés générales de ces formes; mais, malheureusement, il n'en a publié jusqu'à présent que quelques-uns des résultats principaux, en ne donnant que des notions générales sur les principes nouveaux dont il s'est servi pour y parvenir. D'un autre côté, la théorie des nombres complexes peut être con-

sidérée comme la théorie de la décomposition des nombres en facteurs irrationnels, et c'est sous ce point de vue qu'elle a un grand intérêt, aussi bien en elle-même que pour les applications nombreuses et importantes qu'on en a faites dans plusieurs questions relatives à l'Arithmétique et à l'Algèbre supérieure.

Je ne traiterai, dans ce Mémoire, que les nombres complexes dont les irrationnalités sont les racines imaginaires de l'unité ou de l'équation binôme

$$\alpha^{\lambda} = 1,$$

genre spécial de nombres complexes, mais duquel l'importance pour la théorie générale est comparable à celle qu'il faut attribuer à la solution de l'équation binôme pour les équations algébriques les plus générales. La théorie de ces nombres complexes a été depuis longtemps le sujet de mes recherches, que j'ai publiées dans les *Comptes rendus de l'Académie de Berlin* et dans le Journal de M. Crelle [*]. En reprenant ici cette matière, j'ai en vue de compléter et de réunir la substance principale de ces divers Mémoires pour en former un Traité entier et continu qui puisse servir de base sûre à des recherches ultérieures dans cette partie de la théorie des nombres. J'ajouterai aussi deux applications des nombres complexes, dont l'une se rapporte à la théorie de la division du cercle, l'autre à la démonstration du dernier théorème de Fermat.

§ I.

Définitions et théorèmes préliminaires.

Les nombres complexes dont nous nous occuperons dans ce Mémoire sont des fonctions rationnelles et entières, à coefficients entiers, d'une racine imaginaire de l'équation

$$\alpha^{\lambda} = 1,$$

λ étant un nombre premier impair. A l'aide de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

[*] Rappelons aussi les premiers essais, déjà très-intéressants, que M. Kummer avait consignés dans un Mémoire imprimé d'abord à Breslau, en 1844, et inséré depuis au tome XII du présent Journal. (J. Liouville.)

qui contient toutes les racines imaginaires de l'équation $\alpha^\lambda = 1$, un nombre complexe $f(\alpha)$ est toujours réductible à la forme

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2},$$

a, a_1, a_2,..., $a_{\lambda-2}$ étant des nombres entiers. On démontre aisément que cette réduction ne pourrait être effectuée que d'une seule manière; car, si l'on avait

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2}$$

et

$$f(\alpha) = b + b_1\alpha + b_2\alpha^2 + \ldots + b_{\lambda-2}\alpha^{\lambda-2},$$

on en conclurait

$$a - b + (a_1 - b_1)\alpha + (a_2 - b_2)\alpha^2 + \ldots + (a_{\lambda-2} - b_{\lambda-2})\alpha^{\lambda-2} = 0,$$

équation qui ne peut pas subsister à cause de l'irréductibilité de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0.$$

En prenant pour α successivement toutes les racines différentes, que nous représenterons comme puissances de l'une d'elles par α, α^2, α^3,..., $\alpha^{\lambda-1}$, on obtient les $\lambda - 1$ nombres complexes

$$f(\alpha),\quad f(\alpha^2),\quad f(\alpha^3),\ldots,\quad f(\alpha^{\lambda-1}),$$

que nous appellerons *nombres complexes conjugués*. Deux nombres conjugués, tels que $f(\alpha^n)$ et $f(\alpha^{-n})$, dont les racines sont réciproques, seront appelés *nombres complexes réciproques*.

Le produit de tous les nombres conjugués

$$f(\alpha),\quad f(\alpha^2),\quad f(\alpha^3),\ldots,\quad f(\alpha^{\lambda-1}),$$

étant une fonction symétrique de toutes les racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

se réduit à un nombre rationnel et entier qui, suivant M. Lejeune-Dirichlet, sera appelé la *norme* du nombre complexe $f(\alpha)$, et qui sera

désigné par la lettre N, en sorte qu'on ait

$$\mathrm{N}f(\alpha) = f(\alpha) \cdot f(\alpha^2) \cdot f(\alpha^3) \ldots f(\alpha^{\lambda-1}).$$

Il suit immédiatement de la définition :

1°. Que les nombres conjugués ont tous la même norme

$$\mathrm{N}f(\alpha^k) = \mathrm{N}f(\alpha);$$

2°. Que la norme du produit de deux ou de plusieurs nombres complexes est égale au produit des normes des facteurs

$$\mathrm{N}[f(\alpha) \cdot \varphi(\alpha)] = \mathrm{N}f(\alpha) \cdot \mathrm{N}\varphi(\alpha).$$

La norme du nombre complexe

$$f(\alpha) = a + a_1 \alpha + a_2 \alpha^2 + \ldots + a_{\lambda-2} \alpha^{\lambda-2}$$

est une fonction homogène du degré $\lambda - 1$ des $\lambda - 1$ nombres indéterminés a, a_1, a_2,..., $a_{\lambda-2}$. Donc la théorie des nombres complexes est, au fond, la même que la théorie de ces formes, et, pour cette raison, elle donne lieu à des questions semblables à celles qu'on connaît de la théorie des formes quadratiques. Le développement effectif de la norme comme forme du degré $\lambda - 1$ étant très-pénible, nous pourrons nous en dispenser en la représentant toujours comme produit de facteurs conjugués; d'ailleurs la discussion de ces formes nous paraît moins simple que celle des nombres complexes eux-mêmes, qui en sont les facteurs, les éléments, pour ainsi dire, et dont l'analogie avec les nombres entiers est frappante, comme on le verra dans la suite.

L'addition et la soustraction des nombres complexes n'offrent aucune difficulté, car les deux nombres complexes

$$f(\alpha) = a + a_1 \alpha + a_2 \alpha^2 + \ldots + a_{\lambda-2} \alpha^{\lambda-2}$$

et

$$\varphi(\alpha) = b + b_1 \alpha + b_2 \alpha^2 + \ldots + b_{\lambda-2} \alpha^{\lambda-2},$$

donnent immédiatement la somme et la différence

$$f(\alpha) \pm \varphi(\alpha) = a \pm b + (a_1 \pm b_1)\alpha + (a_2 \pm b_2)\alpha^2 + \ldots + (a_{\lambda-2} \pm b_{\lambda-2})\alpha^{\lambda-2}.$$

Le résultat de la multiplication des nombres $f(\alpha)$ et $\varphi(\alpha)$ sera toujours un nombre $\psi(\alpha)$ de la forme

$$\psi(\alpha) = c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-1}\alpha^{\lambda-1},$$

qui, au moyen de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

se réduira à

$$\psi(\alpha) = c - c_{\lambda-1} + (c_1 - c_{\lambda-1})\alpha + (c_2 - c_{\lambda-1})\alpha^2 + \ldots + (c_{\lambda-2} - c_{\lambda-1})\alpha^{\lambda-2},$$

et l'on aura

$$\begin{aligned} c &= ab + a_{\lambda-2}b_1 + a_{\lambda-3}b_2 + \ldots + a_2 b_{\lambda-2},\\ c_1 &= a_1 b + ab_1 + a_{\lambda-2}b_2 + \ldots + a_3 b_{\lambda-2},\\ c_2 &= a_2 b + a_1 b_1 + ab_2 + \ldots + a_4 b_{\lambda-2},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ c_{\lambda-1} &= a_{\lambda-2}b_1 + a_{\lambda-3}b_2 + \ldots + a_1 b_{\lambda-2}. \end{aligned}$$

L'addition de ces équations donne

$$\begin{aligned} &c + c_1 + c_2 + \ldots + c_{\lambda-1}\\ &= (a + a_1 + a_2 + \ldots + a_{\lambda-2})(b + b_1 + b_2 + \ldots + b_{\lambda-2}), \end{aligned}$$

et la somme des coefficients du produit $\psi(\alpha)$ dans sa forme réduite, étant égale à

$$c + c_1 + c_2 + \ldots + c_{\lambda-1} - \lambda c_{\lambda-1},$$

on en conclut ce théorème :

La somme des coefficients du produit de deux nombres complexes est congrue au produit des sommes des coefficients des facteurs pour le module λ.

Il est clair que ce théorème subsiste également pour un nombre quelconque de facteurs. En l'appliquant aux facteurs conjugués dont se compose la norme du nombre

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2},$$

pour lesquels les sommes des coefficients sont toutes égales, on aura

$$\mathrm{N}f(\alpha) \equiv (a + a_1 + a_2 + \ldots + a_{\lambda-2})^{\lambda-1} \pmod{\lambda}.$$

On en conclut :

Pour que la norme d'un nombre complexe soit divisible par λ, *il faut et il suffit que la somme des coefficients de ce nombre soit divisible par* λ.

Mais si cette somme n'est pas divisible par λ, on a, en vertu du théorème de Fermat,

$$(a + a_1 + a_2 + \ldots + a_{\lambda-2})^{\lambda-1} \equiv 1 \pmod{\lambda},$$

et, par conséquent,

$$\mathrm{N}f(\alpha) \equiv 1 \pmod{\lambda}.$$

Il suit de là cet autre théorème :

La norme de tout nombre complexe dont la somme des coefficients n'est pas divisible par λ, *est de la forme linéaire* $m\lambda + 1$.

La division des nombres complexes se réduit immédiatement au cas où le diviseur est un nombre entier non complexe. En effet, $\varphi(\alpha)$ étant le dividende et $f(\alpha)$ le diviseur, on les multipliera tous les deux par $f(\alpha^2).f(\alpha^3)\ldots f(\alpha^{\lambda-1})$ et l'on aura le diviseur $\mathrm{N}f(\alpha)$, qui sera entier. Pour que $\varphi(\alpha)$ soit divisible par $f(\alpha)$, il faut que le quotient soit égal à un nombre entier complexe $\psi(\alpha)$. L'équation

$$\frac{\varphi(\alpha)}{f(\alpha)} = \psi(\alpha)$$

donne

$$\frac{\varphi(\alpha)f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})}{\mathrm{N}f(\alpha)} = \psi(\alpha),$$

d'où l'on conclut que, dans le produit

$$\varphi(\alpha).f(\alpha^2).f(\alpha^3)\ldots f(\alpha^{\lambda-1}),$$

développé et réduit à la forme

$$c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-2}\alpha^{\lambda-2},$$

tous les coefficients c, c_1, c_2,..., $c_{\lambda-2}$ doivent être divisibles par $\mathrm{N}f(\alpha)$, et cette condition étant remplie, on aura effectivement $\varphi(\alpha)$ divisible par $f(\alpha)$.

§ II.

Théorie des unités complexes.

Les nombres complexes dont la norme est égale à l'unité sont appelés *unités complexes*. Ces unités, toujours infinies en nombre, excepté le seul cas de $\lambda = 3$, jouent un rôle principal dans toutes les questions sur les nombres complexes, et c'est pour cette raison que la discussion des unités doit être mise à la tête de cette théorie.

D'abord, il est visible que

$$\pm 1, \quad \pm \alpha, \quad \pm \alpha^2, \ldots, \quad \pm \alpha^{\lambda-1}$$

satisfont à la définition des unités; nous les appellerons des *unités simples*. De plus, il est aisé de voir que le nombre complexe

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{r-1} = \frac{1-\alpha^r}{1-\alpha},$$

r désignant un nombre entier quelconque, non divisible par λ, a pour norme la fraction

$$\frac{(1-\alpha^r)(1-\alpha^{2r})(1-\alpha^{3r})\ldots[1-\alpha^{(\lambda-1)r}]}{(1-\alpha)(1-\alpha^2)(1-\alpha^3)\ldots(1-\alpha^{\lambda-1})}$$

qui se réduit à l'unité. Donc $\frac{1-\alpha^r}{1-\alpha}$ sera aussi une unité complexe, et, puisqu'une puissance entière quelconque et le produit de plusieurs unités sont toujours une unité, il est clair que

$$\pm \alpha^k \left(\frac{1-\alpha^r}{1-\alpha}\right)^m \left(\frac{1-\alpha^s}{1-\alpha}\right)^n \left(\frac{1-\alpha^t}{1-\alpha}\right)^p \ldots$$

sera une unité pour toutes les valeurs entières des exposants m, n, p, etc. On a ainsi, en général, une infinité d'unités différentes. Mais ce qui constitue dans cette théorie la question la plus importante et en même temps la plus délicate, c'est la représentation de *toutes* les unités sous la forme la plus simple.

Nous allons aborder cette question par la démonstration du théorème :

Chaque unité complexe, divisée par sa réciproque, donne pour quotient une unité simple.

C'est-à-dire $E(\alpha)$ étant une unité quelconque, on a toujours

$$\frac{E(\alpha)}{E(\alpha^{-1})} = \pm \alpha^k.$$

D'abord il est visible que ce quotient est un entier complexe. Nous pourrons donc poser

$$\frac{E(\alpha)}{E(\alpha^{-1})} = \varphi(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1},$$

et nous aurons

$$\varphi(\alpha)\varphi(\alpha^{-1}) = 1.$$

En effectuant la multiplication, on trouve

$$\begin{aligned}
\varphi(\alpha)\varphi(\alpha^{-1}) &= A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1},\\
A &= a^2 + a_1^2 + a_2^2 + \ldots + a_{\lambda-1}^2,\\
A_1 &= aa_1 + a_1a_2 + a_2a_3 + \ldots + a_{\lambda-1}a,\\
A_2 &= aa_2 + a_1a_3 + a_2a_4 + \ldots + a_{\lambda-1}a_1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
A_{\lambda-1} &= aa_{\lambda-1} + a_1a + a_2a_1 + \ldots + a_{\lambda-1}a_{\lambda-2},
\end{aligned}$$

et, en prenant la somme de ces coefficients,

$$A + A_1 + A_2 + \ldots + A_{\lambda-1} = (a + a_1 + a_2 + \ldots + a_{\lambda-1})^2.$$

De l'équation

$$\varphi(\alpha)\varphi(\alpha^{-1}) = A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1} = 1$$

il suit aussi

$$A_1 = A_2 = A_3 = \ldots = A_{\lambda-1} \quad \text{et} \quad A = A_1 + 1,$$

et de là

$$1 + \lambda A_1 = (a + a_1 + a_2 + \ldots + a_{\lambda-1})^2$$

ou

$$\pm 1 \equiv a + a_1 + a_2 + \ldots + a_{\lambda-1} \pmod{\lambda};$$

et, puisque le nombre complexe $\varphi(\alpha)$ ne change pas de valeur quand on augmente ou diminue tous ses coefficients d'une même quantité, il est évident qu'on peut prendre

$$a + a_1 + a_2 + \ldots + a_{\lambda-1} = \pm 1,$$

et de là on a

$$A_1 = 0, \quad A_2 = 0, \quad A_3 = 0, \ldots, \quad A_{\lambda-1} = 0,$$
$$A = a^2 + a_1^2 + a_2^2 + \ldots + a_{\lambda-1}^2 = 1.$$

Mais la somme des carrés des nombres entiers $a, a_1, a_2, \ldots, a_{\lambda-1}$ ne pourra jamais être égale à l'unité, à moins qu'un quelconque d'entre eux ne soit égal à l'unité et tous les autres égaux à zéro. On a donc effectivement

$$\frac{E(\alpha)}{E(\alpha^{-1})} = \varphi(\alpha) = \pm \alpha^k.$$

On conclut facilement de ce théorème, que toutes les unités complexes peuvent être décomposées en deux facteurs, dont l'un soit une unité simple α^h, et l'autre une fonction des périodes à deux termes $\alpha + \alpha^{-1}$, $\alpha^2 + \alpha^{-2}$, $\alpha^3 + \alpha^{-3}$, etc., de sorte qu'on a toujours

$$E(\alpha) = \alpha^h \left[c + c_1 (\alpha + \alpha^{-1}) + c_2 (\alpha^2 + \alpha^{-2}) + \ldots + c_\mu (\alpha^\mu + \alpha^{-\mu}) \right],$$

où nous avons fait, pour abréger,

$$\frac{\lambda - 1}{2} = \mu.$$

Ainsi, pour le cas de $\lambda = 3$, on a

$$E(\alpha) = \alpha^h \left[c + c_1 (\alpha + \alpha^{-1}) \right]$$

et, en réduisant au moyen de l'équation $1 + \alpha + \alpha^2 = 0$,

$$E(\alpha) = \alpha^h (c - c_1),$$

d'où

$$c - c_1 = \pm 1;$$

donc, dans ce cas, il n'y a pas d'autres unités que

$$\pm 1, \quad \pm \alpha, \quad \pm \alpha^2.$$

Pour le cas de $\lambda = 5$, on a

$$E(\alpha) = \alpha^h [c + c_1 (\alpha + \alpha^{-1}) + c_2 (\alpha^2 + \alpha^{-2})],$$

et, en réduisant et mettant pour abréger $c - c_2 = t$, $c_1 - c_2 = u$,

$$E(\alpha) = \alpha^h [t + (\alpha + \alpha^4) u],$$

et de là

$$E(\alpha) E(\alpha^2) = \alpha^{3h} (t^2 - tu - u^2).$$

On en conclut que la forme quadratique $t^2 - tu - u^2$ doit être égale à l'unité, et connaissant la solution générale de l'équation

$$t^2 - tu - u^2 = 1,$$

on en tire toutes les valeurs des unités complexes pour le cas de $\lambda = 5$, lesquelles peuvent être représentées sous la forme simple

$$E(\alpha) = \pm \alpha^h (\alpha + \alpha^4)^m,$$

m étant un entier quelconque positif ou négatif.

L'exemple donné pour $\lambda = 5$ suffit pour faire voir ce qu'il faut chercher pour une valeur quelconque du nombre premier λ. Mais, en allant plus loin, on est bientôt arrêté par de grandes difficultés qu'on ne pourra guère surmonter qu'à l'aide de principes nouveaux. Ces principes, dont nous ferons usage dans la théorie des unités complexes, sont dus à M. Lejeune-Dirichlet qui les a signalés dans une Note insérée dans les *Comptes rendus de l'Académie de Berlin* du 30 mars de l'année 1846. Nous reproduirons aussi plusieurs des beaux résultats trouvés par M. Kronecker, et publiés en 1845 dans un Mémoire sur les unités complexes.

Prenons un système de $\frac{\lambda - 3}{2}$ unités complexes

$$c_1(\alpha), \quad c_2(\alpha), \quad c_3(\alpha), \ldots, \quad c_{\mu-1}(\alpha),$$

où

$$\mu = \frac{\lambda - 1}{2},$$

qui soient toutes dégagées du facteur $\pm \alpha^h$, en sorte qu'elles ne contiennent que les périodes à deux termes $\alpha + \alpha^{-1}$, $\alpha^2 + \alpha^{-2}$, etc. Ces unités seront évidemment des quantités réelles que nous prendrons toujours comme positives. Cela posé, nous en composons la forme

$$c_1(\alpha)^{m_1} . c_2(\alpha)^{m_2} . c_3(\alpha)^{m_3} \ldots c_{\mu-1}(\alpha)^{m_{\mu-1}},$$

où les exposants m_1, m_2, m_3, etc., sont entiers.

Si cette forme a la propriété que, pour des valeurs différentes des exposants entiers m_1, m_2, m_3, etc., elle ne donne que des unités réellement différentes, ou, ce qui est au fond la même chose, qu'elle ne donne jamais l'unité ordinaire 1 tant que ces exposants ne sont pas tous égaux à zéro, le système des unités

$$c_1(\alpha), \quad c_2(\alpha), \quad c_3(\alpha), \ldots, \quad c_{\mu-1}(\alpha),$$

selon M. Dirichlet, est appelé *un système indépendant*.

La condition du système indépendant que nous venons d'énoncer revient à ce que le déterminant D des quantités logarithmiques

$$\begin{array}{llll}
\mathrm{l}\, c_1(\alpha), & \mathrm{l}\, c_2(\alpha), & \mathrm{l}\, c_3(\alpha), \ldots, & \mathrm{l}\, c_{\mu-1}(\alpha), \\
\mathrm{l}\, c_1(\alpha^{\gamma}), & \mathrm{l}\, c_2(\alpha^{\gamma}), & \mathrm{l}\, c_3(\alpha^{\gamma}), \ldots, & \mathrm{l}\, c_{\mu-1}(\alpha^{\gamma}), \\
\mathrm{l}\, c_1(\alpha^{\gamma^2}), & \mathrm{l}\, c_2(\alpha^{\gamma^2}), & \mathrm{l}\, c_3(\alpha^{\gamma^2}), \ldots, & \mathrm{l}\, c_{\mu-1}(\alpha^{\gamma^2}), \\
\ldots & \ldots & \ldots & \ldots \\
\mathrm{l}\, c_1(\alpha^{\gamma^{\mu-2}}), & \mathrm{l}\, c_2(\alpha^{\gamma^{\mu-2}}), & \mathrm{l}\, c_3(\alpha^{\gamma^{\mu-2}}), \ldots, & \mathrm{l}\, c_{\mu-1}(\alpha^{\gamma^{\mu-2}}).
\end{array}$$

ne soit pas égal à zéro. (La lettre γ désigne ici, comme dans les formules suivantes, une racine primitive de la congruence $\gamma^{\lambda-1} \equiv 1 \pmod{\lambda}$, et l'on fait toujours $\mu = \frac{\lambda-1}{2}$).

Pour le prouver, posons

$$c_1(\alpha)^{m_1} c_2(\alpha)^{m_2} \ldots c_{\mu-1}(\alpha)^{m_{\mu-1}} = c_1(\alpha)^{n_1} c_2(\alpha)^{n_2} \ldots c_{\mu-1}(\alpha)^{n_{\mu-1}};$$

en divisant par le second membre de cette équation, et faisant

$$m_1 - n_1 = x_1, \quad m_2 - n_2 = x_2, \ldots,$$

on aurait

$$c_1(\alpha)^{x_1} c_2(\alpha)^{x_2} \ldots c_{\mu-1}(\alpha)^{x_{\mu-1}} = 1,$$

et, en changeant la racine α en α^γ, $\alpha^{\gamma^2}, \ldots, \alpha^{\gamma^{\mu-1}}$, on aurait de même

$$c_1(\alpha^\gamma)^{x_1} . c_2(\alpha^\gamma)^{x_2} \ldots c_{\mu-1}(\alpha^\gamma)^{x_{\mu-1}} = 1,$$

$$c_1(\alpha^{\gamma^2})^{x_1} . c_2(\alpha^{\gamma^2})^{x_2} \ldots c_{\mu-1}(\alpha^{\gamma^2})^{x_{\mu-1}} = 1,$$

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

$$c_1\left(\alpha^{\gamma^{\mu-1}}\right)^{x_1} . c_2\left(\alpha^{\gamma^{\mu-1}}\right)^{x_2} \ldots c_{\mu-1}\left(\alpha^{\gamma^{\mu-1}}\right)^{x_{\mu-1}} = 1,$$

et, en prenant les logarithmes,

$$x_1 \operatorname{l} c_1(\alpha) + x_2 \operatorname{l} c_2(\alpha) + \ldots + x_{\mu-1} \operatorname{l} c_{\mu-1}(\alpha) = 0,$$

$$x_1 \operatorname{l} c_1(\alpha^\gamma) + x_2 \operatorname{l} c_2(\alpha^\gamma) + \ldots + x_{\mu-1} \operatorname{l} c_{\mu-1}(\alpha^\gamma) = 0,$$

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

$$x_1 \operatorname{l} c_1\left(\alpha^{\gamma^{\mu-1}}\right) + x_2 \operatorname{l} c_2\left(\alpha^{\gamma^{\mu-1}}\right) + \ldots + x_{\mu-1} \operatorname{l} c_{\mu-1}\left(\alpha^{\gamma^{\mu-1}}\right) = 0.$$

En ajoutant ces équations et observant qu'on a

$$c_k(\alpha) . c_k\left(\alpha^\gamma\right) . c_k\left(\alpha^{\gamma^2}\right) \ldots c_k\left(\alpha^{\gamma^{\mu-1}}\right) = 1,$$

et de là

$$\operatorname{l} c_k(\alpha) + \operatorname{l} c_k\left(\alpha^\gamma\right) + \operatorname{l} c_k\left(\alpha^{\gamma^2}\right) + \ldots + \operatorname{l} c_k\left(\alpha^{\gamma^{\mu-1}}\right) = 0,$$

on obtient le résultat identique

$$0 = 0.$$

On voit par là qu'une de ces μ équations, par exemple la dernière, peut être rejetée comme déjà contenue dans les autres; on n'aura donc que $\mu - 1$ équations différentes à un même nombre d'inconnues $x_1, x_2, \ldots, x_{\mu-1}$. On sait que, si le déterminant de ce système n'est pas égal à zéro, on n'a que la seule solution

$$x_1 = 0, \quad x_2 = 0, \ldots, \quad x_{\mu-1} = 0,$$

ce qui donne

$$m_1 = n_1, \quad m_2 = n_2, \ldots, \quad m_{\mu-1} = n_{\mu-1};$$

mais on sait aussi que le système a une infinité de solutions différentes si le déterminant est égal à zéro. Donc le système des unités

$$c_1(\alpha), \quad c_2(\alpha), \ldots, \quad c_{\mu-1}(\alpha)$$

sera un système indépendant si le déterminant D n'est pas égal à zéro. et il ne sera jamais un système indépendant si $D = 0$.

C'est un point principal de la théorie générale des unités complexes de prouver qu'il est effectivement des systèmes indépendants de $\mu - 1$ unités. Pour ce but, nous proposons le système de $\mu - 1$ unités conjuguées

$$c(\alpha), \quad c\left(\alpha^{\gamma}\right), \quad c\left(\alpha^{\gamma^2}\right), \ldots, \quad c\left(\alpha^{\gamma^{\mu-2}}\right),$$

dans lequel $c(\alpha)$ signifie l'unité spéciale

$$c(\alpha) = \sqrt{\frac{(1-\alpha^{\gamma})(1-\alpha^{-\gamma})}{(1-\alpha)(1-\alpha^{-1})}} = \pm \frac{\alpha^{\frac{(\lambda-1)(\gamma-1)}{2}}(1-\alpha^{\gamma})}{1-\alpha}.$$

D'après le système exposé ci-dessus, ce système sera indépendant si le déterminant D des quantités

$$\begin{array}{llll}
\mathrm{l}\, c(\alpha), & \mathrm{l}\, c\left(\alpha^{\gamma}\right), & \mathrm{l}\, c\left(\alpha^{\gamma^2}\right), \ldots, & \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-2}}\right), \\
\mathrm{l}\, c\left(\alpha^{\gamma}\right), & \mathrm{l}\, c\left(\alpha^{\gamma^2}\right), & \mathrm{l}\, c\left(\alpha^{\gamma^3}\right), \ldots, & \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-1}}\right), \\
\ldots & \ldots & \ldots & \ldots \\
\mathrm{l}\, c\left(\alpha^{\gamma^{\mu-2}}\right), & \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-1}}\right), & \mathrm{l}\, c\left(\alpha^{\gamma^{\mu}}\right), \ldots, & \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-4}}\right),
\end{array}$$

n'est pas égal à zéro. Nous tirerons ce déterminant de la résolution effective du système des équations linéaires

$$\begin{array}{l}
x\, \mathrm{l}\, c(\alpha) + x_1\, \mathrm{l}\, c\left(\alpha^{\gamma}\right) + \ldots + x_{\mu-2}\, \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-2}}\right) = \mathrm{A}, \\
x\, \mathrm{l}\, c\left(\alpha^{\gamma}\right) + x_1\, \mathrm{l}\, c\left(\alpha^{\gamma^2}\right) + \ldots + x_{\mu-2}\, \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-1}}\right) = \mathrm{A}_1, \\
\ldots \\
x\, \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-2}}\right) + x_1\, \mathrm{l}\, c\left(\alpha^{\gamma}\quad\right) + \ldots + x_{\mu-2}\, \mathrm{l}\, c\left(\alpha^{\gamma^{\mu-4}}\right) = \mathrm{A}_{\mu-2}.
\end{array}$$

En les ajoutant et faisant

$$A + A_1 + \ldots + A_{\mu-2} = - A_{\mu-1},$$

au moyen de l'équation

$$lc(\alpha) + lc\left(\alpha^{\gamma}\right) + lc\left(\alpha^{\gamma^2}\right) + \ldots + lc\left(\alpha^{\gamma^{\mu-1}}\right) = 0,$$

on en déduit encore l'équation suivante qu'on peut regarder comme complémentaire,

$$x\, lc\left(\alpha^{\gamma^{\mu-1}}\right) + x_1 lc(\alpha) + \ldots + x_{\mu-2} lc\left(\alpha^{\gamma^{\mu-3}}\right) = A_{\mu-1}.$$

En multipliant ces équations par 1, β^{2k}, β^{4k},..., $\beta^{2(\mu-1)k}$ respectivement, β étant une racine primitive de l'équation

$$\beta^{\lambda-1} = 1,$$

et ajoutant, on reconnaît facilement que le premier membre de cette somme se décompose en deux facteurs, et il en résulte

$$\begin{aligned}&(x + \beta^{-2k} x_1 + \beta^{-4k} x_2 + \ldots + \beta^{-2(\mu-2)k} x_{\mu-2})\\ &\times \left[lc(\alpha) + \beta^{2k} lc\left(\alpha^{\gamma}\right) + \beta^{4k} lc\left(\alpha^{\gamma^2}\right) + \ldots + \beta^{2(\mu-1)k} lc\left(\alpha^{\gamma^{\mu-1}}\right)\right]\\ &= A + \beta^{2k} A_1 + \beta^{4k} A_2 + \ldots + \beta^{2(\mu-1)k} A_{\mu-1};\end{aligned}$$

de là, en posant, pour abréger,

$$\begin{aligned}&lc(\alpha) + \beta^{2k} lc\left(\alpha^{\gamma}\right) + \beta^{4k} lc\left(\alpha^{\gamma^2}\right) + \ldots\\ &\qquad + \beta^{2(\mu-1)k} lc\left(\alpha^{\gamma^{\mu-1}}\right) = L(\beta^{2k})\end{aligned}$$

et

$$A + \beta^{2k} A_1 + \beta^{4k} A_2 + \ldots + \beta^{2(\mu-1)k} A_{\mu-1} = \psi(\beta^{2k}),$$

on a

$$x + \beta^{-2k} x_1 + \beta^{-4k} x_2 + \ldots + \beta^{-2(\mu-2)k} x_{\mu-2} = \frac{\psi(\beta^{2k})}{L(\beta^{2k})}.$$

et de là, en multipliant par $\beta^{2kh} - \beta^{-2k}$, prenant

$$k = 1,\ 2,\ 3,\ldots,\ \mu - 1,$$

et ajoutant, on trouve la solution complète du système proposé de

équations linéaires

$$\mu x_h = \frac{(\beta^{-2h}-\beta^2)\psi(\beta^2)}{L(\beta^2)} + \frac{(\beta^{4h}-\beta^{-4})\psi(\beta^4)}{L(\beta^4)} + \dots + \frac{[\beta^{2(\mu-1)h}-\beta^{-2(\mu-1)}]\psi[\beta^{2(\mu-1)}]}{L[\beta^{2(\mu-1)}]}.$$

On en conclut que le dénominateur commun de toutes les inconnues x, $x_1,\dots, x_{\mu-2}$ est donné par le produit

$$L(\beta^2).L(\beta^4)\dots L(\beta^{2\mu-2}),$$

lequel, dégagé du facteur étranger μ, donne le déterminant cherché

$$D = \frac{L(\beta^2).L(\beta^4).L(\beta^6)\dots L(\beta^{2\mu-2})}{\mu}.$$

Ainsi la démonstration de l'indépendance du système proposé des unités conjuguées

$$c(\alpha),\quad c(\alpha^\gamma),\dots,\quad c(\alpha^{\gamma^{\mu-2}})$$

est réduite à prouver que l'expression

$$L(\beta^{2k}) = l\,c(\alpha) + \beta^{2k}\,l\,c(\alpha^\gamma) + \beta^{4k}\,l\,c(\alpha^{\gamma^2}) + \dots + \beta^{2(\mu-1)}\,l\,c(\alpha^{\gamma^{\mu-1}})$$

n'est égale à zéro pour aucune des valeurs

$$k = 1,\ 2,\ 3,\dots,\ \mu-1.$$

Pour cela, nous renvoyons le lecteur au célèbre Mémoire de M. Lejeune-Dirichlet, inséré dans les *Actes de l'Académie de Berlin* de l'année 1837, dans lequel il a démontré le premier que toute série arithmétique dont le premier membre et la différence sont sans facteur commun, contient une infinité de nombres premiers [*]. La méthode ingénieuse de ce grand géomètre repose de même sur cette proposition dont il a donné une démonstration rigoureuse à l'endroit cité. Il est donc prouvé que le système des $\mu-1$ unités conjuguées

$$c(\alpha),\quad c(\alpha^\gamma),\quad c(\alpha^{\gamma^2}),\dots,\quad c(\alpha^{\gamma^{\mu-2}})$$

---

[*] Une traduction française de ce Mémoire, par M. Terquem, a paru au tome IV du présent Journal. (J. Liouville.)

est un système indépendant, et, par conséquent, toutes les propriétés générales des systèmes indépendants que nous allons expliquer, conviendront toujours à ce système remarquable.

Revenons au système général des $\mu - 1$ unités

$$c_1(\alpha), \quad c_2(\alpha), \quad c_3(\alpha), \ldots, \quad c_{\mu-1}(\alpha),$$

et supposons toujours qu'il soit indépendant, c'est-à-dire que le déterminant D des logarithmes de ces unités et de leurs conjuguées ne soit pas égal à zéro. Alors nous savons que toutes les unités contenues dans la forme

$$c_1(\alpha)^{m_1} \cdot c_2(\alpha)^{m_2} \cdot c_3(\alpha)^{m_3} \ldots c_{\mu-1}(\alpha)^{m_{\mu-1}}$$

sont différentes entre elles; mais, en général, pour toutes les valeurs entieres positives et négatives des nombres $m_1, m_2, \ldots, m_{\mu-1}$, cette forme, multipliée par l'unité simple $\pm \alpha^h$, ne contient pas toutes les unités possibles. Pour remédier à ce défaut, nous ferons abstraction de la restriction que les exposants doivent être des nombres entiers, et nous essayerons d'exprimer toutes les unités, dégagées des unités simples $\pm \alpha^h$, par la forme

$$\mathrm{E}(\alpha) = c_1(\alpha)^{x_1} \cdot c_2(\alpha)^{x_2} \cdot c_3(\alpha)^{x_3} \ldots c_{\mu-1}(\alpha)^{x_{\mu-1}},$$

dans laquelle $x_1, x_2, x_3, \ldots, x_{\mu-1}$ désignent des quantités numériques quelconques. En prenant les logarithmes des deux membres de l'équation proposée et changeant α en $\alpha^\gamma, \alpha^{\gamma^2}, \ldots, \alpha^{\gamma^{\mu-1}}$, on obtient ce système d'équations linéaires

$$x_1 \mathrm{l}\, c_1(\alpha) + x_2 \mathrm{l}\, c_2(\alpha) + \ldots + x_{\mu-1} \mathrm{l}\, c_{\mu-1}(\alpha) = \mathrm{l}\, \mathrm{E}(\alpha),$$

$$x_1 \mathrm{l}\, c_1(\alpha^\gamma) + x_2 \mathrm{l}\, c_2(\alpha^\gamma) + \ldots + x_{\mu-1} \mathrm{l}\, c_{\mu-1}(\alpha^\gamma) = \mathrm{l}\, \mathrm{E}(\alpha^\gamma),$$

. . . . . .

$$x_1 \mathrm{l}\, c_1(\alpha^{\gamma^{\mu-1}}) + x_2 \mathrm{l}\, c_2(\alpha^{\gamma^{\mu-1}}) + \ldots + x_{\mu-1} \mathrm{l}\, c_{\mu-1}(\alpha^{\gamma^{\mu-1}}) = \mathrm{l}\, \mathrm{E}(\alpha^{\gamma^{\mu-1}}),$$

dont l'une, par exemple la dernière, peut être rejetée parce qu'elle est déjà contenue dans les autres. La résolution de ces équations linéaires, dont le déterminant par l'hypothèse n'est pas égal à zéro,

donne toujours des valeurs finies et déterminées des inconnues x_1, $x_2,\ldots,$ $x_{\mu-1}$ qui sont indépendantes de la racine α, parce que ce système reste le même quand on y change α en α^{γ}, α^{γ^2}, etc. Donc :

Toutes les unités complexes sans exception peuvent être représentées comme produits des puissances de $\mu - 1$ unités indépendantes, jointes aux unités simples $\pm\alpha^h$, en admettant des exposants numériques quelconques de ces puissances.

Si, dans l'expression

$$E(\alpha) = c_1(\alpha)^{x_1} \cdot c_2(\alpha)^{x_2} \cdot c_3(\alpha)^{x_3} \ldots c_{\mu-1}(\alpha)^{x_{\mu-1}},$$

on sépare les plus grands entiers contenus dans les exposants, et qu'on pose

$$x_1 = m_1 + \delta_1, \quad x_2 = m_2 + \delta_2, \ldots, \quad x_{\mu-1} = m_{\mu-1} + \delta_{\mu-1},$$

où δ_1, $\delta_2,\ldots,$ $\delta_{\mu-1}$ sont renfermés entre les limites o et 1, on a

$$E(\alpha) = c_1(\alpha)^{m_1} \cdot c_2(\alpha)^{m_2} \ldots c_{\mu-1}(\alpha)^{m_{\mu-1}} \cdot c_1(\alpha)^{\delta_1} \cdot c_2(\alpha)^{\delta_2} \ldots c_{\mu-1}(\alpha)^{\delta_{\mu-1}}.$$

Le second facteur $c_1(\alpha)^{\delta_1} \cdot c_2(\alpha)^{\delta_2} \ldots c_{\mu-1}(\alpha)^{\delta_{\mu-1}}$, que nous désignons, pour abréger, par $F(\alpha)$, doit être une unité entière complexe aussi bien que $E(\alpha)$. Soit donc

$$F(\alpha) = a(\alpha + \alpha^{-1}) + a_1\left(\alpha^{\gamma} + \alpha^{-\gamma}\right) + \ldots + a_{\mu-1}\left(\alpha^{\gamma^{\mu-1}} + \alpha^{-\gamma^{\mu-1}}\right),$$

et de là

$$F\left(\alpha^{\gamma}\right) = a\left(\alpha^{\gamma} + \alpha^{-\gamma}\right) + a_1\left(\alpha^{\gamma^2} + \alpha^{-\gamma^2}\right) + \ldots + a_{\mu-1}(\alpha + \alpha^{-1}),$$

$$F\left(\alpha^{\gamma^2}\right) = a\left(\alpha^{\gamma^2} + \alpha^{-\gamma^2}\right) + a_1\left(\alpha^{\gamma^3} + \alpha^{-\gamma^3}\right) + \ldots + a_{\mu-1}\left(\alpha^{\gamma} + \alpha^{-\gamma}\right).$$

. . . . . .

$$F\left(\alpha^{\gamma^{\mu-1}}\right) = a\left(\alpha^{\gamma^{\mu-1}} + \alpha^{-\gamma^{\mu-1}}\right) + a_1(\alpha + \alpha^{-1}) + \ldots + a_{\mu-1}\left(\alpha^{\gamma^{\mu-2}} + \alpha^{-\gamma^{\mu-2}}\right)$$

En résolvant ce système d'équations par rapport aux coefficients a,

$a_1, a_2, \ldots, a_{\mu-1}$, on trouve facilement

$$-\lambda a = (2 - \alpha - \alpha^{-1})\,\mathrm{F}(\alpha) + \left(2 - \alpha^{\gamma} - \alpha^{-\gamma}\right)\mathrm{F}\left(\alpha^{\gamma}\right) + \ldots + \left(2 - \alpha^{\gamma^{\mu-1}} - \alpha^{-\gamma^{\mu-1}}\right)\mathrm{F}\left(\alpha^{\gamma^{\mu-1}}\right),$$

$$-\lambda a_1 = \left(2 - \alpha^{\gamma} - \alpha^{-\gamma}\right)\mathrm{F}(\alpha) + \left(2 - \alpha^{\gamma^2} - \alpha^{-\gamma^2}\right)\mathrm{F}\left(\alpha^{\gamma}\right) + \ldots + (2 - \alpha - \alpha^{-1})\,\mathrm{F}\left(\alpha^{\gamma^{\mu-1}}\right),$$

. . . . . .

$$-\lambda a_{\mu-1} = \left(2 - \alpha^{\gamma^{\mu-1}} - \alpha^{-\gamma^{\mu-1}}\right)\mathrm{F}(\alpha) + (2 - \alpha - \alpha^{-1})\,\mathrm{F}\left(\alpha^{\gamma}\right) + \ldots + \left(2 - \alpha^{\gamma^{\mu-2}} - \alpha^{-\gamma^{\mu-2}}\right)\mathrm{F}\left(\alpha^{\gamma^{\mu-1}}\right).$$

Les quantités $2 - \alpha - \alpha^{-1}$, $2 - \alpha^{\gamma} - \alpha^{-\gamma}$, etc., sont toutes positives et contenues entre les limites o et 4, car on a

$$\alpha + \alpha^{-1} = 2\cos\frac{2k\pi}{\lambda}$$

et

$$2 - \alpha - \alpha^{-1} = \left(2\sin\frac{k\pi}{\lambda}\right)^2.$$

En considérant que les exposants $\delta_1, \delta_2, \ldots, \delta_{\mu-1}$ sont renfermés entre les limites o et 1, on voit aussi que, pour chaque système donné d'unités indépendantes, les quantités $\mathrm{F}(\alpha)$, $\mathrm{F}\left(\alpha^{\gamma}\right)$, etc., ne peuvent surpasser certaines limites qu'on peut fixer en chaque cas particulier. Il suit de là que les coefficients a, a_1, $a_2, \ldots, a_{\mu-1}$ sont tous négatifs et qu'ils sont contenus entre des limites fixes; et, en considérant encore que ces coefficients sont des nombres entiers, on conclut qu'il n'y a qu'un nombre fini et limité de valeurs convenables de ces coefficients, et, par conséquent, qu'il n'y a qu'un nombre fini d'unités, telles que $\mathrm{F}(\alpha)$.

Le résultat trouvé peut être énoncé comme il suit :

$c_1(\alpha)$, $c_2(\alpha), \ldots, c_{\mu-1}(\alpha)$ étant $\mu - 1$ unités indépendantes et m_1, m_2, $m_3, \ldots, m_{\mu-1}$ tous les nombres entiers positifs et négatifs, il y a tou-

jours un nombre fini d'unités qui, multipliées par les unités contenues dans la forme

$$\pm \alpha^h c_1(\alpha)^{m_1} . c_2(\alpha)^{m_2} \dots c_{\mu-1}(\alpha)^{m_{\mu-1}},$$

produisent toutes les unités possibles.

Revenons à présent à la forme

$$E(\alpha) = c_1(\alpha)^{x_1} . c_2(\alpha)^{x_2} . c_3(\alpha)^{x_3} \dots c_{\mu-1}(\alpha)^{x_{\mu-1}},$$

et supposons que les exposants x_1, x_2,..., $x_{\mu-1}$ soient déterminés de manière à rendre $E(\alpha)$ une unité entière complexe. Élevons à une puissance entière indéterminée n, et séparons les plus grands entiers de

$$nx_1 = m_1 + \delta_1, \quad nx_2 = m_2 + \delta_2, \dots, \quad nx_{\mu-1} = m_{\mu-1} + \delta_{\mu-1},$$

de manière que δ_1, δ_2,..., $\delta_{\mu-1}$ soient tous entre les limites o et 1 ; nous aurons ainsi

$$E(\alpha)^n = c_1(\alpha)^{m_1} . c_2(\alpha)^{m_2} . c_{\mu-1}(\alpha)^{m_{\mu-1}} . c_1(\alpha)^{\delta_1} . c_2(\alpha)^{\delta_2} \dots c_{\mu-1}(\alpha)^{\delta_{\mu-1}}.$$

Maintenant, en donnant à l'exposant n les valeurs 1, 2, 3, 4,..., et ainsi de suite, les nombres entiers m_1, m_2,..., $m_{\mu-1}$ et les fractions δ_1, δ_2,..., $\delta_{\mu-1}$ changeront de valeur. Mais, parce qu'il est démontré que la forme

$$c_1(\alpha)^{\delta_1} . c_2(\alpha)^{\delta_2} \dots c_{\mu-1}(\alpha)^{\delta_{\mu-1}},$$

δ_1, δ_2,..., $\delta_{\mu-1}$ étant toujours entre o et 1, ne peut contenir qu'un nombre fini d'unités différentes, il s'ensuit que ce second facteur se reproduira nécessairement et qu'il restera le même pour une certaine suite de valeurs de l'exposant n. Soient n et n' deux exposants auxquels appartient le même second facteur, et soient m'_1, m'_2,..., $m'_{\mu-1}$ des exposants entiers dans l'expression de $E(\alpha)^{n'}$, on aura

$$E(\alpha)^n = c_1(\alpha)^{m_1} . c_2(\alpha)^{m_2} \dots c_{\mu-1}(\alpha)^{m_{\mu-1}} . c_1(\alpha)^{\delta_1} . c_2(\alpha)^{\delta_2} \dots c_{\mu-1}(\alpha)^{\delta_{\mu-1}},$$

$$E(\alpha)^{n'} = c_1(\alpha)^{m'_1} . c_2(\alpha)^{m'_2} \dots c_{\mu-1}(\alpha)^{m'_{\mu-1}} . c_1(\alpha)^{\delta_1} . c_2(\alpha)^{\delta_2} \dots c_{\mu-1}(\alpha)^{\delta_{\mu-1}}.$$

et, en divisant,

$$E(\alpha)^{n-n'} = c_1(\alpha)^{m_1-m'_1} \cdot c_2(\alpha)^{m_2-m'_2} \dots c_{\mu-1}(\alpha)^{m_{\mu-1}-m'_{\mu-1}}.$$

Nous en concluons le théorème suivant :

Il y a toujours une certaine puissance entière de toute unité complexe telle, que cette puissance de l'unité complexe puisse être exprimée par le produit de puissances entières d'un système donné de $\mu - 1$ *unités indépendantes.*

Le même résultat peut aussi s'énoncer comme il suit :

La forme

$$\pm \alpha^h c_1(\alpha)^{x_1} \cdot c_2(\alpha)^{x_2} \cdot c_3(\alpha)^{x_3} \dots c_{\mu-1}(\alpha)^{x_{\mu-1}}$$

ne contient des unités entières complexes que pour des valeurs rationnelles des exposants $x_1, x_2, \dots, x_{\mu-1}$ *dont les dénominateurs ne surpassent pas une certaine limite fixe, mais pour de telles valeurs elle représente toutes les unités possibles.*

Ainsi, par exemple, le système des unités

$$c(\alpha), \quad c(\alpha^\gamma), \quad (c^{\gamma^2}), \dots, \quad c(\alpha^{\gamma^{\mu-1}}),$$

où

$$c(\alpha) = \sqrt{\frac{(1-\alpha^\gamma)(1-\alpha^{-\gamma})}{(1-\alpha)(1-\alpha^{-1})}},$$

que nous avons démontré être indépendant, suffit pour représenter toutes les unités complexes. Mais, comme cette représentation a l'inconvénient qu'elle exige, en général, des puissances fractionnaires ou des radicaux, et qu'elle ne donne des unités rationnelles et entières que pour des systèmes de valeurs de ces exposants fractionnaires qu'on ne saurait assigner à priori, nous allons en déduire un autre système d'unités indépendantes tel, que le produit de ses puissances *entières* contienne toutes les unités possibles.

Prenons un système de $\mu - 1$ unités indépendantes

$$\varepsilon_1(\alpha), \quad \varepsilon_2(\alpha), \quad \varepsilon_3(\alpha), \dots, \quad \varepsilon_{\mu-1}(\alpha).$$

D'après le théorème que nous venons de démontrer, certaines puissances entières de ces unités pourront être exprimées comme puissances entières des unités

$$c(\alpha),\quad c\left(\alpha^{\gamma}\right),\quad c\left(\alpha^{\gamma^2}\right),\ldots,\quad c\left(\alpha^{\gamma^{\mu-1}}\right);$$

nous pouvons donc poser

$$\varepsilon_1(\alpha)^{n_1} = c(\alpha)^{r_1^1}.c\left(\alpha^{\gamma}\right)^{r_2^1}\ldots c\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}^1},$$

$$\varepsilon_2(\alpha)^{n_2} = c(\alpha)^{r_1^2}.c\left(\alpha^{\gamma}\right)^{r_2^2}\ldots c\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}^2},$$

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

$$\varepsilon_{\mu-1}(\alpha)^{n_{\mu-1}} = c(\alpha)^{r_1^{\mu-1}}.c\left(\alpha^{\gamma}\right)^{r_2^{\mu-1}}\ldots c\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}^{\mu-1}},$$

les exposants n_1, n_2,..., $n_{\mu-1}$ étant des nombres entiers qui ne surpassent pas des limites finies et déterminées, et les exposants r_1^1, r_2^1, etc., étant également des nombres entiers. En prenant les logarithmes de ces équations, on a

$$n_1 \operatorname{l}\varepsilon_1(\alpha) = r_1^1 \operatorname{l} c(\alpha) + r_2^1 \operatorname{l} c\left(\alpha^{\gamma}\right) + \ldots + r_{\mu-1}^1 \operatorname{l} c\left(\alpha^{\gamma^{\mu-2}}\right),$$

$$n_2 \operatorname{l}\varepsilon_2(\alpha) = r_1^2 \operatorname{l} c(\alpha) + r_2^2 \operatorname{l} c\left(\alpha^{\gamma}\right) + \ldots + r_{\mu-1}^2 \operatorname{l} c\left(\alpha^{\gamma^{\mu-2}}\right),$$

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

$$n_{\mu-1} \operatorname{l}\varepsilon_{\mu-1}(\alpha) = r_1^{\mu-1} \operatorname{l} c(\alpha) + r_2^{\mu-1} \operatorname{l} c\left(\alpha^{\gamma}\right) + \ldots + r_{\mu-1}^{\mu-1} \operatorname{l} c\left(\alpha^{\gamma^{\mu-2}}\right).$$

Désignons par la lettre Δ le déterminant des quantités

$$\begin{array}{lll}
\operatorname{l}\varepsilon_1(\alpha), & \operatorname{l}\varepsilon_2(\alpha),\ldots, & \operatorname{l}\varepsilon_{\mu-1}(\alpha),\\
\operatorname{l}\varepsilon_1\left(\alpha^{\gamma}\right), & \operatorname{l}\varepsilon_2\left(\alpha^{\gamma}\right),\ldots, & \operatorname{l}\varepsilon_{\mu-1}\left(\alpha^{\gamma}\right),\\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\\
\operatorname{l}\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right), & \operatorname{l}\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right),\ldots, & \operatorname{l}\varepsilon_{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right).
\end{array}$$

Soit de même D le déterminant des quantités

$$\begin{array}{lll} \mathrm{I}\,c(\alpha), & \mathrm{I}\,c(\alpha^{\gamma}),\ldots, & \mathrm{I}\,c(\alpha^{\gamma^{\mu-2}}), \\ \mathrm{I}\,c(\alpha^{\gamma}), & \mathrm{I}\,c(\alpha^{\gamma^2}),\ldots, & \mathrm{I}\,c(\alpha^{\gamma^{\mu-1}}), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & \\ \mathrm{I}\,c(\alpha^{\gamma^{\mu-2}}), & \mathrm{I}\,c(\alpha^{\gamma^{\mu-1}}),\ldots, & \mathrm{I}\,c(\alpha^{\gamma^{\mu-4}}), \end{array}$$

et R le déterminant du système des nombres

$$\begin{array}{lll} r_1^1, & r_2^1,\ldots, & r_{\mu-1}^1, \\ r_1^2, & r_2^2,\ldots, & r_{\mu-1}^2, \\ \cdots\cdots\cdots\cdots & & \\ r_1^{\mu-1}, & r_2^{\mu-1},\ldots, & r_{\mu-1}^{\mu-1}. \end{array}$$

En examinant les expressions des quantités $\mathrm{I}\,\varepsilon_1(\alpha)$, $\mathrm{I}\,\varepsilon_2(\alpha)$, etc., et celles qu'on en tire par le changement de la racine α en α^{γ}, α^{γ^2}, etc., on reconnaît facilement que le déterminant Δ se compose des deux déterminants D et R; en effet, on a

$$\Delta = \frac{\mathrm{R}.\mathrm{D}}{n_1.n_2\ldots n_{\mu-1}}.$$

En excluant tous les systèmes de valeurs des entiers r_k^h, qui donneraient

$$\mathrm{R} = 0,$$

et, par conséquent aussi,

$$\Delta = 0,$$

la plus petite valeur de R, qui est un nombre entier, sera

$$\mathrm{R} = 1.$$

De plus, nous savons que le déterminant D a une valeur finie et déterminée différente de zéro, et que les nombres $n_1, n_2,\ldots, n_{\mu-1}$ ne surpassent pas une limite fixe; nous en concluons qu'il y aura toujours une valeur *minimum* finie et déterminée de Δ, c'est-à-dire

que, parmi les systèmes en nombres infinis de $\mu - 1$ unités indépendantes, il n'y en aura jamais aucun dont le déterminant Δ soit inférieur à une certaine limite finie.

Nous appelons *système fondamental* tout système indépendant de $\mu - 1$ unités pour lequel le déterminant Δ a cette valeur du *minimum* dont nous venons de prouver l'existence. Supposons aussi que les unités

$$\varepsilon_1(\alpha), \quad \varepsilon_2(\alpha), \ldots, \quad \varepsilon_{\mu-1}(\alpha)$$

représentent un tel système fondamental dont le déterminant Δ ait la valeur la moindre possible. Cela posé, nous allons démontrer que la forme

$$\pm \alpha^h \varepsilon_1(\alpha)^{m_1} . \varepsilon_2(\alpha)^{m_2} . \varepsilon_3(\alpha)^{m_3} \ldots \varepsilon_{\mu-1}(\alpha)^{m_{\mu-1}},$$

pour des valeurs *entières* des exposants m_1, m_2, $m_3, \ldots$, $m_{\mu-1}$, donne toutes les unités sans exception. En effet, imaginons qu'il y ait une unité non comprise dans cette forme, nous savons qu'elle pourrait toujours être représentée par la forme

$$\pm \alpha^h \varepsilon_1(\alpha)^{x_1} . \varepsilon_2(\alpha)^{x_2} . \varepsilon_3(\alpha)^{x_3} \ldots \varepsilon_{\mu-1}(\alpha)^{x_{\mu-1}},$$

pour des valeurs fractionnaires de x_1, $x_2, \ldots$, $x_{\mu-1}$; séparant donc les plus grands entiers contenus dans ces exposants, et faisant comme ci-dessus,

$$x_1 = m_1 + \delta_1, \quad x_2 = m_2 + \delta_2, \ldots, \quad x_{\mu-1} = m_{\mu-1} + \delta_{\mu-1},$$

où m_1, $m_2, \ldots$, $m_{\mu-1}$ sont entiers et δ_1, $\delta_2, \ldots$, $\delta_{\mu-1}$ contenus entre 0 et 1, cette unité complexe prendrait la forme

$$\pm \alpha^h \varepsilon_1(\alpha)^{m_1} . \varepsilon_2(\alpha)^{m_2} \ldots \varepsilon_{\mu-1}(\alpha)^{m_{\mu-1}} . \varepsilon_1(\alpha)^{\delta_1} . \varepsilon_2(\alpha)^{\delta_2} \ldots \varepsilon_{\mu-1}(\alpha)^{\delta_{\mu-1}},$$

et de là il suivrait que

$$\varepsilon_1(\alpha)^{\delta_1} . \varepsilon_2(\alpha)^{\delta_2} \ldots \varepsilon_{\mu-1}(\alpha)^{\delta_{\mu-1}} = \mathrm{E}(\alpha)$$

serait encore une unité entière complexe. Les quantités δ_1, $\delta_2, \ldots$, $\delta_{\mu-1}$ qui sont moindres que l'unité ne pourraient pas toutes être égales à zéro; supposons donc que δ_1 soit différent de zéro et prenons le

nouveau système de $\mu - 1$ unités

$$E(\alpha), \quad \varepsilon_2(\alpha), \quad \varepsilon_3(\alpha), \ldots, \quad \varepsilon_{\mu-1}(\alpha).$$

Le déterminant des logarithmes de ce système, que nous désignerons par Δ',

$$\begin{array}{llll} lE(\alpha), & l\varepsilon_2(\alpha), & l\varepsilon_3(\alpha), \ldots, & l\varepsilon_{\mu-1}(\alpha), \\ lE(\alpha^\gamma), & l\varepsilon_2(\alpha^\gamma), & l\varepsilon_3(\alpha^\gamma), \ldots, & l\varepsilon_{\mu-1}(\alpha^\gamma), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & \\ lE(\alpha^{\gamma^{\mu-2}}), & l\varepsilon_2(\alpha^{\gamma^{\mu-2}}), & l\varepsilon_3(\alpha^{\gamma^{\mu-2}}), \ldots, & l\varepsilon_{\mu-1}(\alpha^{\gamma^{\mu-2}}), \end{array}$$

se réduit immédiatement au déterminant Δ; car, au moyen de l'équation

$$lE(\alpha) = \vartheta_1 l\varepsilon_1(\alpha) + \vartheta_2 l\varepsilon_2(\alpha) + \ldots + \vartheta_{\mu-1} l\varepsilon_{\mu-1}(\alpha),$$

et de celles qu'on en déduit en changeant α en α^γ, $\alpha^{\gamma^2}, \ldots, \alpha^{\gamma^{\mu-1}}$, on trouve

$$\Delta' = \vartheta_1 \Delta.$$

Mais, ϑ_1 étant moindre que 1 et différent de zéro, on en conclut qu'il y aurait un système de $\mu - 1$ unités indépendantes à qui appartiendrait un déterminant Δ' moindre que Δ, c'est-à-dire moindre que le plus petit de tous, ce qui serait absurde. Nous avons donc ce théorème important :

Il existe toujours des systèmes de $\mu - 1$ unités fondamentales telles, qu'en les élevant à des puissances entières, multipliant et joignant le facteur $\pm \alpha^h$, on produit toutes les unités possibles, et qu'en prenant des combinaisons différentes des exposants on ne produira que des unités vraiment différentes.

Le calcul effectif de systèmes d'unités fondamentales étant toujours très-pénible, nous ne nous arrêterons pas à expliquer les méthodes propres à ce but; mais nous terminerons cet abrégé des propriétés principales des unités complexes en démontrant qu'il y a toujours une infinité de systèmes différents d'unités fondamentales, et en faisant voir le rapport qui existe entre eux.

Pour cela, nous prenons les $\mu - 1$ unités

$$E_1(\alpha), \quad E_2(\alpha), \quad E_3(\alpha), \ldots, \quad E_{\mu-1}(\alpha),$$

qui s'expriment par les unités fondamentales

$$\varepsilon_1(\alpha), \quad \varepsilon_2(\alpha), \ldots, \quad \varepsilon_{\mu-1}(\alpha),$$

comme il suit :

$$\begin{aligned}
E_1(\alpha) &= \varepsilon_1(\alpha)^{r_1^1} \cdot \varepsilon_2(\alpha)^{r_2^1} \ldots \varepsilon_{\mu-1}(\alpha)^{r_{\mu-1}^1}, \\
E_2(\alpha) &= \varepsilon_1(\alpha)^{r_1^2} \cdot \varepsilon_2(\alpha)^{r_2^2} \ldots \varepsilon_{\mu-1}(\alpha)^{r_{\mu-1}^2}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
E_{\mu-1}(\alpha) &= \varepsilon_1(\alpha)^{r_1^{\mu-1}} \cdot \varepsilon_2(\alpha)^{r_2^{\mu-1}} \ldots \varepsilon_{\mu-1}(\alpha)^{r_{\mu-1}^{\mu-1}},
\end{aligned}$$

où tous les exposants r_k^h sont entiers. En prenant les logarithmes, on a

$$\begin{aligned}
\mathrm{l}\,E_1(\alpha) &= r_1^1\,\mathrm{l}\,\varepsilon_1(\alpha) + r_2^1\,\mathrm{l}\,\varepsilon_2(\alpha) + \ldots + r_{\mu-1}^1\,\mathrm{l}\,\varepsilon_{\mu-1}(\alpha), \\
\mathrm{l}\,E_2(\alpha) &= r_1^2\,\mathrm{l}\,\varepsilon_1(\alpha) + r_2^2\,\mathrm{l}\,\varepsilon_2(\alpha) + \ldots + r_{\mu-1}^2\,\mathrm{l}\,\varepsilon_{\mu-1}(\alpha), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\mathrm{l}\,E_{\mu-1}(\alpha) &= r_1^{\mu-1}\,\mathrm{l}\,\varepsilon_1(\alpha) + r_2^{\mu-1}\,\mathrm{l}\,\varepsilon_2(\alpha) + \ldots + r_{\mu-1}^{\mu-1}\,\mathrm{l}\,\varepsilon_{\mu-1}(\alpha).
\end{aligned}$$

Donc, en désignant, comme ci-dessus, par R le déterminant des entiers r_1^1, r_2^1, etc., par Δ le déterminant du système des unités fondamentales

$$\varepsilon_1(\alpha), \quad \varepsilon_2(\alpha), \ldots, \quad \varepsilon_{\mu-1}(\alpha),$$

et, de plus, par Δ_1 le déterminant analogue des logarithmes du système $E_1(\alpha)$, $E_2(\alpha)$, etc., on aura, par la même raison que ci-dessus,

$$\Delta_1 = R\,\Delta.$$

Ainsi, toutes les fois que le déterminant R est égal à l'unité, on aura

$$\Delta_1 = \Delta,$$

et, par conséquent, le système des unités

$$E_1(\alpha), \quad E_2(\alpha), \ldots \quad E_{\mu-1}(\alpha)$$

sera un système fondamental. Ainsi, d'un seul système fondamental on déduira l'infinité de tous les autres sans exception.

En observant que le déterminant R est un nombre entier, on voit aussi que le quotient qu'on obtient en divisant le déterminant d'un système indépendant quelconque par le déterminant du système fondamental est un nombre entier.

§ III.

Des périodes des racines de l'équation $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$ *et de leur correspondance avec les racines de congruences analogues.*

Après avoir traité le cas où la norme d'un nombre complexe est égale à l'unité, nous passons à la discussion générale des nombres complexes dont les normes sont des entiers quelconques. Mais pour aborder la question dans toute la généralité qu'elle exige, nous ne nous bornerons pas au cas où les nombres complexes sont composés des simples racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

mais nous admettrons aussi qu'ils contiennent les périodes de ces racines. Au premier aspect, les nombres complexes composés des périodes paraissent être moins généraux que ceux qui contiennent les simples racines; mais, en considérant que les périodes qui ne consistent qu'en un seul terme sont les simples racines, on voit que la discussion des nombres complexes composés des périodes embrassera tous les nombres complexes, tels que nous les avons proposés au commencement.

Nous commençons par exposer les principes du calcul des périodes dont nous ferons usage dans la suite de ce Mémoire. Soient e et f deux facteurs du nombre $\lambda - 1$, en sorte qu'on ait

$$\lambda - 1 = e.f;$$

soit, comme ci-dessus, γ une racine primitive de la congruence

$$\gamma^{\lambda-1} \equiv 1 \pmod{\lambda}.$$

Cela posé, les racines imaginaires de l'équation

$$\alpha^{\lambda} = 1$$

pourront être rangées en e périodes à f termes, comme il suit :

$$\eta = \alpha + \alpha^{\gamma^e} + \alpha^{\gamma^{2e}} + \ldots + \alpha^{\gamma^{(f-1)e}},$$

$$\eta_1 = \alpha^{\gamma} + \alpha^{\gamma^{e+1}} + \alpha^{\gamma^{2e+1}} + \ldots + \alpha^{\gamma^{(f-1)e+1}},$$

$$\eta_2 = \alpha^{\gamma^2} + \alpha^{\gamma^{e+2}} + \alpha^{\gamma^{2e+2}} + \ldots + \alpha^{\gamma^{(f-1)e+2}},$$

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

$$\eta_{e-1} = \alpha^{\gamma^{e-1}} + \alpha^{\gamma^{2e-1}} + \alpha^{\gamma^{3e-1}} + \ldots + \alpha^{\gamma^{fe-1}}.$$

Ces périodes forment un cycle tel, qu'en continuant la série

$$\eta, \quad \eta_1, \quad \eta_2, \quad \eta_{e-1},$$

on aura

$$\eta_e = \eta, \quad \eta_{e+1} = \eta_1,$$

et généralement

$$\eta_{ke+h} = \eta_h.$$

Le changement de α en α^{γ^k} ne changera pas l'ordre cyclique des périodes, car au lieu de la suite

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1},$$

on aura respectivement

$$\eta_k, \quad \eta_{k+1}, \quad \eta_{k+2}, \ldots, \quad \eta_{k-1}.$$

La somme de toutes les périodes étant la même que la somme de toutes les racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$$

est égale à l'unité négative

$$\eta + \eta_1 + \eta_2 + \ldots + \eta_{e-1} = -1.$$

Le produit de deux périodes est toujours une fonction linéaire de toutes les périodes du même rang. En exécutant la multiplication de-

deux périodes η et η_k, on trouve

$$\eta\eta_k = n^k f + m^k\eta + m_1^k\eta_1 + m_2^k\eta_2 + \ldots + m_{e-1}^k\eta_{e-1}.$$

En changeant les périodes η en η_r, η_1 en η_{r+1}, η_2 en η_{r+2}, etc., on a aussi

$$\eta_r\eta_{r+k} = n^k f + m^k\eta_r + m_1^k\eta_{r+1} + m_2^k\eta_{r+2} + \ldots + m_{e-1}^k\eta_{r-1},$$

et, en faisant

$$k = 0,\ 1,\ 2,\ldots,\ e-1,$$

on a le système d'équations

$$(A)\quad \begin{cases} \eta^2 = nf + m\eta + m_1\eta_1 + m_2\eta_2 + \ldots + m_{e-1}\eta_{e-1}, \\ \eta\eta_1 = n^1 f + m^1\eta + m_1^1\eta_1 + m_2^1\eta_2 + \ldots + m_{e-1}^1\eta_{e-1}, \\ \eta\eta_2 = n^2 f + m^2\eta + m_1^2\eta_1 + m_2^2\eta_2 + \ldots + m_{e-1}^2\eta_{e-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta\eta_{e-1} = n^{e-1} f + m^{e-1}\eta + m_1^{e-1}\eta_1 + m_2^{e-1}\eta_2 + \ldots + m_{e-1}^{e-1}\eta_{e-1}. \end{cases}$$

Dans ces équations fondamentales pour le calcul des périodes, les coefficients n^k sont toujours égaux à zéro, excepté : 1° pour f pair et $k = 0$; 2° pour f impair et $k = \frac{1}{2}e$; on a pour ces deux cas $n^k = 1$. Les autres coefficients m_h^k sont des nombres entiers, tels que m_h^k sera égal au nombre des valeurs positives et moindres que f (zéro y compris) de x et y qui satisfont à la conguence

$$\gamma^{k+2e} + 1 \equiv \gamma^{k+ye} \pmod{\lambda}.$$

En regardant les simples racines α, α^γ, α^{γ^2}, etc., dont chaque période contient un nombre f, on voit que le produit de deux périodes en contiendra f^2, et de là il est aisé de conclure qu'on aura toujours

$$n^k + m^k + m_1^k + m_2^k + \ldots + m_{e-1}^k = f.$$

Si, dans la formule qui donne le produit des deux périodes η_r, η_{r+k}, on fait successivement

$$r = 0,\ 1,\ 2,\ldots,\ e-1.$$

et qu'on ajoute, on trouve

$$\eta\eta_k + \eta_1\eta_{k+1} + \eta_2\eta_{k+2} + \ldots + \eta_{e-1}\eta_{k-1}$$
$$= n^k ef - m^k - m_1^k - m_2^k - \ldots - m_{e-1}^k,$$

et de là

$$\eta\eta_k + \eta_1\eta_{k+1} + \eta_2\eta_{k+2} + \ldots + \eta_{e-1}\eta_{k-1} = n^k\lambda - f.$$

Donc, d'après la valeur donnée de n^k, cette somme est égale à $-f$, excepté les cas : 1° f pair et $k = 0$; 2° f impair et $k = \frac{1}{2}e$, où cette somme est égale à $\lambda - f$.

En multipliant l'expression donnée du produit de deux périodes η_r, η_{r+k} par η_{r+h}, prenant ensuite

$$r = 0,\ 1,\ 2, \ldots,\ e-1,$$

ajoutant et réduisant à l'aide des formules données ci-dessus, on trouve

$$\eta\eta_k\eta_h + \eta_1\eta_{k+1}\eta_{h+1} + \eta_2\eta_{k+2}\eta_{h+2} + \ldots + \eta_{e-1}\eta_{k-1}\eta_{h-1}$$
$$= -f^2 + \lambda m_h^k,$$

si f est un nombre pair;

$$\eta\eta_k\eta_h + \eta_1\eta_{k+1}\eta_{h+1} + \eta_2\eta_{k+2}\eta_{h+2} + \ldots + \eta_{e-1}\eta_{k-1}\eta_{h-1}$$
$$= -f^2 + \lambda m_{h+\frac{1}{2}e}^k,$$

si f est un nombre impair.

Parce que, dans ces formules, les lettres k et h peuvent être échangées entre elles, on en tire cette propriété remarquable des coefficients du système des équations (A),

$$m_h^k = m_k^h,$$

si f est pair;

$$m_{h+\frac{1}{2}e}^k = m_{k+\frac{1}{2}e}^h,$$

si f est impair.

Une autre relation du même genre provient de l'expression du produit $\eta_r\eta_{r+k}$, en y changeant k en $e-k$ et r en $r+k$, et comparant avec l'expression primitive, on trouve

$$m_h^k = m_{h-k}^{e-k}.$$

Dans le système des équations (A) on peut considérer comme inconnues les e périodes, et ces équations suffiront toujours pour les trouver complétement. En effet, l'élimination des périodes

$$\eta_1, \quad \eta_2, \quad \eta_3, \ldots, \quad \eta_{e-1}$$

donnera une équation du degré e à coefficients entiers pour déterminer la première période η, et puisque, évidemment, toute période peut être regardée comme première, cette équation aura nécessairement comme racines toutes les e périodes

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1}.$$

On aura ainsi l'équation

$$y^e - A_1 y^{e-1} + A_2 y^{e-2} - A_3 y^{e-3} + \ldots \pm A_e = 0,$$

dont les racines sont toutes les e périodes et dont les coefficients A_1, $A_2, \ldots, A_e$ sont des nombres entiers. De plus, si dans le système (A) on prend la première période η comme connue et les autres comme inconnues, toutes ces équations ne sont que linéaires par rapport aux inconnues $\eta_1, \eta_2, \ldots, \eta_{e-1}$; et de là, en résolvant ces équations, après avoir rejeté une quelconque d'entre elles comme superflue, on trouvera les périodes $\eta_1, \eta_2, \ldots, \eta_{e-1}$ exprimées rationnellement par la première η. Le résultat de la résolution des équations (A) pourra toujours être réduit à la forme

$$D\eta_k = B + B_1 \eta + B_2 \eta^2 + B_3 \eta^3 + \ldots + B_{e-1} \eta^{e-1},$$

où B, B_1, $B_2, \ldots, B_{e-1}$ et D sont entiers.

Nous ajoutons encore le théorème important, que toute fonction rationnelle et entière des périodes peut être représentée comme fonction *linéaire* de ces périodes. En effet, au moyen des équations (A) on a le produit de deux périodes quelconques exprimé comme fonction linéaire de toutes les périodes; il suit de là qu'en répétant cette réduction, on parviendra à réduire à la forme linéaire les produits de plusieurs périodes, et, par conséquent aussi, toute fonction entière et rationnelle des périodes. De plus, il est aisé de démontrer qu'une telle fonction ne peut être ramenée à la forme

$$a\eta + a_1 \eta_1 + a_2 \eta_2 + \ldots + a_{e-1} \eta_{e-1}$$

que d'une seule manière; car, si l'on avait aussi

$$b\eta + b_1\eta_1 + b_2\eta_2 + \ldots + b_{e-1}\eta_{e-1}$$

égal à la même fonction rationnelle, il s'ensuivrait

$$a\eta + a_1\eta_1 + \ldots + a_{e-1}\eta_{e-1} = b\eta + b_1\eta_1 + \ldots + b_{e-1}\eta_{e-1},$$

et de là

$$(a-b)\eta + (a_1-b_1)\eta_1 + \ldots + (a_{e-1}-b_{e-1})\eta_{e-1} = 0,$$

en exprimant les périodes par les racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

et divisant par α, on aurait une équation à coefficients entiers du degré $\lambda-2$ dont la racine serait α, ce qu'on sait être impossible.

Une propriété très-importante de toutes les équations rationnelles entre les périodes

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1},$$

c'est de donner toujours des solutions réelles lorsqu'on les envisage comme congruences pour une certaine classe de modules, en sorte qu'à chaque période corresponde un certain nombre entier. Cette correspondance intime entre les périodes comme racines des équations proposées et les racines des congruences analogues nous servira de base pour la recherche des facteurs, et surtout des facteurs premiers des nombres complexes; c'est pour cette raison que nous en donnerons ici les développements nécessaires.

D'abord nous expliquerons une amplification de la définition des congruences dont nous ferons usage dans la suite de ce Mémoire, qui consiste en ce que nous y admettons aussi les périodes

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1}.$$

Le sens de telles congruences est fixé comme il suit :

Deux fonctions rationnelles et entières des périodes à coefficients entiers sont censées congrues par rapport à un module entier donné si, dans leur différence réduite à la forme linéaire

$$a\eta + a_1\eta_1 + \ldots + a_{e-1}\eta_{e-1},$$

tous les coefficients $a, a_1, a_2, \ldots, a_{e-1}$ *sont divisibles par le module.*

Une congruence contenant les périodes à f termes équivaut donc toujours à e congruences pour des nombres entiers, qui sont complétement déterminées parce qu'une fonction rationnelle et entière des periodes n'est réductible à cette forme linéaire que d'une seule manière. Selon cette définition, on pourra opérer sur les congruences qui contiennent les périodes de la même manière que sur les congruences ordinaires.

Cela posé, nous partons de la proposition connue que, dans le produit développé de q facteurs,

$$z(z-1)(z-2)\dots(z-q+1) = z^q - b_1 z^{q-1} + b_2 z^{q-2} - \dots + b_{q-1} z,$$

où q est un nombre premier, tous les coefficients b_1, b_2, b_3,..., b_{q-2} sont divisibles par q, excepté le dernier b_{q-1} qui donne le reste -1. En posant donc

$$z = y - \eta_k,$$

où y est un nombre entier, et négligeant les termes divisibles par le module q, on aura la congruence

$$\begin{aligned}(y-\eta_k)(y-1-\eta_k)(y-2-\eta_k)\dots(y-q+1-\eta_k)\\ \equiv (y-\eta_k)^q - (y-\eta_k) \pmod q.\end{aligned}$$

Observons aussi que, dans le développement de la puissance du binôme $(y-\eta_k)^q$, q étant un nombre premier, tous les termes sont divisibles par q, excepté le premier et le dernier, d'où

$$(y-\eta_k)^q \equiv y^q - \eta_k^q \pmod q.$$

De même, en élevant le polynôme

$$\eta_k = \alpha^{\gamma^k} + \alpha^{\gamma^{k+e}} + \alpha^{\gamma^{k+2e}} + \dots + \alpha^{\gamma^{k+(f-1)e}}$$

à la puissance q, et rejetant tous les termes divisibles par q, on aura

$$\eta_k^q \equiv \alpha^{\gamma^k q} + \alpha^{\gamma^{k+e} q} + \alpha^{\gamma^{k+2e} q} + \dots + \alpha^{\gamma^{k+(f-1)e} q} \pmod q;$$

et de là, en posant $q \equiv \gamma^r \pmod \lambda$,

$$\eta_k^q \equiv \eta_{k+r} \pmod q.$$

Enfin on a, en vertu du théorème de Fermat,

$$y^q \equiv y \pmod{q},$$

d'où

$$(y-\eta_e)(y-1-\eta_k)(y-2-\eta_k)\dots(y-q+1-\eta_k) \equiv \eta_k - \eta_{k+r} \pmod{q}.$$

Supposons maintenant que r soit un multiple de e, en sorte qu'on ait

$$q \equiv \gamma^{re} \pmod{\lambda},$$

ou, ce qui revient au même,

$$q^f \equiv 1 \pmod{\lambda};$$

alors, le second membre de la congruence se réduisant à zéro, on a

$$(y-\eta_k)(y-1-\eta_k)(y-2-\eta_k)\dots(y-q+1-\eta_k) \equiv 0 \pmod{q}.$$

En multipliant les e congruences contenues dans celle-ci pour les valeurs de

$$k = 0,\ 1,\ 2,\dots,\ e-1,$$

et en désignant, pour abréger, par $\varphi(y)$ le produit

$$(y-\eta)(y-\eta_1)(y-\eta_2)\dots(y-\eta_{e-1}),$$

on aura cette congruence pour le module q^e,

$$\varphi(y)\varphi(y-1)\varphi(y-2)\dots\varphi(y-q+1) \equiv 0 \pmod{q^e}.$$

On en conclut aisément que la congruence

$$\varphi(y) \equiv 0 \pmod{q}$$

aura toujours e racines réelles; en observant encore que le produit désigné par $\varphi(y)$ est exactement le premier membre de l'équation

$$y^e - A_1 y^{e-1} + A_2 y^{e-2} - \dots \pm A_e = 0,$$

dont les racines sont les e périodes, on aura ce résultat :

L'équation du degré e, dont les racines sont les périodes à f termes, prise pour congruence par rapport à un module q, nombre premier, qui

satisfait à la condition

$$q^f \equiv 1 \pmod{\lambda},$$

a toujours e racines réelles.

Cela étant, nous établissons ce système de congruences parfaitement analogues au système des équations (A) :

$$(B)\quad \left\{\begin{array}{l} uu \equiv nf + mu + m_1 u_1 + \ldots + m_{e-1} u_{e-1} \\ uu_1 \equiv n^1 f + m^1 u + m_1^1 u_1 + \ldots + m_{e-1}^1 u_{e-1} \\ uu_2 \equiv n^2 f + m^2 u + m_1^2 u_1 + \ldots + m_{e-1}^2 u_{e-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ uu_{e-1} \equiv n^{e-1} f + m^{e-1} u + m_1^{e-1} u + \ldots + m_{e-1}^{e-1} u_{e-1} \end{array}\right\} \pmod{q},$$

où le module q soit un nombre premier, tel qu'on ait

$$q^f \equiv 1 \pmod{\lambda}.$$

L'élimination des $e-1$ des inconnus

$$u,\quad u_1,\quad u_2, \ldots,\quad u_{e-1}$$

donne nécessairement une congruence du degré e qui sera parfaitement conforme à l'équation dont les e racines sont les périodes, savoir,

$$y^e - A_1 y^{e-1} + A_2 y^{e-2} - \ldots \pm A_e \equiv 0 \pmod{q},$$

et, puisque cette congruence a toutes ses racines réelles, on en tirera les valeurs réelles des inconnus

$$u,\quad u_1,\quad u_2, \ldots,\quad u_{e-1}.$$

Ainsi, le système des congruences (B) est toujours résoluble par des nombres entiers réels. Observons aussi que, pour le premier des inconnus u, on peut choisir une quelconque des racines de cette congruence; mais celle-ci une fois déterminée, on ne pourra plus choisir arbitrairement la seconde, la troisième et les autres, puisque l'ordre de ces racines dépend des congruences (B).

La conformité des équations (A) avec les congruences (B) nous conduit à la conclusion, que toutes les réductions et transformations

des fonctions entières des périodes qu'on peut effectuer au moyen des équations (A), seront absolument les mêmes pour les nombres entiers qu'on obtient en remplaçant les périodes

$$\eta,\quad \eta_1,\quad \eta_2,\ldots,\quad \eta_{e-1}$$

par les nombres

$$u,\quad u_1,\quad u_2,\ldots,\quad u_{e-1},$$

et, puisque toutes les équations rationnelles et entières entre les périodes se réduisent à des identités simples, il en sera toujours de même des congruences analogues. Nous avons donc le théorème suivant :

Toute équation qui ne contient que des fonctions rationnelles et entières des périodes donne immédiatement une congruence quand on y remplace les périodes par les nombres entiers correspondants qui satisfont aux congruences (B).

Par exemple, des équations données ci-dessus on tire les congruences

$$u + u_1 + u_2 + \ldots + u_{e+1} \equiv -1 \pmod{q},$$

et

$$uu_k + u_1 u_{k+1} + u_2 u_{k+2} + \ldots + u_{e-1} u_{k-1} \equiv -f, \pmod{q},$$

excepté les cas où f est pair et $k = 0$, ou bien pour f impair et $k = \frac{1}{2}e$, où cette somme est congrue à $\lambda - f$.

§ IV.

Des facteurs premiers de la norme d'un nombre complexe quelconque.

Une fonction rationnelle et entière des périodes à coefficients entiers, c'est-à-dire un nombre complexe contenant les périodes, peut être considéré comme fonction d'une seule période, par exemple de la première η, et, pour cette raison, nous la désignerons simplement par $F(\eta)$. De même, le nombre entier qui en résulte si l'on remplace les périodes

$$\eta,\quad \eta_1,\quad \eta_2,\ldots,\quad \eta_{e-1}$$

par les racines de congruences analogues

$$u,\quad u_1,\quad u_2,\ldots,\quad u_{e-1},$$

sera désigné par $F(u)$, ou, si l'on prend les périodes

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1}$$

respectivement correspondantes aux racines des congruences

$$u_r, \quad u_{r+1}, \quad u_{r+2}, \ldots, \quad u_{r-1},$$

le nombre entier correspondant à $F(\eta)$ sera désigné par $F(u_r)$.

Pour qu'un nombre complexe $F(\eta)$, contenant les périodes seules, soit divisible par un entier non complexe q, il est nécessaire et il suffit que, dans la forme linéaire de ce nombre

$$F(\eta) = a\eta + a_1\eta_1 + a_2\eta_2 + \ldots + a_{e-1}\eta_{e-1},$$

tous les coefficients $a, a_1, a_2, \ldots, a_{e-1}$ aient le facteur commun q. Mais cette méthode de trouver les facteurs entiers non complexes des nombres complexes n'est pas bien applicable au cas d'un nombre complexe donné comme produit de plusieurs facteurs dont la multiplication effective serait très-pénible. Pour ce but, nous ferons usage de ce théorème :

Si une fonction entière rationnelle des périodes à coefficients entiers est divisible par le facteur premier non complexe q, qui satisfait à la congruence

$$q^f \equiv 1 \pmod{\lambda},$$

tous les nombres entiers qu'on déduit de ce nombre complexe en remplaçant les périodes par des racines de congruences analogues, seront divisibles par q. Réciproquement, si tous ces e nombres entiers sont divisibles par q, la fonction des périodes dont ils dérivent le sera aussi.

Au moyen des signes adoptés, ce théorème s'exprime de la manière suivante :

Si l'on a

$$F(\eta) \equiv 0 \pmod{q},$$

où q satisfait à la congruence

$$q^f \equiv 1 \pmod{\lambda},$$

il s'ensuit

$$F(u) \equiv 0, \quad F(u_1) \equiv 0, \quad F(u_2) \equiv 0, \ldots, \quad F(u_{e-1}) \equiv 0 \pmod{q};$$

et, réciproquement, si

$$F(u) \equiv 0, \quad F(u_1) \equiv 0, \ldots, \quad F(u_{e-1}) \equiv 0 \pmod{q},$$

il s'ensuit

$$F(\eta) \equiv 0 \pmod{q}.$$

En effet, supposons $F(\eta)$ réduit à la forme linéaire

$$F(\eta) = a\eta + a_1\eta_1 + a_2\eta_2 + \ldots + a_{e-1}\eta_{e-1}$$

en changeant le terme initial des périodes, nous aurons en même temps

$$\begin{aligned}
F(\eta_1) &= a\eta_1 + a_1\eta_2 + a_2\eta_3 + \ldots + a_{e-1}\eta, \\
F(\eta_2) &= a\eta_2 + a_1\eta_3 + a_2\eta_4 + \ldots + a_{e-1}\eta_1, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
F(\eta_{e-1}) &= a\eta_{e-1} + a_1\eta + a_2\eta_1 + \ldots + a_{e-1}\eta_{e-2}.
\end{aligned}$$

La résolution de ces e équations, linéaires par rapport aux coefficients, donne sans difficulté

$$\lambda a_k = (\eta_k - f)F(\eta) + (\eta_{k+1} - f)F(\eta_1) + \ldots + (\eta_{k-1} - f)F(\eta_{e-1}),$$

si f est pair, et

$$\lambda a_{k+\frac{e}{2}} = (\eta_k - f)F(\eta) + (\eta_{k+1} - f)F(\eta_1) + \ldots + (\eta_{k-1} - f)F(\eta_{e-1}),$$

si f est impair.

Maintenant, si l'on remplace les périodes par les racines des congruences, on a

$$F(u_r) \equiv a u_r + a_1 u_{r+1} + a_2 u_{r+2} + \ldots + a_{e-1} u_{r-1} \pmod{q},$$

et puisque, $F(\eta)$ étant divisible par q, il en sera de même des coefficients a, a_1, $a_2, \ldots$, a_{e-1}, on en conclut que le nombre $F(u_r)$ sera divisible par q pour toutes les valeurs

$$r = 0, 1, 2, \ldots, e-1.$$

De même, on a

$$\lambda a_k \equiv (u_k - f)F(u) + (u_{k+1} - f)F(u_1) + \ldots + (u_{k-1} - f)F(u_{e-1}) \pmod{\lambda},$$

si f est pair, et la même expression est congrue à $\lambda a_{k+\frac{e}{2}}$ si f est impair; donc, si l'on a

$$F(u) \equiv 0, \quad F(u_1) \equiv 0, \ldots, \quad F(u_{e-1}) \equiv 0 \pmod{q},$$

on aura aussi

$$a_k \equiv 0 \pmod{q},$$

pour toutes les valeurs de

$$k = 0, 1, 2, \ldots, e-1,$$

et, par conséquent,

$$F(\eta) \equiv 0 \pmod{q},$$

ce qu'il fallait démontrer.

La norme d'un nombre complexe $F(\eta)$ qui ne contient pas les simples racines α, α^γ, α^{γ^2}, etc., mais seulement les périodes à f termes de ces racines, prise par rapport aux périodes, sera le produit des e facteurs

$$F(\eta), \quad F(\eta_1), \quad F(\eta_2), \ldots, \quad F(\eta_{e-1}),$$

qui est toujours un nombre entier. La norme du même nombre $F(\eta)$, prise par rapport aux diverses valeurs de la racine α, contenue dans les périodes, sera composée de $\lambda - 1 = e \cdot f$ facteurs, dont f à f seront égaux; elle sera donc la $f^{ième}$ puissance de la norme, prise par rapport aux périodes. Nous ne craignons point d'embarras en désignant la norme, prise par rapport aux périodes, par la lettre N, de même que la norme, prise par rapport aux racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0.$$

Donc, en mettant

$$NF(\eta) = F(\eta) \cdot F(\eta_1) \cdot F(\eta_2) \ldots F(\eta_{e-1}),$$

et en substituant aux périodes les racines des congruences, nous avons

$$NF(\eta) \equiv F(u) \cdot F(u_1) \cdot F(u_2) \ldots F(u_{e-1}) \pmod{q}.$$

Cette congruence donne immédiatement le théorème suivant :

Si la norme d'un nombre complexe $F(\eta)$, *composé des périodes*

seules, est divisible par q, un des nombres

$$F(u),\quad F(u_1),\quad F(u_2),\ldots,\quad F(u_{e-1})$$

sera de même divisible par q ; et réciproquement, si l'un de ces nombres est divisible par q, q sera nécessairement facteur de la norme.

Nous allons maintenant discuter les conditions nécessaires pour que la norme d'un nombre complexe quelconque, composé des racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

ait un facteur premier donné. Quant au nombre λ, nous avons trouvé cette condition dans le § I^er^ de ce Mémoire, savoir, que la somme des coefficients d'un nombre complexe doit être divisible par λ pour que la norme ait le facteur λ, et réciproquement. Tous les autres nombres premiers peuvent être rangés selon les exposants auxquels ils appartiennent pour le module λ (*voyez* M. Gauss, *Disquisitiones arithmeticæ*, § LII), et cette classification convient parfaitement aux divers diviseurs de la norme dont les caractères sont intimement liés aux plus petits exposants de ses puissances qui sont congrues à l'unité pour le module λ. Nous supposons donc, comme ci-dessus, que q soit un nombre premier tel que

$$q^f \equiv 1 \pmod{\lambda};$$

mais, désormais, nous ajoutons la condition que q appartienne à l'exposant f, en sorte qu'aucune puissance de q inférieure à la $f^{ième}$ ne soit congrue à l'unité. La puissance d'une racine primitive γ, congrue à un nombre q qui appartient à l'exposant f, sera

$$q \equiv \gamma^{re} \pmod{\lambda},$$

où r n'a aucun facteur commun avec f ; car, si l'on prend

$$q \equiv \gamma^k,$$

la condition

$$q^f \equiv 1$$

donne

$$\gamma^{kf} \equiv 1;$$

il suit de là

$$kf \equiv 0 \pmod{\lambda - 1},$$

et puisque

$$\lambda - 1 = ef,$$

on a

$$k \equiv 0 \pmod{e},$$

ou

$$k = re$$

et

$$q \equiv \gamma^{re} \pmod{\lambda}.$$

On voit aussi qu'à cause de la condition que q *appartienne* à l'exposant f, le nombre r doit être premier à f; car, si r et f avaient un facteur commun n, on pourrait poser

$$r = nr' \quad \text{et} \quad f = nf',$$

on aurait ainsi

$$q^{f'} \equiv \gamma^{nr'ef'} \equiv \gamma^{r'(\lambda-1)} \equiv 1 \pmod{\lambda},$$

et la puissance $q^{f'}$, inférieure à q^f, serait congrue à l'unité, ce qui est contre l'hypothèse.

Cela posé, nous élevons le nombre complexe

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \ldots + a_{\lambda-2}\alpha^{\lambda-2}$$

à la puissance q. En rejetant tous les termes divisibles par q, nous aurons

$$f(\alpha)^q \equiv a^q + a_1^q\alpha^q + a_2^q\alpha^{2q} + \ldots + a_{\lambda-2}^q\alpha^{(\lambda-2)q} \pmod{q}.$$

Donc, en observant que

$$a_k^q \equiv a_k \pmod{q},$$

on a la congruence

$$f(\alpha)^q \equiv f(\alpha^q) \pmod{q},$$

et, en répétant la même opération, on a plus généralement

$$f(\alpha)^{q^h} \equiv f(\alpha^{q^h}) \pmod{q}.$$

Mettant à présent

$$h = 0, 1, 2, \ldots, f-1,$$

et multipliant toutes ces congruences, on a

$$f(\alpha)^{1+q+q^2+\ldots+q^{f-1}} \equiv f(\alpha)f(\alpha^q)f(\alpha^{q^2})\ldots f(\alpha^{q^{f-1}}) \pmod{q},$$

et, en prenant

$$q \equiv \gamma^{re} \pmod{\lambda},$$

et changeant α en α^{γ^m}, cette congruence devient

$$f\left(\alpha^{\gamma^m}\right)^{1+q+q^2+\ldots+q^{f-1}} \equiv f\left(\alpha^{\gamma^m}\right).f\left(\alpha^{\gamma^{m+re}}\right).f\left(\alpha^{\gamma^{m+2re}}\right)\ldots f\left(\alpha^{\gamma^{m+(f-1)re}}\right).$$

Prenons maintenant, pour m, e valeurs incongrues par rapport au module e, et multiplions ces e congruences; nous aurons

$$\left[\Pi f\left(\alpha^{\gamma^m}\right)\right]^{1+q+q^2+\ldots+q^{f-1}} \equiv \mathrm{N} f(\alpha) \pmod{q},$$

où le signe du produit Π s'étend à toutes les valeurs du nombre m qui sont incongrues par rapport au module e. D'où, en supposant $\mathrm{N} f(\alpha)$ divisible par q,

$$\left[\Pi f\left(\alpha^{\gamma^m}\right)\right]^{1+q+q^2+\ldots+q^{f-1}} \equiv 0 \pmod{q}.$$

En élevant à la puissance $q-1$, multipliant par $\Pi f\left(\alpha^{\gamma^m}\right)$ et observant que, pour tout nombre complexe, l'on a

$$\varphi(\alpha)^{q^f} \equiv \varphi(\alpha) \pmod{q},$$

on obtient enfin

$$\Pi f\left(\alpha^{\gamma^m}\right) \equiv 0 \pmod{q},$$

et de là le théorème suivant :

Si la norme d'un nombre complexe $f(\alpha)$ est divisible par q (nombre premier qui appartient à l'exposant f), il faut que le produit de e à e des $\lambda - 1$ nombres conjugués représentés par $f\left(\alpha^{\gamma^m}\right)$, pour lesquels m n'ait que des valeurs incongrues par rapport au module e, soit divisible par q.

De ce théorème il suit aussi, comme corollaire :

Si la norme d'un nombre complexe $f(\alpha)$ est divisible par un nombre premier q qui appartient à l'exposant f, il faut qu'elle contienne ce facteur f fois, de manière qu'elle soit toujours divisible par q^f.

Cherchons maintenant les conditions qui doivent avoir lieu entre

les coefficients du nombre complexe $f(\alpha)$ pour que sa norme soit divisible par q. On sait que toutes les f racines de l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

qui sont contenues dans une seule période à f termes, sont en même temps les racines d'une équation du degré f de la forme

$$\alpha^f + P_1 \alpha^{f-1} + P_2 \alpha^{f-2} + \ldots + P_f = 0,$$

dont les coefficients P_1, P_2, etc., sont des fonctions entières et rationnelles des périodes

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1}.$$

Au moyen de cette équation, on pourra éliminer toutes les puissances de α supérieures à α^{f-1} de l'expression du nombre complexe

$$f(\alpha) = a + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + \ldots + a_{\lambda-2} \alpha^{\lambda-2};$$

donc on aura cette forme

$$f(\alpha) = \varphi(\eta) + \alpha \varphi_1(\eta) + \alpha^2 \varphi_2(\eta) + \ldots + \alpha^{f-1} \varphi_{f-1}(\eta),$$

où

$$\varphi(\eta), \quad \varphi_1(\eta), \quad \varphi_2(\eta), \ldots, \quad \varphi_{f-1}(\eta)$$

désignent des nombres entiers complexes contenant les périodes seules. On voit aussi qu'un nombre complexe donné n'aura jamais deux représentations différentes par cette forme.

Cela posé, nous considérons le produit des e facteurs :

$$\left[c f(\alpha) + c_1 f\left(\alpha^{\gamma^e}\right) + c_2 f\left(\alpha^{\gamma^{2e}}\right) + \ldots + c_{f-1} f\left(\alpha^{\gamma^{(f-1)e}}\right)\right]$$

$$\times\left[c f\left(\alpha^{\gamma}\right) + c_1 f\left(\alpha^{\gamma^{e+1}}\right) + c_2 f\left(\alpha^{\gamma^{2e+1}}\right) + \ldots + c_{f-1} f\left(\alpha^{\gamma^{(f-1)e+1}}\right)\right]$$

. . . . . .

$$\times\left[c f\left(\alpha^{\gamma^{e-1}}\right) + c_1 f\left(\alpha^{\gamma^{2e-1}}\right) + c_2 f\left(\alpha^{\gamma^{3e-1}}\right) + \ldots + c_{f-1} f\left(\alpha^{\gamma^{fe-1}}\right)\right].$$

En effectuant la multiplication on voit que tous les termes contiendront un de ces produits $\Pi f\left(\alpha^{\gamma^m}\right)$ où m a e valeurs incongrues par rapport au module e; donc, en vertu du théorème que nous venons de démontrer, le produit proposé sera divisible par q en même temps

que $\mathrm{N} f(\alpha)$, quelles que soient les quantités

$$c, \quad c_1, \quad c_2, \ldots, \quad c_{f-1}.$$

Prenons pour $f(\alpha)$ la forme

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

et pour $f\left(\alpha^\gamma\right)$, $f\left(\alpha^{\gamma^2}\right)$, etc., les expressions qu'on déduit de celle-ci en changeant α en α^γ, α^{γ^2}, etc. Posons de plus

$$\begin{aligned}
&c + c_1 + c_2 + \ldots + c_{f-1} = \mathrm{C},\\
&\alpha c + \alpha^{\gamma^e} c_1 + \alpha^{\gamma^{2e}} c_2 + \ldots + \alpha^{\gamma^{(f-1)e}} c_{f-1} = \mathrm{C}_1,\\
&\alpha^2 c + \alpha^{2\gamma^e} c_2 + \alpha^{2\gamma^{2e}} c_2 + \ldots + \alpha^{2\gamma^{(f-1)e}} c_{f-1} = \mathrm{C}_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\alpha^{f-1} c + \alpha^{(f-1)\gamma^e} c_1 + \alpha^{(f-1)\gamma^{2e}} c_2 + \ldots + \alpha^{(f-1)\gamma^{(f-1)e}} c_{f-1} = \mathrm{C}_{f-1},
\end{aligned}$$

nous aurons cette transformation du produit proposé,

$$\begin{aligned}
&[\mathrm{C}\varphi(\eta) + \mathrm{C}_1\varphi_1(\eta) + \mathrm{C}_2\varphi_2(\eta) + \ldots + \mathrm{C}_{f-1}\varphi_{f-1}(\eta)]\\
&\times [\mathrm{C}\varphi(\eta_1) + \mathrm{C}_1\varphi_1(\eta_1) + \mathrm{C}_2\varphi_2(\eta_1) + \ldots + \mathrm{C}_{f-1}\varphi_{f-1}(\eta_1)]\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\times [\mathrm{C}\varphi(\eta_{e-1}) + \mathrm{C}_1\varphi_1(\eta_{e-1}) + \mathrm{C}_2\varphi_2(\eta_{e-1}) + \ldots + \mathrm{C}_{f-1}\varphi_{f-1}(\eta_{e-1})],
\end{aligned}$$

qui sera divisible par q en même temps que $\mathrm{N} f(\alpha)$ pour toutes les valeurs des quantités

$$\mathrm{C}, \quad \mathrm{C}_1, \quad \mathrm{C}_2, \ldots, \quad \mathrm{C}_{f-1},$$

qui sont tout à fait arbitraires aussi bien que

$$c, \quad c_1, \quad c_2, \ldots, \quad c_{f-1}.$$

Ce produit étant une norme prise par rapport aux périodes, pour qu'il soit divisible par q il faut et il suffit qu'on ait

$$\mathrm{C}\varphi(u_r) + \mathrm{C}_1\varphi_1(u_r) + \mathrm{C}_2\varphi_2(u_r) + \ldots + \mathrm{C}_{f-1}\varphi_{f-1}(u_r) \equiv 0 \pmod{q},$$

pour quelqu'une des valeurs de

$$r = 0,\ 1,\ 2,\ldots,\ e-1,$$

et parce que les coefficients

$$C,\ C_1,\ C_2,\ldots,\ C_{f-1}$$

sont arbitraires, il faut qu'on ait séparément les f congruences

$$\varphi(u_r) \equiv 0,\quad \varphi_1(u_r) \equiv 0,\ldots,\quad \varphi_{f-1}(u_r) \equiv 0 \pmod{q}.$$

On a donc ce théorème :

Si la norme d'un nombre complexe $f(\alpha)$ est divisible par un nombre premier q, qui appartient à l'exposant f pour le module λ, il faut que les f congruences

$$\varphi(u_r) \equiv 0,\quad \varphi_1(u_r) \equiv 0,\quad \varphi_2(u_r) \equiv 0,\ldots,\quad \varphi_{f-1}(u_r) \equiv 0 \pmod{q},$$

qu'on obtient en mettant le nombre $f(\alpha)$ sous la forme

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

et remplaçant les e périodes à f termes par les racines de congruences correspondantes, aient lieu pour une certaine valeur de r. Réciproquement, si ces f congruences ont lieu, la norme de $f(\alpha)$ sera divisible par q.

On peut aussi déterminer la condition pour que la norme d'un nombre complexe $f(\alpha)$ soit divisible par q, en faisant

$$f(\alpha) \cdot f\left(\alpha^{\gamma^e}\right) \cdot f\left(\alpha^{\gamma^{2e}}\right) \ldots f\left(\alpha^{\gamma^{(f-1)e}}\right) = F(\eta).$$

Ce produit étant une fonction symétrique de toutes les racines contenues dans l'une des périodes ne sera qu'une fonction des périodes, à cause de quoi nous l'avons désigné par $F(\eta)$. Il suit de là

$$Nf(\alpha) = F(\eta) \cdot F(\eta_1) \cdot F(\eta_2) \ldots F(\eta_{e-1}),$$

et, par conséquent, la condition nécessaire et suffisante pour que $Nf(\alpha)$ soit divisible par q revient simplement à ce que $F(u_r)$ soit divisible par q pour une certaine valeur de r. Ainsi, la même con-

dition pour laquelle nous avons trouvé les f congruences

$$\varphi(u_r) \equiv 0, \quad \varphi_1(u_r) \equiv 0, \quad \text{etc.},$$

linéaires par rapport aux coefficients du nombre complexe $f(\alpha)$, est exprimée par la seule congruence du degré f,

$$F(u_r) \equiv 0 \pmod{q}.$$

Si pour un nombre complexe quelconque

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

les f congruences

$$\varphi(u_r) \equiv 0, \quad \varphi_1(u_r) \equiv 0, \ldots, \quad \varphi_{f-1}(u_r) \equiv 0 \pmod{q}$$

ont lieu, nous dirons simplement que ce nombre complexe $f(\alpha)$ est congru à zéro, par rapport au module q, pour

$$\eta = u_r, \quad \eta_1 = u_{r+1}, \quad \eta_2 = u_{r+2}, \ldots, \quad \eta_{e-1} = u_{r-1},$$

où il suffira aussi d'écrire seulement la condition

$$\eta = u_r$$

qui entraîne les autres.

Cela posé, il est évident qu'un des facteurs d'un produit de deux ou de plusieurs nombres complexes étant congru à zéro pour $\eta = u_r$, il en sera de même du produit développé; mais le théorème réciproque exige une démonstration particulière. Soit donc

$$f(\alpha) \cdot \varphi(\alpha) = \chi(\alpha),$$

et, par hypothèse,

$$\chi(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad \eta = u_r;$$

nous prouverons que l'un des deux facteurs $f(\alpha)$ ou $\varphi(\alpha)$ doit être aussi congru à zéro pour $\eta = u_r$. En effet, en posant

$$f(\alpha) \cdot f\left(\alpha^{\gamma^e}\right) \cdot f\left(\alpha^{\gamma^{2e}}\right) \ldots f\left(\alpha^{\gamma^{(f-1)e}}\right) = F(\eta),$$

$$\varphi(\alpha) \cdot \varphi\left(\alpha^{\gamma^e}\right) \cdot \varphi\left(\alpha^{\gamma^{2e}}\right) \ldots \varphi\left(\alpha^{\gamma^{(f-1)e}}\right) = \Phi(\eta),$$

$$\chi(\alpha) \cdot \chi\left(\alpha^{\gamma^e}\right) \cdot \chi\left(\alpha^{\gamma^{2e}}\right) \ldots \chi\left(\alpha^{\gamma^{(f-1)e}}\right) = X(\eta),$$

on aura

$$F(\eta)\Phi(\eta) = X(\eta),$$

et, puisque par l'hypothèse $\chi(\alpha)$ est congru à zéro pour $\eta = u_r$, on aura aussi

$$X(u_r) \equiv o \pmod{q}.$$

Il suit de là que l'un des nombres $F(u_r)$ ou $\Phi(u_r)$ doit de même être congru à zéro, et, en remplaçant la congruence

$$F(u_r) \equiv o \pmod{q}$$

par les f congruences équivalentes, qu'on est convenu d'exprimer par

$$f(\alpha) \equiv o \pmod{q} \quad \text{pour} \quad \eta = u_r,$$

on en conclut ce théorème :

La condition

$$f(\alpha) \equiv o \pmod{q}$$

pour $\eta = u_r$ est toujours la même pour un nombre complexe, soit qu'il consiste de facteurs, soit qu'il ait la forme développée.

De là découle aussi cet autre théorème, qu'on peut regarder comme une généralisation du premier théorème de ce paragraphe, parce qu'il donne, pour les nombres complexes quelconques $f(\alpha)$, la même condition que cet autre pour les nombres complexes des périodes :

Pour qu'un nombre complexe quelconque, représenté comme produit de plusieurs facteurs, soit divisible par q, il faut et il suffit que, pour toutes les substitutions

$$\eta = u_r, \quad \eta = u_1, \quad \eta = u_2, \ldots, \quad \eta = u_{e-1},$$

un de ses facteurs soit congru à zéro pour le module q.

Nous terminerons cette discussion des facteurs premiers de la norme d'un nombre complexe quelconque, en montrant encore une autre manière très-simple et très-utile d'exprimer les f congruences contenues dans l'énoncé

$$f(\alpha) \equiv o \pmod{q} \quad \text{pour} \quad \eta = u_r.$$

Pour cela, nous avons besoin d'un nombre complexe contenant les périodes seules dont la norme, prise par rapport aux périodes, soit divisible par q sans être divisible par q^2. De tels nombres existent toujours, et à l'ordinaire ils s'offrent d'eux-mêmes; par exemple, parmi les simples nombres

$$u - \eta, \quad u_1 - \eta, \quad u_2 - \eta, \ldots, \quad u_{e-1} - \eta,$$

dont les normes sont toutes divisibles par q, il y en aura presque toujours plusieurs qui satisferont à la condition requise; mais dans certains cas il se pourrait que les normes de tous ces nombres fussent aussi divisibles par q^2. Alors on fera usage du nombre complexe

$$\psi(\eta) = \lambda - f - u\eta - u_1\eta_1 - u_2\eta_2 - \ldots - u_{e-1}\eta_{e-1}.$$

En remplaçant les périodes par les racines des congruences, on a toujours

$$\psi(u_r) \equiv \lambda \pmod{q},$$

à l'exception des deux cas : 1° de f pair et $r = 0$, où l'on a

$$\psi(u) \equiv 0;$$

2° de f impair et $r = \frac{1}{2}e$, où l'on a

$$\psi\left(u_{\frac{e}{2}}\right) \equiv 0.$$

De là, en appliquant le premier et le second théorème de ce paragraphe, on conclut que $\mathrm{N}\psi(\eta)$ est toujours divisible par q, mais que le produit

$$\Psi(\eta) = \psi(\eta_1) \cdot \psi(\eta_2) \cdot \psi(\eta_3) \ldots \psi(\eta_{e-1})$$

n'est pas divisible par q. Observons aussi que le produit $\Psi(\eta_r)\,\Psi(\eta_s)$, tant que r et s ne sont pas égaux, contient toujours tous les facteurs de la norme $\mathrm{N}\psi(\eta)$, et que, par conséquent, il est divisible par q. Cela étant, développons la norme de $\psi(\eta) + q$, en rejetant tous les termes divisibles par q^2, ce qui donne

$$\mathrm{N}[\psi(\eta) + q]$$
$$\equiv \mathrm{N}\psi(\eta) + q[\Psi(\eta) + \Psi(\eta_1) + \ldots + \Psi(\eta_{e-1})] \pmod{q^2};$$

multipliant encore par $\Psi(\eta)$ et rejetant les termes divisibles par q^2, nous aurons

$$\Psi(\eta)\,\mathrm{N}[\psi(\eta)+q]\equiv\Psi(\eta)\,\mathrm{N}\psi(\eta)+q[\Psi(\eta)]^2 \pmod{q^2}.$$

Maintenant, si $\mathrm{N}\psi(\eta)$ n'est pas divisible par q^2, mais seulement par q, $\psi(\eta)$ est un nombre complexe tel qu'on le désire. Mais s'il arrivait que $\mathrm{N}\psi(\eta)$ contînt le facteur q^2, on aurait

$$\Psi(\eta)\,\mathrm{N}[\psi(\eta)+q]\equiv q[\Psi(\eta)]^2 \pmod{q^2}:$$

on voit que la norme du nombre complexe $\psi(\eta)+q$ ne pourrait être divisible par q^2. Ainsi, l'un des deux nombres complexes $\psi(\eta)$ ou $\psi(\eta)+q$ satisfait toujours à la condition exigée.

Soit donc $\psi(\eta)$ un nombre complexe, tel qu'on ait

$$\mathrm{N}\psi(\eta)\equiv 0 \pmod{q},$$

sans que

$$\mathrm{N}\psi(\eta)\equiv 0 \pmod{q^2};$$

soit aussi

$$\psi(u)\equiv 0 \pmod{q},$$

et posons, pour abréger,

$$\psi(\eta_1)\cdot\psi(\eta_2)\cdot\psi(\eta_3)\ldots\psi(\eta_{e-1})=\Psi(\eta),$$

je dis que *les f congruences comprises dans l'énoncé*

$$f(\alpha)\equiv 0 \pmod{q}$$

pour $\eta=u_r$ sont équivalentes à la congruence

$$f(\alpha)\Psi(\eta_{e-r})\equiv 0 \pmod{q}.$$

En effet, d'après les principes établis dans le § III, on conclut de l'expression de $\Psi(\eta)$,

$$\Psi(u_r)\equiv\psi(u_{r+1})\cdot\psi(u_{r+2})\ldots\psi(u_{r-1}) \pmod{q};$$

et puisqu'on a

$$\psi(u)\equiv 0 \pmod{q},$$

on voit qu'on aura toujours

$$\Psi(u_r)\equiv 0,$$

excepté le seul cas $r=0$. Or nous savons que, pour avoir

$$f(\alpha)\Psi(\eta_{e-r})\equiv 0 \pmod{q},$$

il faut et il suffit qu'on ait pour chacune des suppositions

$$\eta = u, \quad \eta = u_1, \quad \eta = u_2, \ldots, \quad \eta = u_{e-1},$$

ou

$$f(\alpha) \equiv 0 \pmod{q},$$

ou

$$\Psi(\eta_{e-r}) \equiv 0 \pmod{q};$$

et puisque, pour $\eta = u_r$, le second facteur, qui devient $\Psi(u)$, n'est pas congru à zéro, il s'ensuit nécessairement

$$f(\alpha) \equiv 0$$

pour $\eta = u_r$. Réciproquement, si l'on a

$$f(\alpha) \equiv 0 \pmod{q}$$

pour $\eta = u_r$, le produit $f(\alpha)\,\Psi(\eta_{e-r})$ est divisible par q, parce que pour $\eta = u_r$ le premier facteur $f(\alpha)$, et pour toutes les autres substitutions

$$\eta = u, \quad \eta = u_1, \ldots, \quad \eta = u_{r-1}, \quad \eta = u_{r+1}, \ldots, \quad \eta = u_{e-1},$$

le second facteur $\Psi(\eta_{e-r})$ est congru à zéro.

§ V.

Définition et propriétés générales des facteurs idéaux d'un nombre complexe.

Au moyen des résultats trouvés dans le paragraphe précédent, nous serons en état d'assigner tous les nombres complexes dont les normes ont un facteur premier donné; voyons maintenant si, parmi tous ces nombres complexes, il y en a un ou plusieurs dont les normes soient *égales* à ce nombre premier même. D'abord nous savons que quand la norme d'un nombre complexe $f(\alpha)$, prise par rapport aux racines α, est divisible par le nombre premier q qui appartient à l'exposant f, elle ne peut pas être égale à q, à moins qu'on n'ait

$$f = 1,$$

c'est-à-dire à moins que q, appartenant à l'exposant 1, n'ait la forme

linéaire

$$q = m\lambda + 1.$$

Cela tient à ce que toute norme est de la forme linéaire $m\lambda + 1$ ou à ce que toute norme divisible par q doit avoir le facteur q^f. Mais parmi les nombres complexes contenant les périodes à f termes, il pourra y en avoir dont les normes prises par rapport aux périodes soient égales au nombre premier q. Donc, il se pourra qu'un nombre premier q, appartenant à l'exposant f, soit décomposable en e facteurs conjugués contenant les périodes à f termes, en sorte qu'on ait

$$\varphi(\eta) \cdot \varphi(\eta_1) \cdot \varphi(\eta_2) \dots \varphi(\eta_{e-1}) = \mathrm{N}\varphi(\eta) = q,$$

et en particulier, pour le cas de $f = 1$, il se pourra qu'un nombre premier p de la forme $m\lambda + 1$ soit égal à la norme d'un nombre complexe $f(\alpha)$, en sorte qu'on ait

$$f(\alpha) \cdot f(\alpha^2) \cdot f(\alpha^3) \dots f(\alpha^{\lambda-1}) = \mathrm{N} f(\alpha) = p.$$

Mais il s'en faut de beaucoup que chaque nombre premier appartenant à l'exposant f soit décomposable en e facteurs premiers complexes. On distinguera plutôt deux classes de tous les nombres premiers, les uns qui peuvent être représentés comme normes, ainsi que nous venons de l'expliquer, les autres qui n'admettent pas une telle décomposition en facteurs conjugués.

En supposant toujours q premier et appartenant à l'exposant f, sans exclure le cas de $f = 1$, nous aurons pour un nombre q de la première classe,

$$\varphi(\eta) \cdot \varphi(\eta_1) \cdot \varphi(\eta_2) \dots \varphi(\eta_{e-1}) = \mathrm{N}\varphi(\eta) = q.$$

Le nombre complexe $\varphi(\eta)$, dont la norme est un nombre premier, n'admet aucune décomposition ultérieure en deux facteurs, sans que l'un de ces facteurs soit une unité complexe. En effet, si l'on avait

$$\varphi(\eta) = \mathrm{F}(\alpha) \cdot \mathrm{G}(\alpha),$$

en prenant la norme par rapport aux racines α, on aurait

$$\mathrm{N}\varphi(\eta) = q^f = \mathrm{NF}(\alpha) \cdot \mathrm{NG}(\alpha),$$

et puisque l'une de ces deux normes, par exemple $\mathrm{NF}(\alpha)$ divisible par q, doit être divisible par q^f, on aura nécessairement

$$\mathrm{NF}(\alpha) = q^f, \quad \text{d'où} \quad \mathrm{NG}(\alpha) = 1,$$

ou bien $\mathrm{G}(\alpha)$ sera une unité complexe. Pour cette raison, tout nombre complexe $\varphi(\eta)$, dont la norme est un nombre premier, sera appelé *nombre premier complexe*. Ainsi, tout nombre premier non complexe q de notre première classe se compose de e facteurs *premiers complexes*.

Pour distinguer les facteurs premiers du nombre q, nous ferons usage des nombres

$$u, \quad u_1, \quad u_2, \ldots, \quad u_{e-1}$$

correspondants aux périodes. En les substituant, on aura pour une certaine valeur de r,

$$\varphi(u_r) \equiv 0 \pmod{q},$$

condition nécessaire pour que la norme de $\varphi(\eta)$ soit divisible par q; on voit par là que, pour tous les divers facteurs premiers de q, on a

$$\begin{aligned}
\varphi(\eta) &\equiv 0 \quad \text{pour} \quad \eta = u_r, \\
\varphi(\eta_1) &\equiv 0 \quad \text{pour} \quad \eta = u_{r-1}, \\
\varphi(\eta_2) &\equiv 0 \quad \text{pour} \quad \eta = u_{r-2},
\end{aligned}$$

et généralement

$$\varphi(\eta_k) \equiv 0 \quad \text{pour} \quad \eta = u_{r-k}.$$

Nous distinguerons donc les e facteurs premiers conjugués du nombre q selon les racines de congruences qui doivent être choisies comme correspondantes aux périodes pour que chacun de ces facteurs premiers complexes soit congru à zéro pour le module q.

Lorsqu'on multiplie un nombre premier complexe $\varphi(\eta)$, pour lequel on a

$$\varphi(\eta) \equiv 0 \pmod{q} \quad \text{pour} \quad \eta = u_r,$$

par un nombre complexe quelconque $f(\alpha)$, le produit développé

$$\varphi(\eta) f(\alpha) = \mathrm{F}(\alpha)$$

satisfera toujours à

$$\mathrm{F}(\alpha) \equiv 0 \quad \text{pour} \quad \eta = u_r.$$

Réciproquement, si un nombre complexe $f(\alpha)$ satisfait à

$$F(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad n = u_r,$$

je dis qu'il contiendra nécessairement le facteur premier $\varphi(n)$. En effet, le nombre $\varphi(n_r)$, dont la norme est égale à q et qui est congru à zéro pour $n = u$, est un de ces nombres complexes que nous avons désignés par $\psi(n)$ dans le paragraphe précédent, à l'aide desquels la condition

$$F(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad n = u_r$$

s'exprime par la simple congruence

$$F(\alpha)\Psi(n_{e-r}) \equiv 0 \pmod{q}.$$

Prenant donc

$$\varphi(n_r) = \psi(n)$$

et

$$\Psi(n) = \varphi(n_{r+1}) \cdot \varphi(n_{r+2}) \cdots \varphi(n_{r-1}),$$

et, par conséquent,

$$\Psi(n_{e-r}) = \varphi(n_1) \cdot \varphi(n_2) \cdot \varphi(n_3) \cdots \varphi(n_{e-1}),$$

de l'hypothèse

$$F(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad n = u_r,$$

on conclut

$$F(\alpha) \cdot \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_{e-1}) \equiv 0 \pmod{q};$$

on pourra donc poser

$$F(\alpha) \cdot \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_{e-1}) = q f(\alpha);$$

enfin, en multipliant par $\varphi(n)$ et divisant par

$$\varphi(n) \cdot \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_{e-1}) = q,$$

on aura

$$F(\alpha) = \varphi(n) f(\alpha).$$

Donc, $F(\alpha)$ a effectivement le facteur $\varphi(n)$. Nous voyons par là que la condition

$$F(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad n = u_r$$

définit complétement un facteur premier complexe $\varphi(n)$, contenu dans le nombre $F(\alpha)$ toutes les fois que le nombre premier $\varphi(n)$ existe

réellement, c'est-à-dire que q est décomposable en e facteurs premiers conjugués.

Supposons à présent que q soit un nombre premier qui n'admet pas de décomposition en e facteurs conjugués, ou qui ne saurait être représenté comme norme d'un nombre complexe contenant les périodes à f termes. Alors on ne pourra plus isoler un facteur premier d'un nombre complexe $f(\alpha)$ satisfaisant à la condition

$$f(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad \eta = u_r,$$

mais nous dirons néanmoins que ce nombre complexe contient un facteur premier complexe du nombre q, que nous appellerons *facteur premier idéal* du nombre premier q; et puisque nous avons vu que les e facteurs premiers du nombre q, s'ils existent effectivement, sont distingués en ce que chacun d'entre eux devient congru à zéro pour une certaine substitution des racines de congruences au lieu des périodes, nous désignerons ce facteur premier idéal de q comme *appartenant à la substitution* $\eta = u_r$. Un tel facteur idéal, qui ne subsiste pas par soi-même, mais qui a une existence effective dans la combinaison avec les autres facteurs du nombre complexe, dans lequel il est contenu, sera donc défini complétement comme il suit :

Si un nombre complexe $f(\alpha)$ *satisfait à la condition*

$$f(\alpha) \equiv 0 \pmod{q} \quad \textit{pour} \quad \eta = u_r,$$

nous dirons qu'il contient le facteur premier idéal du nombre premier q *qui appartient à la substitution* $\eta = u_r$.

Quoiqu'il n'y ait rien d'obscur dans la définition, nous allons expliquer rapidement pourquoi nous avons désigné cette condition de congruence de $f(\alpha)$ par le nom de *facteur idéal* de ce nombre complexe, tout en observant que les développements seuls de la théorie pourront justifier une telle innovation. A cause de l'analogie frappante qui règne entre les facteurs premiers idéaux et les facteurs complexes ordinaires, la dénomination servira à simplifier extrêmement les énoncés des théorèmes. Mais cela ne constitue pas l'avantage principal de la théorie nouvelle; nous croyons surtout que les facteurs

idéaux rendent visible, pour ainsi dire, la constitution intérieure des nombres, en sorte que leurs propriétés essentielles soient mises dans leur jour. Un nombre complexe satisfaisant à plusieurs des conditions que nous regardons comme facteurs idéaux de ce nombre, quoiqu'il ne soit pas décomposable en facteurs complexes, se comporte tout à fait comme un nombre composé, et c'est pour cela que nous le considérons en quelque sorte comme un produit de facteurs. L'Algèbre, l'Arithmétique et la Géométrie offrent des analogies nombreuses à notre théorie. On décompose, par exemple, les fonctions rationnelles et entières d'une seule variable en facteurs linéaires, quoique ces facteurs isolés n'existent qu'en des cas particuliers; c'est pour ce but qu'on a créé les quantités imaginaires. En Géométrie, on parle d'une droite passant par les points d'intersection de deux cercles, quand même les points d'intersection n'existent pas. Dans cet exemple, la propriété permanente que les tangentes menées d'un point quelconque de cette ligne aux deux cercles, sont égales entre elles, est l'analogie de la propriété permanente du nombre complexe

$$f(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad n = u_r,$$

et la propriété accidentelle de cette ligne, de passer par les points d'intersection des deux cercles, est de même analogue à la propriété accidentelle du nombre complexe $f(\alpha)$, d'avoir un facteur premier existant $\varphi(n)$. Enfin, l'idée de considérer des facteurs idéaux des nombres complexes est, au fond, la même que celle qui a procréé les nombres complexes eux-mêmes. En effet, on sait que M. Gauss, en observant que, dans la recherche des lois de réciprocité entre les résidus biquadratiques, les nombres premiers de la forme $4n+1$ se comportaient comme nombres composés, les a décomposés en facteurs imaginaires de la forme $a+b\sqrt{-1}$, et qu'il a jeté par là les fondements de la théorie générale des nombres complexes.

Nous avons fixé le sens d'un facteur premier idéal d'un nombre complexe $f(\alpha)$ par la condition

$$f(\alpha) \equiv 0 \pmod{q} \quad \text{pour} \quad n = u_r,$$

qui en elle-même n'est qu'une manière concise d'exprimer que les f

congruences

$$\varphi(u_r) \equiv 0, \quad \varphi_1(u_r) \equiv 0, \quad \varphi_2(u_r) \equiv 0, \ldots, \quad \varphi_{f-1}(u_r) \equiv 0 \pmod{q}$$

ont lieu en même temps, congruences qu'on obtient en mettant le nombre $f(\alpha)$ sous la forme

$$f(\alpha) = \varphi(n) + \alpha\varphi_1(n) + \alpha^2\varphi_2(n) + \ldots + \alpha^{f-1}\varphi_{f-1}(n),$$

et remplaçant les périodes par les racines des congruences correspondantes. Nous savons aussi que ces f congruences sont comprises dans cette seule,

$$f(\alpha)\Psi(n_{e-r}) \equiv 0 \pmod{q},$$

où $\Psi(n)$ désigne le produit de $e-1$ facteurs

$$\Psi(n) = \psi(n_1)\cdot\psi(n_2)\ldots\psi(n_{e-1}),$$

$\psi(n)$ étant un nombre complexe qui donne

$$\psi(u) \equiv 0 \pmod{q},$$

et dont la norme, divisible par q, ne soit pas divisible par q^2. Nous pouvons donc énoncer la définition des facteurs premiers idéaux comme il suit :

Si le nombre complexe $f(\alpha)$ satisfait à la congruence

$$f(\alpha)\Psi(n_{e-r}) \equiv 0 \pmod{q},$$

où $\Psi(n)$ désigne le produit des $e-1$ facteurs

$$\Psi(n) = \psi(n_1)\cdot\psi(n_2)\ldots\psi(n_{e-1}),$$

et $\psi(n)$ un nombre complexe tel qu'on ait

$$\psi(u) \equiv 0 \pmod{q},$$

et dont la norme, divisible par q, ne soit pas divisible par q^2, nous dirons que $f(\alpha)$ contient le facteur premier idéal du nombre q, qui appartient à la substitution $n = u_r$.

Pour introduire la multiplicité d'un facteur premier idéal, nous généralisons la définition précédente comme il suit :

Le nombre complexe $f(\alpha)$ est censé contenir exactement n fois

le facteur premier idéal du nombre q, qui appartient à la substitution $\eta = u_r$, *lorsqu'il satisfait à la congruence*

$$f(\alpha)[\Psi(\eta_{e-r})]^n \equiv 0 \pmod{q^n},$$

sans que la congruence

$$f(\alpha)[\Psi(\eta_{e-r})]^{n+1} \equiv 0 \pmod{q^{n+1}}$$

ait lieu.

Nous remarquons aussi que la notion du nombre ou facteur complexe idéal sera employée aussi bien dans le sens plus large où les nombres complexes *existants*, comme cas particuliers, sont compris parmi les nombres complexes *idéaux*, que dans le sens plus étroit où les nombres *idéaux* signifient le contraire des nombres complexes *existants*, de même que, dans l'Algèbre, le mot *imaginaire* est employé dans ce double sens.

La condition qu'un nombre complexe contienne un facteur premier idéal multiple s'exprime encore par des congruences linéaires par rapport aux coefficients de ce nombre complexe. En mettant $f(\alpha)$ sous la forme

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

et supposant que $f(\alpha)$ contient n fois le facteur premier idéal de q, appartenant à la substitution $\eta = u_r$, on aura

$$[\Psi(\eta_{e-r})]^n[\varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta)] \equiv 0$$

pour le module q^n. On en conclut aisément que les f congruences contenues dans la formule

$$[\Psi(\eta_{e-r})]^n \varphi_k(\eta) \equiv 0 \pmod{q^n},$$

doivent avoir lieu séparément pour

$$k = 0,\ 1,\ 2,\ldots,\ f-1.$$

En réduisant à la forme linéaire, on aura

$$[\Psi(\eta_{e-r})]^n \varphi_k(\eta) = C\eta + C_1\eta_1 + C_2\eta_2 + \ldots + C_{e-1}\eta_{e-1},$$

ce qui donne

$$(\Psi\eta_{e-r})^n\varphi_k(\eta) + (\Psi\eta_{e-r})^n\varphi_k(\eta_1) + \ldots + (\Psi\eta_{e-r-1})^n\varphi_k(\eta_{e-1}) = -(C + C_1 + C_2 + \ldots + C_{e-1}).$$

Multipliant encore par $[\Psi(\eta_{e-r})]^n$, et observant que le produit $\Psi(\eta_r)\Psi(\eta_s)$ est toujours divisible par q, excepté le seul cas de $r=s$, on aura la congruence

$$(\Psi\eta_{e-r})^{2n}\varphi_k(\eta) \equiv -(C+C_1+C_2+\ldots+C_{e-1})(\Psi\eta_{e-r})^n \pmod{q^n}.$$

Il suit de là que la condition

$$(\Psi\eta_{e-r})^n\varphi_k(\eta) \equiv 0 \pmod{q^n}$$

est équivalente à la congruence

$$C+C_1+C_2+\ldots+C_{e-1} \equiv 0 \pmod{q^n},$$

qui est linéaire par rapport aux coefficients de $f(\alpha)$. Ainsi, la condition qu'un nombre complexe contienne n fois un facteur premier de q est exprimée par f congruences linéaires par rapport aux coefficients du nombre $f(\alpha)$ pour le module q^n.

Nous allons maintenant démontrer les théorèmes élémentaires pour le calcul des facteurs idéaux, qui seront entièrement les mêmes que pour les facteurs existants. Pour cela, nous proposons d'abord ce théorème :

Le produit de deux ou de plusieurs nombres complexes a précisément les mêmes facteurs premiers idéaux ou existants que les facteurs pris ensemble.

Soient $f(\alpha)$ et $g(\alpha)$ deux nombres complexes et $h(\alpha)$ leur produit, en sorte qu'on ait

$$f(\alpha).g(\alpha)=h(\alpha);$$

si le facteur premier idéal de q, qui appartient à la substitution $\eta=\eta_r$, est contenu précisément n fois dans $f(\alpha)$ et ν fois dans $g(\alpha)$, je dis qu'il sera contenu $n+\nu$ fois précisément dans $h(\alpha)$. D'après l'hypothèse, on a

$$f(\alpha)[\Psi(\eta_{e-r})]^n = q^n F(\alpha)$$

et

$$g(\alpha)[\Psi(\eta_{e-r})]^\nu = q^\nu G(\alpha),$$

où $F(\alpha)$ et $G(\alpha)$ ne sont pas congrus à zéro pour $\eta=\eta_r$, puisqu'on

aurait alors

$$f(\alpha)[\Psi(\eta_{e-r})]^{n+1} \equiv 0 \pmod{q^{n+1}}$$

et

$$g(\alpha)[\Psi(\eta_{e-r})]^{\nu+1} \equiv 0 \pmod{q^{\nu+1}}.$$

De ces deux équations il suit

$$f(\alpha).g(\alpha)[\Psi(\eta_{e-r})]^{n+\nu} = h(\alpha)[\Psi(\eta_{e-r})]^{n+\nu} = q^{n+\nu}\,\mathrm{F}(\alpha).\mathrm{G}(\alpha).$$

En mulipliant de nouveau par $\Psi(\eta_{e-r})$, on a aussi

$$h(\alpha)[\Psi(\eta_{e-r})]^{n+\nu+1} = q^{n+\nu}\,\mathrm{F}(\alpha).\mathrm{G}(\alpha).\Psi(\eta_{e-r}),$$

et puisqu'aucun des trois facteurs du produit $\mathrm{F}(\alpha).\mathrm{G}(\alpha).\Psi(\eta_{e-r})$ n'est congru à zéro pour $\eta = u_r$, ce produit n'est pas divisible par q. On a donc

$$h(\alpha)[\Psi(\eta_{e-r})]^{n+\nu} \equiv 0 \pmod{q^{n+\nu}},$$

sans avoir

$$h(\alpha)[\Psi(\eta_{e-r})]^{n+\nu+1} \equiv 0 \pmod{q^{n+\nu+1}},$$

c'est-à-dire le produit $h(\alpha)$ contient le facteur premier idéal de q, qui appartient à la substitution $\eta = u_r$, $n+\nu$ fois précisément. Ce résultat donne sans peine la démonstration du théorème proposé, car tout ce que nous avons démontré pour le facteur premier idéal de q, qui appartient à la substitution $\eta = u_r$, subsiste de même pour tous les facteurs premiers idéaux, et puisqu'on peut regarder les deux facteurs eux-mêmes comme composés de facteurs, et ainsi de suite, on voit qu'il subsiste également pour un produit d'un nombre quelconque de facteurs.

En faisant usage de la dénomination nouvelle de facteurs premiers idéaux, le théorème du paragraphe précédent, relatif à la condition qu'un nombre complexe $f(\alpha)$ soit divisible par q, pourra être énoncé comme il suit :

Pour qu'un nombre complexe quelconque, représenté comme produit

de plusieurs facteurs, soit divisible par q, il faut et il suffit qu'il contienne tous les e facteurs premiers idéaux du nombre q [*].

En supposant que dans le nombre $f(\alpha)$ chacun des facteurs premiers idéaux de q soit contenu n fois au moins, on aura les congruences

$$\left.\begin{array}{l} f(\alpha)[\Psi(\eta)]^n \equiv 0, \\ f(\alpha)[\Psi(\eta_1)]^n \equiv 0, \ldots, \\ f(\alpha)[\Psi(\eta_{e-r})]^n \equiv 0, \end{array}\right\} \pmod{q^n},$$

et, en ajoutant ces congruences,

$$f(\alpha)[\Psi(\eta)]^n + [\Psi(\eta_1)]^n + \ldots + [\Psi(\eta_{e-1})]^n \equiv 0 \pmod{q^n}.$$

Le second facteur de ce produit, comme fonction symétrique de toutes les périodes, sera un nombre entier non complexe; de plus, il n'est pas divisible par q, puisqu'aucun des facteurs idéaux de q n'y est contenu; il faut donc que le premier facteur soit divisible par q^n, ce qui donne cette généralisation du théorème précédent :

Un nombre complexe, contenant tous les facteurs premiers idéaux de q, chacun n fois au moins, est divisible par q^n.

Supposons maintenant que $f(\alpha)$ contienne n facteurs premiers idéaux de q, soit tous différents ou non, alors chacun des nombres

---

[*] Remarquons ici qu'au moyen de ce théorème on pourra reconnaître le motif de l'emploi des multiplicateurs désignés par $\Psi(\eta)$, qui consistent des $e-1$ facteurs

$$\psi(\eta_1)\cdot\psi(\eta_2)\ldots\psi(\eta_{e-1}).$$

En effet, la condition

$$\psi(u) \equiv 0 \pmod{q}$$

fait voir que $\psi(\eta)$ contient le facteur premier idéal de q, qui appartient à la substitution $\eta = u$, et la condition que $N\psi(\eta)$ ne soit pas divisible par q^2 exclut tous les autres facteurs premiers idéaux du nombre premier q qui pourraient troubler le résultat. Il s'ensuit que $\Psi(\eta_{e-r})$ contient tous les facteurs idéaux de q, à l'exception d'un seul, qui appartient à la substitution $\eta = u_r$. En multipliant donc par $\Psi(\eta_{e-r})$ un nombre donné $f(\alpha)$, contenant le facteur idéal de q, qui appartient à la substitution $\eta = u_r$, on aura un produit divisible par q, parce qu'il contient tous les facteurs idéaux de q; mais si le nombre $f(\alpha)$ ne contient pas ce facteur idéal, le produit ne sera jamais divisible par q, puisqu'un des facteurs idéaux du nombre q n'y est pas contenu.

conjugués

$$f(\alpha),\quad f(\alpha^{\gamma}),\quad f(\alpha^{\gamma^2}),\ldots,\quad f(\alpha^{\gamma^{\lambda-2}})$$

contiendra de même n facteurs idéaux de q, et le produit de ces $\lambda-1$ nombres conjugués, c'est-à-dire la norme $\mathrm{N}f(\alpha)$, en contiendra $(\lambda-1)n$. De plus, il est aisé de voir que tous ces facteurs idéaux dans la norme $\mathrm{N}f(\alpha)$ se trouveront en nombre égal; donc chacun d'entre eux s'y trouvera $\frac{n(\lambda-1)}{e}$ fois, ce qui est nf fois précisément. Donc, au moyen de la proposition précédente, on a le théorème très-important :

Si le nombre complexe $f(\alpha)$ contient n facteurs premiers idéaux du nombre q (appartenant à l'exposant f), soit que tous ces facteurs soient différents ou non, la norme $\mathrm{N}f(\alpha)$ contiendra toujours le facteur q^{nf}, mais elle ne contiendra jamais une puissance plus élevée de q.

Le nombre premier λ, le seul qui n'est pas contenu dans les nombres désignés par q, se décompose en $\lambda-1$ facteurs premiers conjugués de la manière suivante :

$$(1-\alpha)(1-\alpha^2)(1-\alpha^3)\ldots(1-\alpha^{\lambda-1}) = \mathrm{N}(1-\alpha) = \lambda.$$

Pour s'assurer que $1-\alpha^k$ est un nombre premier, on fera

$$1-\alpha^k = f(\alpha).\varphi(\alpha);$$

d'où, en prenant les normes, on aura

$$\lambda = \mathrm{N}f(\alpha).\mathrm{N}\varphi(\alpha).$$

On en conclut que l'un des deux facteurs $\mathrm{N}f(\alpha)$ et $\mathrm{N}\varphi(\alpha)$ sera nécessairement égal à λ, l'autre égal à l'unité; donc, $1-\alpha^k$ ne pouvant être décomposé en deux facteurs, sans que l'un d'eux soit une unité complexe, satisfait à la condition d'un nombre premier complexe. Les facteurs premiers de λ sont distingués des facteurs premiers complexes de tous les autres nombres premiers, parce qu'étant dégagés des unités complexes, ils sont tous égaux entre eux. En effet, on a

$$1-\alpha^k = (1-\alpha).(1+\alpha+\alpha^2+\ldots+\alpha^{k-1}),$$

et $1 + \alpha + \alpha^2 + \ldots + \alpha^{k-1}$ n'est qu'une unité complexe. Pour cette raison, il ne s'agira jamais de rechercher *quels* facteurs de λ, mais seulement *combien* de ces facteurs sont contenus dans un nombre complexe donné, et, pour cela, on n'aura qu'à chercher combien de fois la norme du nombre donné contient le facteur λ; car le nombre des facteurs premiers $1 - \alpha$, contenus dans un nombre complexe, est évidemment le même que le nombre des facteurs λ contenus dans sa norme.

Du théorème précédent, et de ce que nous avons remarqué des facteurs premiers du nombre λ, on conclut :

La norme d'un nombre complexe $f(\alpha)$ est toujours de la forme

$$\mathrm{N}f(\alpha) = \lambda^n q^{mf} . q'^{m'f'} . q''^{m''f''} \ldots,$$

où q, q', q'', etc., sont des nombres premiers appartenant respectivement aux exposants f, f', f'', etc., et n, m, m', m'', etc., sont des entiers positifs ou zéro.

En observant que la norme $\mathrm{N}f(\alpha)$ ne contient qu'un nombre fini de facteurs premiers λ, q, q', q''..., on voit que le nombre $f(\alpha)$ lui-même ne peut contenir qu'un nombre fini de facteurs premiers idéaux, qui seront aussi parfaitement déterminés par les définitions établies ci-dessus. Il en résulte ce théorème important :

Tout nombre complexe donné ne contient qu'un nombre fini de facteurs premiers idéaux parfaitement déterminés.

C'est surtout ce théorème qui justifie la notion des facteurs premiers idéaux, en montrant l'identité des règles du calcul des facteurs idéaux et des facteurs premiers de l'Arithmétique élémentaire, où le théorème analogue : Que tout nombre composé ne peut être décomposé en facteurs premiers que d'une seule manière, joue le même rôle principal.

Le théorème réciproque pourra s'énoncer comme il suit :

Deux nombres complexes, contenant les mêmes facteurs premiers idéaux, ne diffèrent que par des unités complexes, par lesquelles ils peuvent être multipliés.

En effet, supposons que $f(\alpha)$ et $\varphi(\alpha)$ aient les mêmes facteurs pre-

miers idéaux, et soit

$$\mathrm{N}f(\alpha) = \mathrm{N}\varphi(\alpha) = \lambda^n . q^{mf} . q'^{m'f'} \ldots ;$$

alors le produit

$$f(\alpha) . \varphi\left(\alpha^{\gamma}\right) . \varphi\left(\alpha^{\gamma^2}\right) \ldots \varphi\left(\alpha^{\gamma^{\lambda-2}}\right)$$

contiendra nécessairement tous les facteurs premiers idéaux de $\mathrm{N}\varphi(\alpha)$: il contiendra $n(\lambda - 1)$ fois le facteur premier $1 - \alpha$, et, par conséquent, il sera divisible par λ^n; il contiendra aussi tous les facteurs premiers idéaux de q chacun mf fois, tous les facteurs premiers idéaux de q', chacun $m'f'$ fois, et ainsi de suite. Mais puisqu'un nombre complexe, contenant tous les facteurs premiers de q, n fois chacun, est divisible par q^n, il s'ensuit que le produit

$$f(\alpha) . \varphi\left(\alpha^{\gamma}\right) . \varphi\left(\alpha^{\gamma^2}\right) \ldots \varphi\left(\alpha^{\gamma^{\lambda-2}}\right)$$

est divisible par q^{mf}, $q'^{m'f'}$, etc., il sera donc divisible par $\mathrm{N}\varphi(\alpha)$. De là nous avons

$$\frac{f(\alpha) . \varphi\left(\alpha^{\gamma}\right) . \varphi\left(\alpha^{\gamma^2}\right) \ldots \varphi\left(\alpha^{\gamma^{\lambda-2}}\right)}{\mathrm{N}\varphi(\alpha)} = \frac{f(\alpha)}{\varphi(\alpha)} = \mathrm{E}(\alpha),$$

$\mathrm{E}(\alpha)$ étant un entier complexe, et il s'ensuit

$$f(\alpha) = \varphi(\alpha)\,\mathrm{E}(\alpha) \quad \text{et} \quad \mathrm{N}f(\alpha) = \mathrm{N}\varphi(\alpha)\,\mathrm{N}\mathrm{E}(\alpha);$$

d'où

$$\mathrm{N}\mathrm{E}(\alpha) = 1. \qquad C.\ Q.\ F.\ D.$$

Pour qu'un nombre complexe $f(\alpha)$ soit divisible par $\varphi(\alpha)$, il faut et il suffit que tous les facteurs premiers idéaux du diviseur $\varphi(\alpha)$ soient contenus dans le dividende $f(\alpha)$.

D'abord il est clair que $f(\alpha)$ ne sera jamais divisible par $\varphi(\alpha)$, à moins qu'il ne contienne tous les facteurs premiers idéaux de $\varphi(\alpha)$; car, si l'on a

$$\frac{f(\alpha)}{\varphi(\alpha)} = \mathrm{Q}(\alpha),$$

$\mathrm{Q}(\alpha)$ étant un entier, il s'ensuit

$$f(\alpha) = \mathrm{Q}(\alpha) . \varphi(\alpha),$$

et, puisque le produit développé $f(\alpha)$ a tous les facteurs premiers idéaux des facteurs $Q(\alpha)$ et $\varphi(\alpha)$, pris ensemble, il faut que $f(\alpha)$ contienne tous les facteurs idéaux de $\varphi(\alpha)$. Pour démontrer que cette condition est suffisante, nous observons que, par la même raison que dans la démonstration du théorème précédent, on aura

$$f(\alpha)\varphi\left(\alpha^{\gamma}\right).\varphi\left(\alpha^{\gamma^2}\right)\ldots\varphi\left(\alpha^{\gamma^{\lambda-2}}\right)$$

divisible par $N\varphi(\alpha)$; d'où

$$\frac{f(\alpha).\varphi\left(\alpha^{\gamma}\right).\varphi\left(\alpha^{\gamma^2}\right)\ldots\varphi\left(\alpha^{\gamma^{\lambda-2}}\right)}{N\varphi(\alpha)}=\frac{f(\alpha)}{\varphi(\alpha)}=Q(\alpha),$$

$Q(\alpha)$ étant un entier.

Pour les applications que nous ferons dans la suite, nous ajoutons encore ce théorème, qui découle immédiatement du théorème principal :

Lorsqu'une puissance d'un nombre complexe est décomposée en plusieurs facteurs premiers entre eux, ces facteurs seront séparément des puissances semblables, multipliées par des unités complexes.

§ VI.

De la composition des nombres complexes idéaux.

Puisque les nombres complexes idéaux, comme facteurs des nombres complexes, jouent le même rôle que les facteurs existants, nous les désignerons désormais de la même manière que ceux-ci, par $f(\alpha)$, $\varphi(\alpha)$, etc., en sorte que $f(\alpha)$ par exemple, sera un nombre complexe, satisfaisant à un certain nombre déterminé de conditions caractéristiques pour les facteurs premiers idéaux, abstraction faite de l'existence du nombre $f(\alpha)$.

Cela posé, la norme d'un nombre complexe idéal sera toujours un nombre complexe existant; car, en supposant que $f(\alpha)$ contient m facteurs idéaux du nombre q, appartenant à l'exposant f, différents ou non, de même m' facteurs idéaux du nombre q', appartenant à l'exposant f', etc., la norme $Nf(\alpha)$ contenant tous les facteurs idéaux

de q, mf fois chacun, sera divisible par q^{mf}, de même elle sera divisible par $q'^{m'f'}$, etc., et, puisque la norme ne contient pas d'autres facteurs idéaux, elle sera égale à $q^{mf}.q'^{m'f'}\ldots$, à une unité près.

Le problème de trouver un nombre complexe existant $\mathrm{F}(\alpha)$, qui eût le facteur idéal $f(\alpha)$, aura toujours une infinité de solutions différentes, c'est-à-dire il y a toujours une infinité de nombres idéaux qui, multipliés par le nombre idéal déterminé $f(\alpha)$, produisent des nombres complexes existants. En choisissant ces multiplicateurs idéaux de manière que la norme du produit soit aussi petite que possible, on parviendra au résultat remarquable, qu'un nombre fini et déterminé de multiplicateurs idéaux suffit à rendre existante l'infinité de tous les nombres idéaux.

Soient, comme ci-dessus, q un nombre premier appartenant à l'exposant f, q' un nombre premier appartenant à l'exposant f', etc., soit $f(\alpha)$ un nombre complexe idéal qui contienne m fois le facteur premier idéal de q, appartenant à la substitution $s = u_r$, de plus m' fois le facteur premier idéal de q', appartenant à la substitution $s' = u'^{r}$, etc., soit enfin

$$\mathrm{F}(\alpha) = x_1\alpha + x_2\alpha^2 + x_3\alpha^3 + \ldots + x_{\lambda-1}\alpha^{\lambda-1}$$

un nombre complexe existant, qui contienne tous les facteurs premiers idéaux de $f(\alpha)$, c'est-à-dire le nombre idéal $f(\alpha)$ lui-même. La condition que $\mathrm{F}(\alpha)$ contienne m fois le facteur premier de q, appartenant à la substitution $s = u_r$, est exprimée par une congruence de la forme

$$[\Psi(\gamma_{e-r})]^m \mathrm{F}(\alpha) \equiv 0 \pmod{q^m},$$

équivalente à f congruences linéaires par rapport aux coefficients de $\mathrm{F}(\alpha)$, pour le même module q^m. Soient donc

$$\Phi \equiv 0, \quad \Phi_1 \equiv 0, \ldots, \quad \Phi_{f-1} \equiv 0 \pmod{q^m},$$

ces f congruences linéaires. Soient de même

$$\Phi' \equiv 0, \quad \Phi'_1 \equiv 0, \ldots, \quad \Phi'_{f'-1} \equiv 0 \pmod{q'^{m'}},$$

les f' congruences nécessaires et suffisantes, pour que $\mathrm{F}(\alpha)$ contienne

m' fois le facteur premier de q', appartenant à la substitution $u' = u'_{r'}$, et ainsi de suite. Cela posé, si l'on donne aux $\lambda - 1$ coefficients $x_1, x_2, x_3, \ldots, x_{\lambda-1}$, toutes les valeurs $0, 1, 2, \ldots, k-1$, en sorte qu'on ait $k_{\lambda-1}$ combinaisons diverses de valeurs de ces coefficients, on voit que chacune des f quantités $\Phi, \Phi_1, \ldots, \Phi_{f-1}$ ne pourra donner que q^m restes différents par rapport au module q^m; de même chacune des f' quantités $\Phi', \Phi'_1, \ldots, \Phi'_{f'-1}$, ne donnera que $q'^{m'}$ restes différents, pour le module $q'^{m'}$, etc. Le nombre de toutes les combinaisons différentes des restes des $f + f' + \ldots$ quantités désignées par Φ, sera donc égal à $q^{mf} \cdot q'^{m'f'} \ldots$. Maintenant si l'on prend le nombre k assez grand pour que le nombre des combinaisons de tous les restes possibles soit inférieur au nombre des combinaisons des valeurs des coefficients, c'est-à-dire $q^{mf} \cdot q'^{m'f'} \ldots < k^{\lambda-1}$, on voit que toutes les combinaisons différentes des valeurs des coefficients ne pourront pas appartenir à des combinaisons différentes des restes, mais que ces combinaisons des restes se reproduiront nécessairement. Soit donc

$$x_1 = a_1, \quad x_2 = a_2, \quad x_3 = a_3, \ldots, \quad x_{\lambda-1} = a_{\lambda-1},$$

une combinaison de valeurs des coefficients, pour lesquelles toutes les quantités désignées par Φ donnent les mêmes restes que pour la combinaison

$$x_1 = b_1, \quad x_2 = b_2, \quad x_3 = b_3, \ldots, \quad x_{\lambda-1} = b_{\lambda-1};$$

par la soustraction des résultats de ces deux substitutions, les restes égaux se détruisent, et puisque les quantités désignées par Φ sont linéaires par rapport aux coefficients $x_1, x_2, x_3, \ldots, x_{\lambda-1}$, on voit que la combinaison des valeurs

$$x_1 = a_1 - b_1, \; x_2 = a_2 - b_2, \; x_3 = a_3 - b_3, \ldots \; x_{\lambda-1} = a_{\lambda-1} - b_{\lambda-1}$$

satisfera à toutes les congruences nécessaires pour que $F(\alpha)$ contienne le facteur idéal $f(\alpha)$. Ainsi, parmi les nombres complexes dont les coefficients entiers positifs ou négatifs ne surpassent pas la valeur $k-1$, où k satisfait à la condition $k^{\lambda-1} > Nf(\alpha)$, il y en aura toujours qui contiennent le facteur idéal $f(\alpha)$.

En développant le produit des deux nombres réciproques $F(\alpha)$ et $F(\alpha^{-1})$, puis changeant α en α^2, α^3,..., $\alpha^{\frac{\lambda-1}{2}}$, et ajoutant, on obtient

$$F(\alpha).F(\alpha^{-1}) + F(\alpha^2).F(\alpha^{-2}) + \ldots + F\left(\alpha^{\frac{\lambda-1}{2}}\right).F\left(\alpha^{-\frac{\lambda-1}{2}}\right)$$
$$= \tfrac{1}{2}\lambda(x_1^2 + x_2^2 + x_3^2 + \ldots + x_{\lambda-1}^2) - \tfrac{1}{2}(x_1 + x_2 + x_3 + \ldots + x_{\lambda-1})^2;$$

et puisque les coefficients x_1, x_2, x_3,..., $x_{\lambda-1}$, abstraction faite des signes, ne sont pas supérieurs à $k-1$, on en déduit facilement l'inégalité

$$F(\alpha).F(\alpha^{-1}) + F(\alpha^2).F(\alpha^{-2}) + \ldots$$
$$+ F\left(\alpha^{\frac{\lambda-1}{2}}\right).F\left(\alpha^{-\frac{\lambda-1}{2}}\right) \leqq \tfrac{1}{2}\lambda(\lambda-1).(k-1)^2,$$

et en faisant usage de la proposition connue, que le produit de n quantités positives est plus petit que la $n^{ième}$ puissance de la moyenne arithmétique de ces quantités, on en conclut sans difficulté

$$NF(\alpha) \leqq \lambda^{\frac{\lambda-1}{2}}(k-1)^{\lambda-1}.$$

Le nombre k, qui doit satisfaire à la condition $k^{\lambda-1} > Nf(\alpha)$ pourra toujours être pris de manière à rendre $(k-1)^{\lambda-1} < Nf(\alpha)$; par cette supposition on a

$$NF(\alpha) < \lambda^{\frac{\lambda-1}{2}} Nf(\alpha).$$

En représentant actuellement le nombre complexe $F(\alpha)$ comme produit des deux facteurs idéaux $\varphi(\alpha)$ et $f(\alpha)$, on aura

$$F(\alpha) = \varphi(\alpha).f(\alpha),$$

d'où

$$NF(\alpha) = N\varphi(\alpha).Nf(\alpha),$$

et, au moyen de l'inégalité trouvée, il vient

$$N\varphi(\alpha) < \lambda^{\frac{\lambda-1}{2}}.$$

Ainsi, les multiplicateurs idéaux, qui, composés avec tous les nombres complexes idéaux, donnent des nombres complexes existants, peuvent toujours être choisis tels, que leurs normes soient plus petites que $\lambda^{\frac{\lambda-1}{2}}$; et puisque le nombre des facteurs idéaux dont les normes ne surpassent pas cette limite fixe est limité, nous avons ce théorème :

Il y a toujours un nombre fini de multiplicateurs idéaux, qui, composés avec les nombres idéaux, en nombre infini, les rendent tous nombres complexes existants.

Les multiplicateurs qui rendent existants les nombres complexes idéaux, avec lesquels ils sont composés, donnent lieu à la classification des nombres complexes idéaux, que nous établissons par cette définition :

Tous les nombres complexes idéaux qui donnent des produits existants lorsqu'on les multiplie par un même nombre idéal, seront appelés NOMBRES IDÉAUX ÉQUIVALENTS, *et ils seront attribués à une même* CLASSE *des nombres complexes idéaux.*

Nous comprenons dans cette classification les nombres existants eux-mêmes, qui constituent une de ces classes que nous appellerons *la classe principale.*

D'abord nous observons qu'un nombre idéal, multiplié par un nombre existant, ne donnera jamais un produit existant, puisqu'alors le quotient de deux nombres existants serait un nombre idéal.

Soient à présent $f(\alpha)$ et $\varphi(\alpha)$ deux nombres idéaux équivalents, $\psi(\alpha)$ le multiplicateur qui les rend existants, soit aussi $\chi(\alpha)$ un multiplicateur de $f(\alpha)$, tel que $\chi(\alpha).f(\alpha)$ soit un nombre existant; je dis que $\chi(\alpha).\varphi(\alpha)$ sera de même un nombre existant. En effet, puisque $\psi(\alpha).f(\alpha)$ est un nombre existant, il en sera de même du produit

$$\psi(\alpha^2).\psi(\alpha^3)\ldots\psi(\alpha^{\lambda-1}).f(\alpha^2).f(\alpha^3)\ldots f(\alpha^{\lambda-1}).$$

Multipliant donc par les deux nombres existants $\psi(\alpha).\varphi(\alpha)$ et $\chi(\alpha).f(\alpha)$, on aura le nombre existant

$$\varphi(\alpha).\chi(\alpha).\mathrm{N}\psi(\alpha).\mathrm{N}f(\alpha),$$

et, en supprimant le facteur existant $N\psi(\alpha) . Nf(\alpha)$, on voit que $\varphi(\alpha) . \chi(\alpha)$ est un nombre existant. Nous en concluons :

Les classes des nombres équivalents sont toujours les mêmes, pour tous les multiplicateurs qu'on pourra choisir.

Soit présentement $f(\alpha)$ équivalent à $\psi(\alpha)$, et de même $\varphi(\alpha)$ équivalent à $\psi(\alpha)$, je dis que $f(\alpha)$ sera équivalent à $\varphi(\alpha)$. En effet, tout multiplicateur de $\psi(\alpha)$, qui donne un produit existant, sera de même multiplicateur de $f(\alpha)$ et de $\varphi(\alpha)$. Donc :

Deux nombres idéaux, équivalents à un même troisième nombre idéal, sont équivalents entre eux.

En rapprochant ces résultats du premier théorème de ce paragraphe, on conclut :

Les classes diverses dans lesquelles tous les nombres idéaux se distribuent, sont en nombre fini et complétement déterminées, en sorte qu'un certain nombre idéal n'appartient qu'à une seule classe.

Soient $f(\alpha)$ et $f_1(\alpha)$ deux nombres idéaux équivalents, $\psi(\alpha)$ le multiplicateur qui les rend existants; soient de même $\varphi(\alpha)$ et $\varphi_1(\alpha)$ deux nombres équivalents, et $\chi(\alpha)$ leur multiplicateur; $\psi(\alpha) . \chi(\alpha)$ sera évidemment un multiplicateur qui rend existant le produit $f(\alpha) . \varphi(\alpha)$, de même que le produit $f_1(\alpha) . \varphi_1(\alpha)$. Ces produits seront donc équivalents. De là ce théorème :

Des nombres équivalents, multipliés par des nombres équivalents, donnent toujours des produits équivalents.

Il suit de là que, lorsqu'on multiplie les nombres idéaux d'une certaine classe avec les nombres idéaux d'une autre classe, tous ces produits appartiendront à une même classe déterminée. Ainsi :

La classe du produit de deux nombres idéaux est complétement déterminée par les classes des facteurs.

Lorsqu'on multiplie un nombre idéal donné par un des nombres de chaque classe, on aura autant de produits qu'on a de classes, et l'on s'assure aisément que tous ces produits appartiennent à des classes

différentes. Parmi ces produits, il y en aura nécessairement un, et il n'y en aura qu'un, qui appartient à la classe principale. Donc :

Il correspond à chaque classe une certaine classe, en sorte que ces deux classes composées produisent la classe principale, c'est-à-dire que le produit de deux nombres quelconques de ces deux classes est un nombre complexe existant.

Les classes qui produisent la classe principale, lorsqu'elles sont composées avec elles-mêmes, seront appelées *classes ambiguës*. La classe principale est toujours une classe ambiguë; d'autres classes ambiguës n'existent que pour des valeurs particulières du nombre λ.

Considérons maintenant les diverses puissances entières d'un nombre idéal $f(\alpha)$. Dans la série

$$f(\alpha),\quad f(\alpha)^2,\quad f(\alpha)^3,\quad f(\alpha)^4,\ldots,$$

il y aura nécessairement des nombres idéaux équivalents, car le nombre de ceux qui appartiennent à des classes diverses est fini, aussi bien que le nombre des classes mêmes.

Soient donc $f(\alpha)^r$ et $f(\alpha)^s$ deux nombres idéaux équivalents de cette série où $s > r$; soit aussi $\Psi(\alpha)$ un multiplicateur qui rend $f(\alpha)^r\Psi(\alpha)$ et $f(\alpha)^s\Psi(\alpha)$ nombres existants; le quotient de ces deux nombres, ou bien $f(\alpha)^{s-r}$, sera de même un nombre existant. Nous avons donc ce théorème important :

Tout nombre complexe idéal, élevé à une certaine puissance entière, donne un nombre complexe existant.

Ou bien :

Tout nombre complexe idéal peut être représenté comme une certaine racine d'un nombre complexe existant.

Si l'exposant h est le plus petit pour lequel $f(\alpha)^h$ est un nombre existant, les nombres de la série de h termes

$$1, f(\alpha),\quad f(\alpha)^2,\quad f(\alpha)^3,\ldots,\quad f(\alpha)^{h-1}$$

appartiendront à des classes diverses; car, si l'on avait $f(\alpha)^r$ équivalent à $f(\alpha)^s$, r et s étant positifs et moindres que h, on en conclurait, comme ci-dessus, que $f(\alpha)^{s-r}$ serait existant. Il y aurait donc un exposant

$s - r$, moindre que h, pour lequel la puissance du nombre idéal $f(\alpha)$ serait un nombre existant, ce qui est contre l'hypothèse. Il se peut maintenant que les h classes, représentées par les nombres idéaux de la série proposée de h termes, embrassent toutes les classes des nombres idéaux; alors le nombre de toutes les classes diverses sera égal à h. Si cela n'a pas lieu, on choisira arbitrairement un nombre idéal $\varphi(\alpha)$, non équivalent aux h nombres idéaux proposés, et l'on en formera ce second groupe de h nombres idéaux

$$\varphi(\alpha),\ \varphi(\alpha).f(\alpha),\ \varphi(\alpha).f(\alpha)^2,\ldots,\ \varphi(\alpha).f(\alpha)^{h-1}.$$

Les h termes de ce groupe ne sont pas équivalents, ni entre eux, ni aux termes du premier groupe. En effet, si l'on avait $\varphi(\alpha).f(\alpha)^r$ équivalent à $\varphi(\alpha).f(\alpha)^s$, r et s étant moindres que h, il s'ensuivrait $f(\alpha)^r$ équivalent à $f(\alpha)^s$, contre l'hypothèse, et, si l'on avait $\varphi(\alpha).f(\alpha)^r$ équivalent à $f(\alpha)^s$, en multipliant par $f(\alpha)^{h-r}$, on aurait aussi $\varphi(\alpha).f(\alpha)^h$ équivalent à $f(\alpha)^{h-r+s}$, ou bien $\varphi(\alpha)$ équivalent à $f(\alpha)^{s-r}$, ce qui est aussi contre l'hypothèse. Maintenant, il se pourra que les $2h$ classes de nombres idéaux, représentées par le premier et le second groupe, embrassent toutes les classes des nombres idéaux. Dans ce cas, le nombre des classes sera égal à $2h$. Mais si cela n'a pas lieu, on prendra arbitrairement un nombre idéal $\psi(\alpha)$, qui ne soit pas équivalent à aucun nombre de ces deux groupes, et l'on en composera ce troisième groupe de h termes,

$$\psi(\alpha),\quad \psi(\alpha).f(\alpha),\quad \psi(\alpha).f(\alpha)^2,\ldots,\quad \psi(\alpha).f(\alpha)^{h-1}.$$

On démontre aisément que ces nombres idéaux ne sont pas équivalents ni entre eux ni aux termes du premier et du second groupe, et l'on en conclut, si ces trois groupes embrassent toutes les classes, que le nombre des classes sera égal à $3h$. Si cela n'a pas lieu, on pourra continuer de la même manière, et l'on voit clairement qu'on parviendra ainsi à ranger toutes les classes des nombres idéaux en groupes de h termes. De là ce théorème :

Le nombre total de toutes les classes des nombres idéaux est un multiple du plus petit exposant de la puissance d'un nombre idéal quelconque qui devient un nombre complexe existant.

Toutes les autres puissances du nombre idéal $f(\alpha)$, qui donnent des nombres complexes existants, seront nécessairement contenues dans la forme $f(\alpha)^{mh}$, d'où l'on conclut ce corollaire :

Si une puissance d'un nombre complexe idéal donne un nombre complexe existant, il faut que l'exposant de cette puissance ait un facteur commun avec le nombre des classes de tous les nombres complexes idéaux.

Il se présente ici la question délicate, si le nombre idéal $f(\alpha)$ pourra toujours être choisi tel, que les nombres idéaux d'un seul groupe

$$1, \quad f(\alpha), \quad f(\alpha)^2, \quad f(\alpha)^3, \ldots, \quad f(\alpha)^{h-1}$$

embrassent toutes les classes des nombres idéaux. Il nous paraît que cela n'a pas lieu dans tous les cas, mais qu'il y a effectivement des nombres premiers λ pour lesquels les puissances d'un seul nombre idéal ne pourront jamais représenter toutes les classes des nombres complexes idéaux. En laissant cela aux recherches plus approfondies des géomètres, nous remarquons que la question analogue pour la composition des formes quadratiques a été traitée par M. Gauss dans la cinquième section, n° 306, des *Disquisitiones Arithmeticæ*.

Remarque. Qu'il me soit permis de signaler ici en peu de mots l'analogie de cette théorie de la composition des nombres idéaux avec les principes fondamentaux de la chimie. La composition des nombres complexes peut être envisagée comme l'analogue de la combinaison chimique; les facteurs premiers correspondent aux éléments, ou plutôt aux équivalents de ces éléments. Les nombres complexes idéaux sont comparables aux radicaux hypothétiques qui n'existent pas par eux-mêmes, mais seulement dans les combinaisons; le fluor, en particulier, comme élément qu'on ne sait pas représenter isolément, peut être comparé à un facteur premier idéal. La notion de l'équivalence des nombres idéaux est, au fond, la même que celle de l'équivalence chimique; car, ainsi que des quantités pondérales équivalentes des matières naturelles peuvent être substituées les unes aux autres pour rendre des sels neutres ou des corps isomorphes, de même les nombres idéaux, remplacés par les facteurs équivalents, ne produisent que des nombres idéaux de la même classe. En comparant les méthodes de

l'analyse chimique à celles de la décomposition des nombres complexes, on trouve encore des analogies surprenantes. Car, de même que les réactifs chimiques, joints à un corps en dissolution, donnent des précipités au moyen desquels on reconnaît les éléments contenus dans le corps proposé, de même les nombres que nous avons désignés par $\Psi(\eta)$ comme réactifs des nombres complexes, font connaître les facteurs premiers contenus dans les nombres complexes en mettant en évidence un facteur premier q analogue au précipité chimique. Toutes ces analogies qu'on pourra poursuivre et augmenter à volonté, ne proviennent pas d'un jeu d'esprit oisif, mais elles sont bien fondées en ce que les mêmes idées fondamentales de la composition et décomposition des éléments règnent aussi bien dans la chimie des matières naturelles que dans celle des nombres complexes.

§ VII.

Application à la théorie de la division du cercle.

On sait que toutes les difficultés de la théorie de la division du cercle, c'est-à-dire de la solution algébrique de l'équation binôme $x^p = 1$, se réduisent à la recherche de certains nombres complexes du genre de ceux qui ont été discutés dans ce qui précède. Sous le point de vue théorique, on désire la connaissance approfondie de la constitution intérieure de ces nombres complexes, et pour la pratique, il reste encore à réduire le calcul de ces nombres à la solution d'un seul problème élémentaire et général. C'est ce que nous compléterons au moyen de notre théorie des nombres complexes.

Soient p un nombre premier de la forme $m\lambda + 1$, g une racine primitive de la congruence $g^{p-1} \equiv 1 \pmod{p}$, x une racine imaginaire de l'équation $x^p = 1$, et soient, comme ci-dessus, α une racine imaginaire de l'équation $\alpha^\lambda = 1$, λ un nombre premier. Cela posé, la partie la plus difficile du problème de la résolution algébrique de l'équation $x^p = 1$ tient à la recherche de la puissance $\lambda^{ième}$ de l'expression résolvante proposée par Lagrange,

$$x + \alpha x^g + \alpha^2 x^{g^2} + \alpha^3 x^{g^3} + \ldots + \alpha^{p-2} x^{g^{p-2}},$$

que nous désignons simplement par (α, x). Cette puissance, indépendante de x, n'est qu'un nombre complexe composé des racines α, α^2, α^3,..., $\alpha^{\lambda-1}$. En faisant usage de l'expression

$$\frac{(\alpha, x)\ (\alpha^k, x)}{(\alpha^{k+1}, x)} = \psi_k(\alpha),$$

qui est de même indépendante de x, et en observant que

$$(\alpha, x).(\alpha^{-1}, x) = p,$$

on aura

$$(\alpha, x)^\lambda = p\psi_1(\alpha).\psi_2(\alpha).\psi_2(\alpha)...\psi_{\lambda-2}(\alpha);$$

d'où l'on voit que tout se réduit à trouver les nombres complexes désignés par $\psi_k(\alpha)$, pour

$$k = 1, 2, 3,..., \lambda - 2.$$

Nous déterminerons ces nombres complexes en définissant les facteurs premiers idéaux qu'ils contiennent, ce qui se fera au moyen de quelques résultats trouvés en même temps par M. Cauchy et par M. Jacobi, et publiés dans les *Mémoires de l'Académie des Sciences de Paris,* de l'année 1840, et dans les *Comptes rendus mensuels de l'Académie de Berlin,* de l'année 1837. Ces deux grands géomètres ont trouvé qu'en désignant par r une racine primitive de l'équation $r^{p-1} = 1$, et faisant

$$x + rx^g + r^2x^{g^2} + ... + r^{p-2}x^{g^{p-2}} = (r, x),$$

$$\frac{(r^{-m}, x).(r^{-n}, x)}{(r^{-m-n}, x)} = \psi(r),$$

la substitution de la racine primitive g de la congruence

$$g^{p-1} \equiv 1 \pmod{p},$$

au lieu de la racine r de l'équation $r^{p-1} = 1$, donne

$$\psi(g) \equiv -\frac{\Pi(m+n)}{\Pi(m)\Pi(n)} \pmod{p},$$

$\Pi(n)$ désignant le produit $1.2.3...n$, d'où il suit

$$\psi(g) \equiv 0 \pmod{p}, \quad \text{si} \quad m < p-1, \quad n < p-1, \quad m+n > p-1.$$

Pour en faire l'application au nombre complexe $\psi_k(\alpha)$, nous ferons

$$m = \frac{h(p-1)}{\lambda}, \quad n = \frac{i(p-1)}{\lambda}, \quad r^{-\frac{p-1}{\lambda}} = z,$$

ce qui donne

$$\psi(r) = \frac{(\alpha^h, x).(\alpha^i, x)}{(\alpha^{h+i}, x)};$$

de là, en faisant $i \equiv hk \pmod{\lambda}$,

$$\psi(r) = \frac{(\alpha^h, x).(\alpha^{hk}, x)}{(\alpha^{h(k+1)}, x)} = \psi_k(\alpha^h).$$

Substituant enfin la racine primitive g au lieu de r, et faisant, pour abréger,

$$g^{\frac{p-1}{\lambda}} \equiv u \pmod{p},$$

nous aurons

$$\psi_k(u^{-h}) \equiv 0 \pmod{p} \quad \text{si} \quad h < \lambda, \quad i < \lambda, \quad h + i > \lambda.$$

En considérant les racines α, α^ν, α^{ν^2},..., $\alpha^{\nu^{\lambda-2}}$ comme périodes monômes, on aura les racines des congruences correspondantes u, u^ν, u^{ν^2},..., $u^{\nu^{\lambda-2}}$; donc le résultat trouvé pourra s'énoncer comme il suit :

Si la somme du nombre h, positif et moindre que λ, et du plus petit reste positif de $hk \pmod{\lambda}$, est plus grande que λ, le nombre complexe $\psi_k(\alpha)$ contient le facteur premier idéal de p, qui appartient à la substitution $\alpha = u^{-h}$.

Le nombre des valeurs de h, qui satisfont à cette condition, est égal à $\frac{\lambda-1}{2}$; car on voit, sans difficulté, que de deux valeurs de h, dont la somme est égale à λ, l'une satisfait toujours, mais qu'elles ne satisfont jamais toutes deux en même temps. Le théorème trouvé fait donc connaître $\frac{\lambda-1}{2}$ facteurs premiers idéaux contenus dans le nombre complexe $\psi_k(\alpha)$, et l'on s'assure facilement qu'il n'y a pas d'autres facteurs premiers dans $\psi_k(\alpha)$. En effet, par l'équation connue

$$\psi_k(\alpha) . \psi_k(\alpha^{-1}) = p,$$

on voit que $\psi_k(\alpha)$ et $\psi_k(\alpha^{-1})$, pris ensemble, contiennent tous les $\lambda - 1$

facteurs premiers de p, et, puisque $\psi_k(\alpha^{-1})$ contient nécessairement autant de facteurs premiers que $\psi_k(\alpha)$, ce nombre complexe contiendra exactement les $\frac{\lambda-1}{2}$ facteurs premiers définis dans le théorème.

En désignant par $f(\alpha)$ le facteur premier (idéal) de p, appartenant à la substitution $\alpha = u$, et par $\left|\frac{k}{h}\right|$ la racine positive, moindre que λ, de la congruence $hx \equiv k \pmod{\lambda}$, nous aurons

$$\psi_k(\alpha) = \mathrm{E}(\alpha)\,\Pi f(\alpha^{-h}),$$

où le signe du produit Π s'étend sur toutes les valeurs de h, moindres que λ, qui satisfont à la condition $\left|\frac{1}{h}\right| + \left|\frac{k}{h}\right| > \lambda$. L'unité complexe $\mathrm{E}(\alpha)$, qu'il faut toujours ajouter au produit de tous les facteurs premiers d'un nombre complexe donné, se réduit, dans ce cas, à l'unité simple $\pm \alpha^r$; car, moyennant la formule

$$\psi_k(\alpha)\,\psi_k(\alpha^{-1}) = p,$$

on a

$$\mathrm{E}(\alpha)\,\mathrm{E}(\alpha^{-1}) = 1,$$

équation qui n'est jamais satisfaite que par les unités simples de la forme $\pm \alpha^r$. L'expression de $\psi_k(\alpha)$ devient donc

$$\psi_k(\alpha) = \pm \alpha^r\,\Pi f(\alpha^{-h}),$$

pour toutes les valeurs positives de $h < \lambda$, qui satisfont à la condition $\left|\frac{1}{h}\right| + \left|\frac{k}{h}\right| > \lambda$. Pour déterminer complétement le signe et l'exposant r de l'unité simple $\pm \alpha^r$, on fera usage de la propriété connue de ces nombres complexes que

$$\psi_k(\alpha) \equiv -1 \quad [\mathrm{mod.}\,(1-\alpha)^2].$$

Des facteurs premiers trouvés de $\psi_k(\alpha)$, on déduit ceux de la puissance

$$(\alpha, x)^{\lambda} = p\,\psi_1(\alpha)\cdot\psi_2(\alpha)\cdot\psi_3(\alpha)\ldots\psi_{\lambda-2}(\alpha).$$

Le facteur premier idéal déterminé $f(\alpha^{-h})$ se trouvera dans le produit

$\psi_1(\alpha)\cdot\psi_2(\alpha)\cdot\psi_3(\alpha)\ldots\psi_{\lambda-2}(\alpha)$ autant de fois précisément qu'il y a de nombres k, pour lesquels on a

$$\left|\frac{1}{h}\right|+\left|\frac{k}{h}\right|>\lambda,$$

et, puisque $\left|\frac{k}{h}\right|$, pour $k=1, 2, 3,\ldots, \lambda-2$, a évidemment toutes les valeurs $\left|\frac{k}{h}\right|=1, 2, 3,\ldots, \lambda-1$, excepté la seule $\left|\frac{\lambda-1}{h}\right|=\lambda-\left|\frac{1}{h}\right|$, le nombre des valeurs de k, qui donnent

$$\left|\frac{1}{h}\right|+\left|\frac{k}{k}\right|>\lambda, \quad \text{ou} \quad \left|\frac{k}{h}\right|>\lambda-\left|\frac{1}{h}\right|,$$

c'est-à-dire le nombre des facteurs $f(\alpha^{-h})$ contenus dans le produit $\psi_1(\alpha)\cdot\psi_2(\alpha)\ldots\psi_{\lambda-2}(\alpha)$, sera égal à $\left|\frac{1}{h}\right|-1$. En y ajoutant un facteur $f(\alpha^{-h})$, contenu dans p, on voit que le facteur premier $f(\alpha^{-h})$ est contenu $\left|\frac{1}{h}\right|$ fois précisément dans la puissance $(\alpha, x)^{\lambda}$. Ainsi, en prenant

$$h=1, 2, 3,\ldots, \lambda-1,$$

on a l'expression

$$(\alpha, x)^{\lambda}=\pm\alpha^{s}f(\alpha^{-1})^{\left|\frac{1}{1}\right|}\cdot f(\alpha^{-2})^{\left|\frac{1}{2}\right|}\cdot f(\alpha^{-3})^{\left|\frac{1}{3}\right|}\ldots f[\alpha^{-(\lambda-1)}]^{\left|\frac{1}{\lambda-1}\right|},$$

ou, ce qui est la même chose,

$$(\alpha, x)^{\lambda}=\pm\alpha^{s}f(\alpha)^{\left|\frac{1}{\lambda-1}\right|}\cdot f(\alpha^{2})^{\left|\frac{1}{\lambda-2}\right|}\cdot f(\alpha^{3})^{\left|\frac{1}{\lambda-3}\right|}\ldots f(\alpha^{\lambda-1})^{\left|\frac{1}{1}\right|}.$$

Ici l'unité simple $\pm\alpha^{s}$ sera, en chaque cas, déterminée complétement par la condition connue

$$(\alpha, x)^{\lambda}\equiv -1 \pmod{\lambda}.$$

La décomposition en facteurs premiers donne en même temps la connaissance parfaite des nombres complexes qui se présentent dans la théorie de la division du cercle, et le moyen le plus simple pour les calculer; car on voit que tout se réduit au seul problème de trouver

un facteur premier complexe du nombre p, qui pourra être représenté comme nombre complexe entier, s'il existe par soi-même, ou comme racine d'un certain degré d'un nombre complexe existant, s'il est idéal. La recherche de ces facteurs premiers se fait assez facilement au moyen de méthodes indirectes qui s'offrent d'elles-mêmes. Il ne serait pas trop pénible, et il serait très-utile, pour cette théorie, de construire une Table de tous les facteurs premiers existants et idéaux des nombres premiers du premier millier, laquelle donnerait tous les nombres nécessaires pour la résolution algébrique de l'équation $x^p = 1$, pour tous les nombres premiers p contenus dans les mêmes limites. Une partie de cette Table a été donnée dans la dissertation *de numeris complexis*, etc., publiée en 1834, et réimprimée dans ce Journal en 1837.

Pour faire mieux apprécier l'usage des formules données dans ce paragraphe, nous rappelons la méthode ingénieuse dont M. Gauss s'est servi pour trouver l'équation du troisième degré, dont les racines sont les trois périodes à $\frac{p-1}{3}$ termes (voir *Disq. Arithm.*, sect. VII, n° 358), qui revient à ce que le nombre $4p$ doit être mis sous la forme du second degré

$$4p = \mathrm{M}^2 + 27\,\mathrm{N}^2.$$

Notre méthode donne la même réduction pour le problème général, où il s'agit de λ périodes à $\frac{p-1}{\lambda}$ termes; car le problème de trouver un facteur premier complexe d'un nombre premier p est essentiellement le même que de représenter le nombre p comme une certaine forme du degré $\lambda - 1$ et du même nombre d'indéterminés; on voit aussi que les coefficients du nombre premier complexe, ou, ce qui revient au même, les valeurs des indéterminés de la forme du degré $\lambda - 1$, jouent le même rôle dans le problème général, que les deux nombres M et N de la forme

$$4p = \mathrm{M}^2 + 27\,\mathrm{N}^2,$$

pour le cas de $\lambda = 3$.

§ VIII.

Recherche du nombre des classes diverses des nombres complexes idéaux.

Les principes nouveaux dont M. Lejeune-Dirichlet s'est servi dans la recherche du nombre des formes quadratiques qui répondent à un déterminant donné, joints aux résultats exposés dans ce qui précède, suffiront pour achever la recherche analogue du nombre des classes des nombres complexes idéaux. Pour en faire l'application, nous considérons la série infinie

$$R = \sum \frac{s-1}{[NF(\alpha)]^s},$$

où le signe sommatoire $\sum$ doit être pris par rapport à tous les nombres complexes différents, existants ou idéaux, et où l'on compte pour différents deux nombres complexes qui ne sont pas composés des mêmes facteurs premiers idéaux. Pour que la série proposée soit convergente, le nombre s est supposé positif et plus grand que l'unité, mais on le fera décroître ci-après jusqu'à la limite 1.

La norme d'un nombre complexe, existant ou idéal, étant toujours de la forme

$$NF(\alpha) = \lambda^n . q^{mf} . q'^{m'f'} . q''^{m''f''} \ldots,$$

où q, q', q'',..., sont des nombres premiers qui appartiennent respectivement aux exposants f, f', f'',..., nous pourrons introduire cette expression dans la série R; mais puisque la même norme convient toujours à plusieurs nombres complexes différents, nous rechercherons d'abord combien de nombres complexes donneront la même norme, c'est-à-dire combien de fois le terme

$$\frac{s-1}{(\lambda^n . q^{mf} . q'^{m'f'} . q''^{m''f''} \ldots)^s}$$

se trouvera dans la série R. On conclut du facteur q^{mf} contenu dans la norme, que le nombre complexe $F(\alpha)$ contiendra nécessairement m facteurs premiers de q, différents ou non, et parce qu'il y a $\frac{\lambda-1}{f} = e$

facteurs premiers de q, on voit qu'en prenant toutes les combinaisons m à m des e facteurs premiers idéaux, sans exclure les facteurs premiers égaux, on aura toutes les manières de produire le facteur q^{mf} de la norme. Cela se fera, comme on sait, de

$$\frac{e(e+1).(e+2)\ \ldots(e+m-1)}{1.2.3\ldots\ m}$$

manières différentes. De même le facteur de la norme $q'^{m'f'}$ pourra être produit de

$$\frac{e'(e'+1).(e'+2)\ \ldots(e'+m'-1)}{1.2.3\ldots\ m'}$$

manières différentes, si

$$e' = \frac{\lambda - 1}{f'},$$

et ainsi de suite. Observons encore que le facteur λ^n ne sera produit que d'une seule manière, savoir par le facteur $(1-\alpha)^n$, qui doit être contenu dans $F(\alpha)$. En combinant ces résultats particuliers, on voit que le terme

$$\frac{s-1}{[NF(\alpha)]^s} = \frac{s-1}{(\lambda^n.q^{mf}.q'^{m'f'}.q''^{m''f''}\ldots)^s},$$

pour des valeurs déterminées des nombres premiers q, q', q'',... et des nombres n, m, m', m'',..., sera contenu

$$\frac{e(e+1)\ldots(e+m-1)}{1.2\ldots\ m}\cdot\frac{e'(e'+1)\ldots(e'+m'-1)}{1.2\ldots\ m'}\cdot\frac{e''(e''+1)\ldots(e''+m''-1)}{1.2\ldots\ m''}\ldots$$

fois précisément dans la série R. Donc cette série pourra être représentée de cette manière,

$$R = (s-1)\sum\frac{\dfrac{e(e+1)\ldots(e+m-1)}{1.2\ldots\ m}\cdot\dfrac{e'(e'+1)\ldots(e'+m'-1)}{1.2\ldots\ m'}\ldots}{\lambda^{ns}.q^{mfs}.q'^{m'f's}\ldots},$$

où le signe sommatoire est pris par rapport à toutes les valeurs entières positives, zéro y compris, des nombres n, m, m', m''.... Toutes ces sommations s'effectuent sans difficulté au moyen des séries binô-

miales

$$1+\frac{1}{\lambda^s}+\frac{1}{\lambda^{2s}}+\frac{1}{\lambda^{3s}}+\ldots=\frac{1}{1-\frac{1}{\lambda^s}},$$

$$1+\frac{e}{1}\frac{1}{q^{fs}}+\frac{e(e+1)}{1.2}\cdot\frac{1}{q^{2fs}}+\ldots=\left(\frac{1}{1-\frac{1}{q^{fs}}}\right)^e,$$

$$1+\frac{e'}{1}\frac{1}{q'^{f's}}+\frac{e'(e'+1)}{1.2}\cdot\frac{1}{q'^{2f's}}+\ldots=\left(\frac{1}{1-\frac{1}{q'^{f's}}}\right)^{e'},$$

. . . . . .

On aura donc la série R exprimée comme produit d'un nombre infini de facteurs

$$R=\frac{s-1}{1-\frac{1}{\lambda^s}}\left(\frac{1}{1-\frac{1}{q^{fs}}}\right)^e\cdot\left(\frac{1}{1-\frac{1}{q'^{f's}}}\right)^{e'}\ldots.$$

En séparant les nombres premiers q, suivant les exposants auxquels ils appartiennent, on aura autant de produits infinis qu'il y a de diviseurs différents de $\lambda-1$. Le produit total donnera

$$R=\frac{s-1}{1-\frac{1}{\lambda^s}}\Pi\left(\frac{1}{1-\frac{1}{q^{fs}}}\right)^e\cdot\Pi\left(\frac{1}{1-\frac{1}{q'^{f's}}}\right)^{e'}\ldots,$$

où le premier signe du produit Π se rapporte à tous les nombres premiers q, qui appartiennent à l'exposant f, le second à ceux qui appartiennent à l'exposant f', et ainsi de suite.

Soient à présent β une racine primitive de l'équation $\beta^{\lambda-1}=1$, r un nombre entier, tel que le plus grand diviseur commun de r et $\lambda-1$ est égal à e; on aura évidemment

$$1-\frac{1}{q^{fs}}=\left(1-\frac{1}{q^s}\right)\cdot\left(1-\frac{\beta^r}{q^s}\right)\cdot\left(1-\frac{\beta^{2r}}{q^s}\right)\ldots\left(1-\frac{\beta^{(f-1)r}}{q^s}\right).$$

En élevant à la puissance $-e$, et observant qu'on a généralement

$$\beta^{kr}=\beta^{(k+f)r}=\beta^{(k+2f)r},\ldots,$$

on conclut de là que

$$\left(\frac{1}{1-\frac{1}{q^{fs}}}\right)^{e} = \left(\frac{1}{1-\frac{1}{q^{s}}}\right)\cdot\left(\frac{1}{1-\frac{\beta^{r}}{q^{s}}}\right)\cdot\left(\frac{1}{1-\frac{\beta^{2r}}{q^{s}}}\right)\cdots\left(\frac{1}{1-\frac{\beta^{(\lambda-2)r}}{q^{s}}}\right).$$

Le nombre r, dont le plus grand diviseur commun avec $\lambda - 1$ doit être égal à e, pourra toujours être pris égal à l'indice de q; car, en posant

$$r \equiv \operatorname{ind} q \pmod{(\lambda-1)},$$

on a

$$q \equiv \gamma^{r} \pmod{\lambda},$$

et puisque q appartient à l'exposant f, on aura

$$q^{f} \equiv \gamma^{rf} \equiv 1,$$

d'où l'on conclut que $r = \operatorname{ind} q$ sera un multiple de e; mais s'il y avait un facteur plus grand de $r = \operatorname{ind} q$ et $\lambda - 1$, f ne serait pas le plus petit exposant pour lequel on a $q^{f} \equiv 1 \pmod{\lambda}$. La substitution de la valeur convenable $r = \operatorname{ind} q$ donne

$$\left(\frac{1}{1-\frac{1}{q^{fs}}}\right)^{e} = \left(\frac{1}{1-\frac{1}{q^{s}}}\right)\cdot\left(\frac{1}{1-\frac{\beta^{\operatorname{ind} q}}{q^{s}}}\right)\cdot\left(\frac{1}{1-\frac{\beta^{2\operatorname{ind} q}}{q^{s}}}\right)\cdots\left(\frac{1}{1-\frac{\beta^{(\lambda-2)\operatorname{ind} q}}{q^{s}}}\right).$$

Les nombres f et e n'étant plus contenus dans cette expression, on voit que le même résultat subsiste non-seulement pour les nombres premiers q, qui appartiennent à l'exposant f, mais aussi pour tous les autres q', q'', etc., qui appartiennent aux exposants f', f'', etc. Donc, si l'on fait subir les mêmes transformations à tous les autres facteurs du produit trouvé, on aura cette nouvelle expression de R,

$$\mathrm{R} = \frac{s-1}{1-\frac{1}{\lambda^{s}}}\,\Pi\left(\frac{1}{1-\frac{1}{q^{s}}}\right)\cdot\Pi\left(\frac{1}{1-\frac{\beta^{\operatorname{ind} q}}{q^{s}}}\right)\cdot\Pi\left(\frac{1}{1-\frac{\beta^{2\operatorname{ind} q}}{q^{s}}}\right)\cdots\Pi\left(\frac{1}{1-\frac{\beta^{(\lambda-2)\operatorname{ind} q}}{q^{s}}}\right),$$

où tous les $\lambda - 1$ signes des produits s'étendent sur tous les nombres premiers, excepté le seul λ.

Les produits infinis de cette formule sont connus par le célèbre Mémoire de M. Lejeune-Dirichlet sur la Progression arithmétique, lu à

l'Académie de Berlin le 27 juillet 1837. Nous ne nous arrêterons pas à développer ici leur transformation en séries infinies très-simples, et la sommation de ces séries, pour le cas de $s = 1$, qu'on trouve dans le premier et dans le quatrième paragraphe du Mémoire cité. En se servant d'une méthode élégante due à Euler, M. Dirichlet a trouvé

$$\Pi \frac{1}{1 - \frac{\beta^{k \operatorname{ind} q}}{q^s}} = \sum \frac{\beta^{k \operatorname{ind} n}}{n^s},$$

où le signe sommatoire s'étend à tous les nombres entiers positifs n, non divisibles par λ. La substitution des séries au lieu des produits donne

$$R = \frac{s-1}{1 - \frac{1}{\lambda^s}} \sum \frac{1}{n^s} \cdot \sum \frac{\beta^{\operatorname{ind} n}}{n^s} \cdot \sum \frac{\beta^{2 \operatorname{ind} n}}{n^s} \cdots \sum \frac{\beta^{(\lambda-2) \operatorname{ind} n}}{n^s}.$$

Maintenant, si l'on fait converger indéfiniment s vers la limite $s = 1$, on aura, d'après un théorème de M. Dirichlet,

$$(s-1) \sum \frac{1}{n^s} = 1 - \frac{1}{\lambda} \quad \text{pour} \quad s = 1,$$

et puisque les autres séries contenues dans l'expression de R ne cessent pas d'être convergentes pour $s = 1$, on a

$$R = \sum \frac{\beta^{\operatorname{ind} n}}{n} \cdot \sum \frac{\beta^{2 \operatorname{ind} n}}{n} \cdots \sum \frac{\beta^{(\lambda-2) \operatorname{ind} n}}{n} \quad \text{pour} \quad s = 1.$$

Les sommes finies de ces séries, trouvées par M. Dirichlet au § IV du Mémoire cité, peuvent être représentées de la manière suivante :

1°. Si k est impair,

$$\sum \frac{\beta^{-k \operatorname{ind} n}}{n} = \frac{\pi \sqrt{-1}}{\lambda (\beta^k, \alpha)} \left[1 + \gamma_1 \beta^k + \gamma_2 + \beta^{2k} + \gamma_3 \beta^{3k} \cdots + \gamma_{\lambda-2} \beta^{(\lambda-2)k} \right],$$

où $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_{\lambda-2}$ désignent les plus petits restes positifs des puissances correspondantes de la racine primitive γ, γ^2, $\gamma^3, \ldots, \gamma^{\lambda-2}$, pour le module λ, et (β^k, α) l'expression connue de la division du cercle

$$(\beta^k, \alpha) = \alpha + \beta^k \alpha^\gamma + \beta^{2k} \alpha^{\gamma^2} + \beta^{3k} \alpha^{\gamma^3} + \ldots + \beta^{(\lambda-2)k} \alpha^{\gamma^{(\lambda-2)}};$$

2°. Si k est pair,

$$\sum \frac{\beta^{-k \operatorname{ind} n}}{n} = \frac{2\left[le(\alpha) + \beta^k le(\alpha^{\gamma^k}) + \beta^{2k} le(\alpha^{\gamma^{2k}}) + \ldots + \beta^{(\mu-1)k} le\left(\alpha^{\gamma^{(\mu-1)k}}\right)\right]}{(1-\beta^{-k}).(\beta^k, \alpha)},$$

où l'on a mis, pour abréger,

$$\mu = \frac{\lambda - 1}{2},$$

et où $e(\alpha)$ désigne l'unité complexe

$$e(\alpha) = \sqrt{\frac{(1-\alpha^{\gamma}).(1-\alpha^{-\gamma})}{(1-\alpha).(1-\alpha^{-1})}} = \pm \frac{\alpha^{\mu(\gamma-1)}(1-\alpha^{\gamma})}{1-\alpha},$$

la même qui nous a donné un système indépendant d'unités dans le deuxième paragraphe de ce Mémoire.

Substituons ces sommes dans l'expression trouvée de R, en faisant, pour abréger,

$$1 + \gamma_1 \beta + \gamma_2 \beta^2 + \gamma_3 \beta^3 + \ldots + \gamma_{\lambda-2} \beta^{\lambda-2} = \varphi(\beta),$$

$$\varphi(\beta).\varphi(\beta^3).\varphi(\beta^5)\ldots\varphi(\beta^{\lambda-2}) = \mathrm{P},$$

et comme ci-dessus, dans le § II,

$$le(\alpha) + \beta^2 le(\alpha) + \beta^4 le(\alpha^{\gamma^2}) + \ldots + \beta^{2\mu-2} le\left(\alpha^{\gamma^{\mu-1}}\right) = \mathrm{L}(\beta^2),$$

nous aurons

$$\mathrm{R} = \frac{2^{\mu-1}\pi^{\mu}(-1)^{\frac{\mu}{2}}\,\mathrm{P}\,\mathrm{L}(\beta^2).\mathrm{L}(\beta^4).\mathrm{L}(\beta^6)\ .\ \mathrm{L}(\beta^{2\mu-2})}{\lambda^{\mu}(\beta, \alpha).(\beta^3, \alpha)\ldots(\beta^{\lambda-2}, \alpha).(1-\beta^{-2})\ (1-\beta^{-4})\ldots(1-\beta^{-(2\mu-2)})}.$$

Or nous avons trouvé, dans le § II, qu'en désignant par D le déterminant des quantités

$$\begin{array}{l} le(\alpha),\ le(\alpha^{\gamma}),\ldots,\ le(\alpha^{\gamma^{\mu-2}}), \\ le(\alpha^{\gamma}),\ le(\alpha^{\gamma^2}),\ldots,\ le(\alpha^{\gamma^{\mu-1}}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ le(\alpha^{\gamma^{\mu-2}}),\ le(\alpha^{\gamma^{\mu-1}}),\ldots,\ le(\alpha^{\gamma^{\mu-4}}), \end{array}$$

on a

$$L(\beta^2).L(\beta^4).L(\beta^6)...L(\beta^{2-\mu-2}) = \mu D;$$

de plus, les équations

$$(\beta^k, \alpha).(\beta^{-k}, \alpha) = \pm \lambda \quad \text{et} \quad (\beta^\mu, \alpha) = (-1, \alpha) = \pm \sqrt{(-1)^{\mu\lambda}}$$

donnent

$$(\beta, \alpha).(\beta^2, \alpha)...(\beta^{\lambda-2}, \alpha) = \pm \lambda^{\mu+\frac{1}{2}} \sqrt{(-1)^\mu},$$

et l'on a

$$(1-\beta^{-2}).(1-\beta^{-4})...(1-\beta^{2-\mu-2}) = \mu :$$

donc on aura enfin l'expression simplifiée

$$R = \frac{2^{\mu-1}\pi^\mu PD}{\lambda^{2\mu-\frac{1}{2}}} \quad \text{pour} \quad s = 1.$$

Après avoir trouvé cette somme de la série R, pour le cas limite $s = 1$, nous venons à la seconde partie de notre recherche, dont le but sera de trouver une nouvelle expression de la même série R, afin que la comparaison de ces deux résultats nous donne le nombre cherché des classes des nombres idéaux.

Dans la série proposée

$$R = \sum \frac{s-1}{[NF(\alpha)]^s},$$

où $F(\alpha)$ représente tous les nombres complexes différents, existants et idéaux, nous séparons les termes suivant les classes diverses auxquelles appartiennent les nombres complexes $F(\alpha)$. En désignant par $f(\alpha)$ tous les nombres de la première classe, c'est-à-dire les nombres complexes existants, par $f_1(\alpha)$ les nombres idéaux de la deuxième classe, par $f_2(\alpha)$ ceux de la troisième classe, et ainsi de suite; et en nommant H le nombre de toutes les classes diverses, nous avons

$$R = \sum \frac{s-1}{[Nf(\alpha)]^s} + \sum \frac{s-1}{[Nf_1(\alpha)]^s} + ... + \sum \frac{s-1}{[Nf_{H-1}(\alpha)]^s};$$

il s'agira donc de trouver les sommes de ces H séries particulières, pour le cas limite $s = 1$. Nous démontrerons ci-après que toutes ces sommes, prises par rapport aux diverses classes des nombres idéaux,

sont égales entre elles; c'est pour cette raison que nous nous bornerons ici à trouver seulement la première somme, qui ne contient que les nombres complexes existants.

Tous les nombres complexes existants sont contenus dans la forme

$$f(\alpha) = x\alpha + x_1\alpha^{\gamma} + x_2\alpha^{\gamma^2} + \ldots + x_{\lambda-2}\alpha^{\gamma^{\lambda-2}},$$

dans laquelle les coefficients

$$x, \quad x_1, \quad x_2, \ldots, \quad x_{\lambda-2}$$

représentent tous les nombres entiers; mais pour toutes ces valeurs différentes des coefficients, on n'obtiendra pas des nombres complexes différents, car on sait qu'au moyen des unités complexes, le même nombre complexe peut être représenté, par la forme proposée, d'une infinité de manières différentes. Il s'agira donc d'abord de trouver les conditions auxquelles les coefficients

$$x, \quad x_1, \quad x_2, \ldots, \quad x_{\lambda-2}$$

doivent être assujettis, pour que $f(\alpha)$ ne soit qu'une seule fois contenu dans cette forme. A cet effet, j'observe que $f'(\alpha)$ étant une expression déterminée du nombre complexe dont il s'agit, on aura toutes les autres expressions du même nombre, en multipliant celui-ci par une unité quelconque; et puisque toutes les unités sont contenues dans la forme

$$\varepsilon(\alpha) = \pm \alpha^n \varepsilon_1(\alpha)^{m_1} \varepsilon_2(\alpha)^{m_2} \ldots \varepsilon_{\mu-1}(\alpha)^{m_{\mu-1}},$$

où $\varepsilon_1(\alpha)$, $\varepsilon_2(\alpha)$,..., $\varepsilon_{\mu-1}(\alpha)$ sont $\mu - 1$ unités fondamentales, la forme

$$f(\alpha) = \pm \alpha^n \varepsilon_1(\alpha)^{m_1} . \varepsilon_2(\alpha)^{m_2} \ldots \varepsilon_{\mu-1}(\alpha)^{m_{\mu-1}} f'(\alpha),$$

pour toutes les valeurs entières des exposants n, m_1, m_2,..., $m_{\mu-1}$, contiendra toutes les expressions possibles du même nombre complexe. Lorsqu'on y change α en α^{-1}, on obtient, en multipliant,

$$f(\alpha).f(\alpha^{-1}) = \varepsilon_1(\alpha)^{2m_1} . \varepsilon_2(\alpha)^{2m_2} \ldots \varepsilon_{\mu-1}(\alpha)^{2m_{\mu-1}} f'(\alpha).f'(\alpha^{-1}).$$

En passant aux logarithmes, et changeant α en α^{γ}, α^{γ^2},..., $\alpha^{\gamma^{\lambda-2}}$,

on a ce système d'équations,

$$\tfrac{1}{2}\,l\,[rf(\alpha).f(\alpha^{-1})] = m_1\,l\varepsilon_1(\alpha) + m_2\,l\varepsilon_2(\alpha) + \ldots + m_{\mu-1}\,l\varepsilon_{\mu-1}(\alpha) + \tfrac{1}{2}\,l\,[rf'(\alpha).f'(\alpha^{-1})],$$

$$\tfrac{1}{2}\,l\,[rf(\alpha^{\gamma}).f(\alpha^{-\gamma})] = m_1\,l\varepsilon_1(\alpha^{\gamma}) + m_2\,l\varepsilon_2(\alpha^{\gamma}) + \ldots + m_{\mu-1}\,l\varepsilon_{\mu-1}(\alpha^{\gamma}) + \tfrac{1}{2}\,l\,[rf'(\alpha^{\gamma}).f'(\alpha^{-\gamma})],$$

. . . . . .

$$\tfrac{1}{2}\,l\left[rf\left(\alpha^{\gamma^{\mu-2}}\right).f\left(\alpha^{-\gamma^{\mu-2}}\right)\right] = m_1\,l\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right) + m_2\,l\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right) + \ldots + m_{\mu-1}\,l\varepsilon^{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right) + \tfrac{1}{2}\,l\left[rf'\left(\alpha^{\gamma^{\mu-2}}\right).f'\left(\alpha^{-\gamma^{\mu-2}}\right)\right],$$

où le nombre r est tout à fait arbitraire.

Mettons à présent

$$\tfrac{1}{2}\,l\,[rf'(\alpha).f'(\alpha^{-1})] = \gamma_1\,l\varepsilon_1(\alpha) + \gamma_2\,l\varepsilon_2(\alpha) + \ldots + \gamma_{\mu-1}\,l\varepsilon_{\mu-1}(\alpha),$$

$$\tfrac{1}{2}\,l\,[rf'(\alpha^{\gamma}).f'(\alpha^{-\gamma})] = \gamma_1\,l\varepsilon_1(\alpha^{\gamma}) + \gamma_2\,l\varepsilon_2(\alpha^{\gamma}) + \ldots + \gamma_{\mu-1}\,l\varepsilon_{\mu-1}(\alpha^{\gamma}),$$

. . . . . .

$$\tfrac{1}{2}\,l\left[rf'\left(\alpha^{\gamma^{\mu-2}}\right).f'\left(\alpha^{\gamma^{\mu-2}}\right)\right] = \gamma_1\,l\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right) + \gamma_2\,l\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right) + \ldots + \gamma_{\mu-1}\,l\varepsilon_{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right);$$

les inconnues $\gamma_1, \gamma_2, \ldots, \gamma_{\mu-1}$ de ce système d'équations linéaires auront toujours des valeurs finies et déterminées, parce que le déterminant du système, ou bien le déterminant Δ du § II de ce Mémoire, n'est pas égal à zéro. Ce système d'équations, ajouté au précédent, donne aussi

$$\tfrac{1}{2}\,l\,[rf(\alpha).f(\alpha^{-1})] = (m_1+\gamma_1)\,l\varepsilon_1(\alpha) + (m_2+\gamma_2)\,l\varepsilon_2(\alpha) + \ldots + (m_{\mu-1}+\gamma_{\mu-1})\,l\varepsilon_{\mu-1}(\alpha),$$

$$\tfrac{1}{2}\,l\,[rf(\alpha^{\gamma}).f(\alpha^{-\gamma})] = (m_1+\gamma_1)\,l\varepsilon_1(\alpha^{\gamma}) + (m_2+\gamma_2)\,l\varepsilon_2(\alpha^{\gamma}) + \ldots + (m_{\mu-1}+\gamma_{\mu-1})\,l\varepsilon_{\mu-1}(\alpha^{\gamma}),$$

. . . . . .

$$\tfrac{1}{2}\,l\left[rf\left(\alpha^{\gamma^{\mu-2}}\right).f\left(\alpha^{-\gamma^{\mu-2}}\right)\right] = (m_1+\gamma_1)\,l\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right) + (m_2+\gamma_2)\,l\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right) + \ldots + (m_{\mu-1}+\gamma_{\mu-1})\,l\varepsilon_{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right).$$

On voit par là que les expressions de

$$\tfrac{1}{2}\,l\,[r f'(\alpha).f'(\alpha^{-1})] \quad \text{et} \quad \tfrac{1}{2}\,l\,r\,[rf(\alpha).f(\alpha^{-1})],$$

et celles qu'on en déduit par le changement de α en α^{γ}, $\alpha^{\gamma^2},\ldots,\alpha^{\gamma^{\mu-1}}$, ne diffèrent qu'en ce que les quantités $\gamma_1,\gamma_2,\ldots,\gamma_{\mu-1}$ sont augmentées des nombres entiers positifs ou négatifs $m_1, m_2,\ldots, m_{\mu-1}$. On pourra donc toujours choisir convenablement les nombres entiers $m_1, m_2,\ldots, m_{\mu-1}$, de manière que les quantités $m_1+\gamma_1, m_2+\gamma_2,\ldots, m_{\mu-1}+\gamma_{\mu-1}$ soient toutes contenues entre les limites o et 1, et par cette condition, les nombres entiers $m_1, m_2,\ldots, m_{\mu-1}$ seront parfaitement déterminés. Mettant donc, pour abréger,

$$m_1+\gamma_1=z_1,\quad m_2+\gamma_2=z_2,\ldots, m_{\mu-1}+\gamma_{\mu-1}=z_{\mu-1},$$

nous concluons que parmi tous les nombres complexes contenus dans la forme

$$f(x)=\varepsilon_1(\alpha)^{m_1}.\varepsilon_2(\alpha)^{m_2}\ldots\varepsilon_{\mu-1}(\alpha)^{m_{\mu-1}}f'(\alpha),$$

il y aura toujours un, et il n'y aura jamais qu'un seul qui satisfait aux conditions

$$\tfrac{1}{2}\,l\,[r f(\alpha)f(\alpha^{-1})]=z_1\,l\,\varepsilon_1(\alpha)+z_2\,l\,\varepsilon_2(\alpha)+\ldots+z_{\mu-1}\,l\,\varepsilon_{\mu-1}(\alpha),$$

$$\tfrac{1}{2}\,l\left[r f\left(\alpha^{\gamma}\right)f\left(\alpha^{-\gamma}\right)\right]=z_1\,l\,\varepsilon_1\left(\alpha^{\gamma}\right)+z_2\,l\,\varepsilon_2\left(\alpha^{\gamma}\right)+\ldots+z_{\mu-1}\,l\,\varepsilon_{\mu-1}\left(\alpha^{\gamma}\right),$$

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

$$\tfrac{1}{2}\,l\left[r f\left(\alpha^{\gamma^{\mu-2}}\right)f\left(\alpha^{-\gamma^{\mu-2}}\right)\right]=z_1\,l\,\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right)+z_2\,l\,\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right)+\ldots$$
$$+z_{\mu-1}\,l\,\varepsilon_{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right),$$

$z_1, z_2,\ldots, z^{\mu-1}$ désignant des quantités contenues entre les limites o et 1. A cause du facteur $\pm\alpha^n$, qu'il faut encore ajouter pour avoir toutes les expressions de $f(\alpha)$, facteur qui donne lieu à 2λ valeurs différentes. il y aura toujours 2λ représentations du nombre $f(\alpha)$, pour lesquelles les conditions posées seront satisfaites. Il serait facile d'ajouter une nouvelle condition des coefficients, en vertu de laquelle le nombre $f(\alpha)$ n'aurait qu'une seule représentation; mais il suffira de savoir que le nombre des représentations de $f(\alpha)$ est exactement égal à 2λ.

D'après les principes établis par M. Lejeune-Dirichlet dans ses recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, on obtient la valeur de la somme

$$\sum \frac{s-1}{[\mathrm{N}f(\alpha)]^s}, \quad \text{pour} \quad s=1,$$

égale au quotient du nombre des termes de cette série, pour lesquels $\mathrm{N}f(\alpha)$ est inférieur à T, divisé par T, lorsqu'on y fait croître la quantité T à l'infini. Nous obtiendrons le nombre des termes pour lesquels on a $\mathrm{N}f(\alpha)<\mathrm{T}$, en recherchant combien il y a de systèmes de valeurs des coefficients x, $x_1,\ldots,$ $x_{\lambda-2}$, compatibles aux $\mu-1$ conditions posées jointes à la condition $\mathrm{N}f(\alpha)<\mathrm{T}$, et puis divisant ce nombre par 2λ. Pour cela, nous changeons les quantités x, $x_1,\ldots,$ $x_{\lambda-2}$ en $\frac{x}{t}, \frac{x_1}{t},\ldots, \frac{x_{\lambda-2}}{t}$; d'où $f(\alpha)$ se change en $\frac{f(\alpha)}{t}$, $\mathrm{N}f(\alpha)$ en $\frac{\mathrm{N}f(\alpha)}{t^{\lambda-1}}$; alors les nouvelles quantités $x, x_1,\ldots, x_{\lambda-1}$ n'obtiendront plus toutes les valeurs entières compatibles aux conditions posées, mais les valeurs d'une série arithmétique doublement infinie, dont la différence est égale à t. Les $\mu-1$ conditions pour les nouvelles quantités $x, x_1,\ldots,$ $x_{\lambda-2}$ ne sont altérées qu'en ce que, au lieu de r on aura $\frac{r}{t^2}$, et puisque r est tout à fait arbitraire, on prendra $r=t^2$, ce qui revient à faire $r=1$ dans les conditions données ci-dessus. De plus, en prenant $\mathrm{T}=\frac{1}{t^{\lambda-1}}$, au lieu de $\mathrm{N}f(\alpha)<\mathrm{T}$, on a pour les nouveaux coefficients du nombre $f(\alpha)$ la condition $\mathrm{N}f(\alpha)<1$. Maintenant, si l'on prend t infiniment petit, les quantités x, $x_1,\ldots,$ $x_{\lambda-2}$ seront des variables continues, le nombre des valeurs de x pourra être représenté sous la forme $\frac{1}{t}\int dx$, le nombre des valeurs de x_1 sous la forme $\frac{1}{t}\int dx_1$, etc.; donc le nombre de toutes les combinaisons des valeurs de $x, x_1,\ldots, x_{\lambda-1}$ sera donné par l'intégrale multiple

$$\frac{1}{t^{\lambda-1}}\int^{(\lambda-1)} dx.dx_1.dx_2\ldots dx_{\lambda-2},$$

ce qui donne, en divisant par $T = \frac{1}{e^{\lambda-1}}$,

$$\int^{(\lambda-1)} dx.dx_1.dx_2...dx_{\lambda-2}.$$

Nous en concluons que la valeur de la somme proposée, pour le cas de $s = 1$, est donnée par la formule

$$\sum \frac{s-1}{[Nf(\alpha)]^s} = \frac{1}{2\lambda} \int^{(\lambda-1)} dx.dx_1.dx_2...dx_{\lambda-2},$$

où les intégrations s'étendent sur toutes les valeurs des variables x, $x_1,\ldots, x_{\lambda-2}$ entre les limites $-\infty$ et $+\infty$, qui satisfont à la condition $Nf(\alpha) > 1$ et aux équations

$$\tfrac{1}{2}l[rf(\alpha).f(\alpha^{-1})] = z_1 l\varepsilon_1(\alpha) + z_2 l\varepsilon_2(\alpha) + \ldots + z_{\mu-1} l\varepsilon_{\mu-1}(\alpha),$$

$$\tfrac{1}{2}l\left[rf(\alpha^{\gamma}).f(\alpha^{-\gamma})\right] = z_1 l\varepsilon_1(\alpha^{\gamma}) + z_2 l\varepsilon_2(\alpha^{\gamma}) + \ldots + z_{\mu-1} l\varepsilon_{\mu-1}(\alpha^{\gamma}),$$

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

$$\tfrac{1}{2}l\left[rf(\alpha^{\gamma^{\mu-2}}).f(\alpha^{-\gamma^{\mu-2}})\right] = z_1 l\varepsilon_1(\alpha^{\gamma^{\mu-2}}) + z_2 l\varepsilon_2(\alpha^{\gamma^{\mu-2}}) + \ldots + z_{\mu-1} l\varepsilon_{\mu-1}(\alpha^{\gamma^{\mu-2}}),$$

où les quantités $z_1, z_2, \ldots, z_{\mu-1}$ sont contenues entre les limites 0 et 1.

Pour déterminer la valeur de l'intégrale

$$\int^{(\lambda-1)} dx.dx_1.dx_2...dx_{\lambda-2} = I,$$

nous y appliquerons quelques transformations successives, qui seront effectuées d'après les règles connues pour la transformation des intégrales multiples.

D'abord nous introduirons les nouvelles variables y, y_1, $y_2,\ldots$, $y_{\lambda-2}$, liées aux variables x, x_1, $x_2,\ldots, x_{\lambda-2}$ par les équations

$$y = f(\alpha), \quad y_1 = f(\alpha^{\gamma}), \quad y_2 = f(\alpha^{\gamma^2}),\ldots, \quad y_{\lambda-2} = f(\alpha^{\gamma^{\lambda-2}}).$$

Les différentielles partielles des nouvelles variables, prises par rapport aux variables x, $x_1, \ldots, x^{\lambda-2}$, sont données par la formule

$$\frac{dy_k}{dx_h} = \alpha^{\gamma^{k+h}},$$

d'où il suit que le déterminant

$$\Sigma\left(\pm \frac{dy}{dx} \cdot \frac{dy_1}{dx_1} \cdots \frac{dy_{\lambda-2}}{dx_{\lambda-2}}\right)$$

sera le déterminant des quantités

$$\begin{array}{llll} \alpha, & \alpha\gamma, & \alpha^{\gamma^2}, \ldots, & \alpha^{\gamma^{\lambda-2}}, \\ \alpha^{\gamma}, & \alpha^{\gamma^2}, & \alpha^{\gamma^3}, \ldots, & \alpha, \\ \cdots & \cdots & \cdots & \cdots \\ \alpha^{\gamma^{\lambda-2}}, & \alpha, & \alpha^{\gamma}, \ldots, & \alpha^{\gamma^{\lambda-3}}, \end{array}$$

qu'on sait être égal au produit des différences de toutes ces quantités prises deux à deux,

$$\begin{array}{l} \left(\alpha - \alpha^{\gamma}\right)\left(\alpha - \alpha^{\gamma^2}\right) \ldots \left(\alpha - \alpha^{\gamma^{\lambda-2}}\right), \\ \qquad \left(\alpha^{\gamma} - \alpha^{\gamma^2}\right) \ldots \left(\alpha^{\gamma} - \alpha^{\gamma^{\lambda-2}}\right), \\ \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\ \qquad\qquad\qquad\qquad \left(\alpha^{\gamma^{\lambda-3}} - \alpha^{\gamma^{\lambda-2}}\right). \end{array}$$

Ce produit, qui contient $\frac{(\lambda-1)(\lambda-2)}{2}$ facteurs premiers de λ, est égal à la puissance $\lambda^{\frac{\lambda-2}{2}}$, d'où résulte

$$\Sigma\left(\pm \frac{dy}{dx} \cdot \frac{dy_1}{dx_1} \cdots \frac{dy_{\lambda-2}}{dx_{\lambda-2}} = \lambda^{\frac{\lambda-2}{2}}\right);$$

et puisqu'on obtient l'intégrale multiple transformée en divisant par ce déterminant, on aura la première transformée

$$\mathrm{I} = \frac{1}{\lambda^{\frac{\lambda-2}{2}}} \int^{(\lambda-1)} dy\, dy_1 \ldots dy_{\lambda-2}.$$

Transformons de nouveau par les substitutions

$$\mathrm{l}\gamma = v + \omega\sqrt{-1},\ \mathrm{l}\gamma_1 = v_1 + \omega_1\sqrt{-1},\ldots,\ \mathrm{l}\gamma_{\mu-1} = v_{\mu-1} + \omega_{\mu-1}\sqrt{-1},$$
$$\mathrm{l}\gamma_\mu = v - \omega\sqrt{-1},\quad \mathrm{l}\gamma_{\mu+1} = v_1 - \omega_1\sqrt{-1},\ldots,$$
$$\mathrm{l}\gamma_{2\mu-1} = v_{\mu-1} - \omega_{\mu-1}\sqrt{-1},$$

nous aurons en général

$$\frac{d\gamma_k}{\gamma_k} = dv_k + \sqrt{-1}\,d\omega_k,\quad \frac{d\gamma_{k+\mu}}{\gamma_{k+\mu}} = dv_k - \sqrt{-1}\,d\omega_k.$$

Alors au lieu de $d\gamma_k\,d\gamma_{k+\mu}$ dans l'intégrale multiple, il faudra substituer l'expression

$$\left(\frac{d\gamma_k}{dv_k}\cdot\frac{d\gamma_{k+\mu}}{d\omega_k} - \frac{d\gamma_k}{d\omega_k}\cdot\frac{d\gamma_{k+\mu}}{dv_k}\right)dv_k\,d\omega_k,$$

qui se réduit à

$$-2\sqrt{-1}\ e^{2v_k}\,dv_k.d\omega_k,$$

et l'on aura l'intégrale transformée

$$\mathrm{I} = \frac{2^\mu}{\lambda^{\frac{\lambda-2}{2}}}\int^{(\lambda-1)} e^{2v}.e^{2v_1}\ldots e^{2v_{\mu-1}}\,dv\,dv_1\ldots dv_{\mu-1}\,d\omega\,d\omega_1\ldots d\omega_{\mu-1}.$$

Ayant posé

$$f\left(\alpha^{\gamma^k}\right) = \gamma_k = e^{v_k+\omega_k\sqrt{-1}},\quad f\left(\alpha^{-\gamma^k}\right) = \gamma_{k+\mu} = e^{v_k-\omega_k\sqrt{-1}},$$

nous avons

$$f\left(\alpha^{\gamma^k}\right).f\left(\alpha^{-\gamma^k}\right) = e^{2v_k},\quad v_k = \tfrac{1}{2}\mathrm{l}\left[f\left(\alpha^{\gamma^k}\right).f\left(\alpha^{-\gamma^k}\right)\right];$$

les limites des nouvelles variables seront donc déterminées par les équations

$$v = z_1\mathrm{l}\varepsilon_1(\alpha) + z_2\mathrm{l}\varepsilon_2(\alpha) + \ldots + z_{\mu-1}\mathrm{l}\varepsilon_{\mu-1}(\alpha),$$
$$v_1 = z_1\mathrm{l}\varepsilon_1\left(\alpha^\gamma\right) + z_2\mathrm{l}\varepsilon_2\left(\alpha^\gamma\right) + \ldots + z_{\mu-1}\mathrm{l}\varepsilon_{\mu-1}\left(\alpha^\gamma\right),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$v_{\mu-2} = z_1\mathrm{l}\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right) + z_2\mathrm{l}\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right) + \ldots + z_{\mu-1}\mathrm{l}\varepsilon_{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right).$$

où $z_1, z_2, \ldots, z_{\mu-1}$ sont contenus entre les limites o et 1. La condition $\mathrm{N} f(\alpha) < 1$ donne, en outre,

$$e^{2v} . e^{2v_1} \ldots e^{2v_{\mu-1}}$$

entre les limites o et 1.

Les μ variables $\omega, \omega_1, \ldots, \omega_{\mu-1}$, qui ne sont pas limitées par ces conditions, sont données comme fonctions des variables primitives $x, x_1, \ldots, x_{\lambda-2}$ par l'équation

$$\operatorname{tang}(\omega_k) = \frac{f\left(\alpha^{\gamma^k}\right) - f\left(\alpha^{-\gamma^k}\right)}{\sqrt{-1}\left[f\left(\alpha^{\gamma^k}\right) + f\left(\alpha^{-\gamma^k}\right)\right]},$$

expression où les quantités imaginaires disparaissent d'elles-mêmes; et, puisque les quantités $x, x_1, \ldots, x_{\lambda-2}$ peuvent varier entre les limites $-\infty$ et $+\infty$, on voit que la même chose aura lieu pour $\operatorname{tang}(\omega_k)$: et, en considérant encore que $\sin\omega_k$ et $\cos\omega_k$ peuvent avoir toutes les valeurs entre les limites -1 et $+1$, on conclut que les limites des variables $\omega, \omega_1, \omega_2, \ldots, \omega_{\mu-1}$ seront $-\frac{\pi}{2}$ et $+\frac{3\pi}{2}$, ou tout autre intervalle de 2π. En effectuant les intégrations par rapport à ces variables, entre les limites $-\frac{\pi}{2}$ et $+\frac{3\pi}{2}$, on a

$$\mathrm{I} = \frac{2^{2\mu}\pi^{\mu}}{\lambda^{\frac{\lambda-2}{2}}} \int^{(\mu)} e^{2v} . e^{2v_1} \ldots e^{2v_{\mu-1}} \, dv . dv_1 \ldots dv_{\mu-1}.$$

Intégrons à présent par rapport à la variable $v_{\mu-1}$, nous aurons

$$\int e^{2v_{\mu-1}} dv_{\mu-1} = \frac{1}{2} e^{2v_{\mu-1}},$$

les limites de cette intégration étant données par la condition $e^{2v} . e^{2v_1} \ldots e^{2v_{\mu-1}} \gtrless \begin{matrix} 0 \\ 1 \end{matrix}$, et celles de $e^{2v_{\mu-1}}$ étant o et $e^{-2v} . e^{-2v_1} \ldots e^{2v_{\mu-2}}$. L'intégration entre ces limites donne le résultat très-simple

$$\frac{2^{2\mu-2}\pi^{\mu}}{\lambda^{\frac{\lambda-2}{2}}} \int^{(\mu-1)} dv . dv_1 \ldots dv_{\mu-2}.$$

Il nous reste encore à effectuer la dernière transformation de cette

intégrale, qui consiste dans la substitution des variables $z_1, z_2, \ldots, z_{\mu-1}$, données par les équations

$$v = z_1 l\varepsilon_1(\alpha) + z_2 l\varepsilon_2(\alpha) + \ldots + z_{\mu-1} l\varepsilon_{\mu-1}(\alpha),$$

$$v_2 = z_1 l\varepsilon_1(\alpha') + z_2 l\varepsilon_2(\alpha') + \ldots + z_{\mu-1} l\varepsilon_{\mu-1}(\alpha'),$$

. . . . . .

$$v_{\mu-2} = z_1 l\varepsilon_1(\alpha^{\gamma^{\mu-2}}) + z_2 l\varepsilon_2(\alpha^{\gamma^{\mu-2}}) + \ldots + z_{\mu-1} l\varepsilon_{\mu-1}(\alpha^{\gamma^{\mu-2}}),$$

au lieu des variables $v, v_1, \ldots, v_{\mu-2}$. En désignant, comme ci-dessus, par Δ le déterminant de ce système d'équations linéaires, nous avons tout de suite l'intégrale transformée, et, parce que toutes les intégrations par rapport aux variables $z_1, z_2, \ldots, z_{\mu-1}$, doivent être prises entre les limites o et 1, la nouvelle intégrale est évidemment égale à l'unité. Donc la valeur cherchée de l'intégrale I devient

$$\mathrm{I} = \frac{2^{2\mu-1}\pi^{\mu}\Delta}{\lambda^{\frac{\lambda-2}{2}}}.$$

De là résulte cette expression de la somme proposée

$$\sum \frac{s-1}{[\mathrm{N}f(\alpha)]^s} = \frac{2^{2\mu-2}\pi^{\mu}\Delta}{\lambda^{\frac{\lambda}{2}}}, \quad \text{pour} \quad s = 1.$$

Nous allons maintenant démontrer que toutes les autres sommes partielles de l'expression

$$\sum \frac{s-1}{[\mathrm{N}\mathrm{F}(\alpha)]^s} = \sum \frac{s-1}{[\mathrm{N}f(\alpha)]^s} + \sum \frac{s-1}{[\mathrm{N}f_1(\alpha)]^s} + \ldots \sum \frac{s-1}{[\mathrm{N}f_{\mathrm{H}-1}(\alpha)]^s}$$

ont les mêmes valeurs que la première, que nous venons de trouver. Pour cela, soit $\varphi(\alpha)$ un multiplicateur idéal qui, joint aux nombres idéaux de la classe $f_k(\alpha)$, les rend tous existants, et posons

$$\varphi(\alpha) f_k(\alpha) = \mathrm{F}_k(\alpha);$$

nous aurons

$$\sum \frac{s-1}{[\mathrm{N}f_k(\alpha)]^s} = \mathrm{N}\varphi(\alpha) \sum \frac{s-1}{[\mathrm{N}\mathrm{F}_k(\alpha)]^s}, \quad \text{pour} \quad s = 1.$$

où $F_k(\alpha)$ désigne tous les nombres complexes existants qui ont le facteur idéal $\varphi(\alpha)$. La recherche de la valeur de la somme

$$\sum \frac{s-1}{[NF_k(\alpha)]^s}, \quad \text{pour} \quad s=1,$$

se fera de la même manière que celle de la somme trouvée ci-dessus, avec la seule différence qu'il y aura quelques conditions de plus pour les coefficients des nombres $F_k(\alpha)$, pour exprimer que $F_k(\alpha)$ doit contenir le facteur idéal $\varphi(\alpha)$. Supposons que $\varphi(\alpha)$ contient un certain facteur premier idéal de q, m fois, de plus un facteur premier idéal de q', m' fois, etc., où q, q', etc., appartiennent respectivement aux exposants f, f', etc.; la condition que $F_k(\alpha)$ soit divisible par $\varphi(\alpha)$ sera exprimée par f congruences linéaires pour les coefficients de $F_k(\alpha)$ par rapport au module q^m, de plus par f' congruences linéaires pour le module $q'^{m'}$, etc. Or il est clair qu'étant donné f congruences linéaires par rapport aux coefficients du nombre $F_k(\alpha)$, pour le module q^m, le nombre de tous les systèmes des valeurs convenables de ces coefficients se réduira à la $q^{mf\,ième}$ partie; de même, les f' congruences pour le module $q'^{m'}$ réduiront ce nombre de valeurs à la $q'^{m'f'\,ième}$ partie, et ainsi de suite. On en conclut que la valeur de la somme proposée sera égale à la $q^{mf}.q'^{m'f'}\ldots^{ième}$ partie de la valeur de la somme trouvée ci-dessus, et, puisque le produit $q^{mf}.q'^{m'f'}\ldots$ est égal à la norme $N\varphi(\alpha)$, on aura

$$\sum \frac{s-1}{[NF_k(\alpha)]^s} = \frac{1}{N\varphi(\alpha)} \sum \frac{s-1}{[Nf(\alpha)]^s}, \quad \text{pour} \quad s=1;$$

enfin cette équation, jointe à la précédente, donne

$$\sum \frac{s-1}{[Nf_k(\alpha)]^s} = \sum \frac{s-1}{[Nf(\alpha)]^s}, \quad \text{pour} \quad s=1,$$

ce qu'il fallait démontrer.

Le nombre des sommes partielles qui donnent la somme totale R étant égal à H, nous avons

$$R = H \sum \frac{s-1}{[Nf(\alpha)]^s}, \quad \text{pour} \quad s=1;$$

d'où, en substituant la valeur trouvée de cette somme, nous avons la

nouvelle expression

$$R = \frac{2^{2\mu-2}\pi^{\mu}\Delta H}{\frac{\lambda}{\lambda^2}};$$

ce qui, comparé à la valeur de la même série R, trouvée dans la première partie de cette recherche,

$$R = \frac{2^{\mu-1}\pi^{\mu}P.D}{\lambda^{2\mu-\frac{1}{2}}},$$

donne l'expression cherchée du nombre des classes des nombres complexes idéaux

$$H = \frac{P.D}{(2\lambda)^{\mu-1}.\Delta}.$$

Je répète que dans cette formule la lettre P désigne le produit

$$P = \varphi(\beta).\varphi(\beta^3).\varphi(\beta^5)\ldots\varphi(\beta^{\lambda-2}),$$

où β est une racine primitive de l'équation $\beta^{\lambda-1} = 1$, et où

$$\varphi(\beta) = 1 + \gamma_1\beta + \gamma_2\beta^2 + \gamma_3\beta^3 + \ldots + \gamma_{\lambda-2}\beta^{\lambda-2},$$

$\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_{\lambda-2}$ étant les plus petits restes positifs des puissances γ, $\gamma^2, \gamma^3, \ldots, \gamma^{\lambda-2}$ d'une racine primitive γ pour le module λ. La lettre μ n'est qu'un signe abrégé de $\frac{\lambda-1}{2}$. D désigne le déterminant des quantités

$$\begin{array}{l} le(\alpha),\quad le(\alpha^{\gamma}),\ldots,\quad le(\alpha^{\gamma^{\mu-2}}),\\ le(\alpha^{\gamma}),\quad le(\alpha^{\gamma^2}),\ldots,\quad le(\alpha^{\gamma^{\mu-1}}),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ le(\alpha^{\gamma^{\mu-2}}),\quad le(\alpha^{\gamma^{\mu-1}}),\ldots,\quad le(\alpha^{\gamma^{\mu-4}}), \end{array}$$

où

$$e(\alpha) = \sqrt{\frac{(1-\alpha^{\gamma}).(1-\alpha^{-\gamma})}{(1-\alpha)\,(1-\alpha^{-1})}} = \pm\frac{\alpha^{\mu(\gamma-1)}(1-\alpha^{\gamma})}{1-\alpha}.$$

Δ désigne le déterminant des quantités

$$\begin{array}{llll} l\,\varepsilon_1(\alpha), & l\,\varepsilon_2(\alpha),\ldots, & l\,\varepsilon_{\mu-1}(\alpha), \\ l\,\varepsilon_1(\alpha^\gamma), & l\,\varepsilon(\alpha^\gamma),\ldots, & l\,\varepsilon_{\mu-1}(\alpha^\gamma), \\ \ldots & \ldots & \ldots \\ l\,\varepsilon_1\left(\alpha^{\gamma^{\mu-2}}\right), & l\,\varepsilon_2\left(\alpha^{\gamma^{\mu-2}}\right),\ldots, & l\,\varepsilon_{\mu-1}\left(\alpha^{\gamma^{\mu-2}}\right), \end{array}$$

où $\varepsilon_1(\alpha)$, $\varepsilon_2(\alpha),\ldots, \varepsilon_{\mu-1}(\alpha)$ représentent un système de $\mu - 1$ unités fondamentales.

Nous terminerons ce paragraphe en faisant quelques remarques sur la formule trouvée pour le nombre H des classes des nombres complexes idéaux. D'abord nous observons que le nombre H consiste de deux facteurs entiers bien distincts, le premier égal à $\frac{P}{(2\lambda)^{\mu-1}}$, le second égal à $\frac{D}{\Delta}$. On démontre aisément que le premier de ces facteurs est un nombre entier, en faisant voir que le produit P contient $(\mu - 1)$ fois le facteur 2, et autant de fois le facteur λ; pour le second facteur, cela découle immédiatement de l'observation faite à la fin du § II de ce Mémoire. Pour le cas de $\lambda = 5$, nous avons trouvé que l'unité $e(\alpha)$ est une unité fondamentale, d'où il suit $D = \Delta$; donc on a

$$\frac{D}{\Delta} = 1, \quad \text{pour} \quad \lambda = 5.$$

Pour le cas de $\lambda = 7$, on trouve sans difficulté que $e(\alpha)$ et $e(\alpha^\gamma)$ sont encore deux unités fondamentales; donc on a de même

$$D = \Delta \quad \text{et} \quad \frac{D}{\Delta} = 1, \quad \text{pour} \quad \lambda = 7.$$

Mais si λ est plus grand, le calcul effectif de ce second facteur est très-pénible, parce qu'il exige qu'on recherche d'abord un système d'unités fondamentales. Le calcul du premier facteur $\frac{P}{(2\lambda)^{\mu-1}}$, que nous désignerons simplement comme fonction de λ par $P'(\lambda)$, n'offre pas cette difficulté; je l'ai calculé pour toutes les valeurs du nombre premier λ

de la première centaine. Voici les résultats de ce calcul :

$$\begin{aligned}
P'(3) &= 1, & P'(43) &= 211,\\
P'(5) &= 1, & P'(47) &= 695 = 5.139,\\
P'(7) &= 1, & P'(53) &= 4889,\\
P'(11) &= 1, & P'(59) &= 41241 = 3.59.233,\\
P'(13) &= 1, & P'(61) &= 76301 = 41.1861,\\
P'(17) &= 1, & P'(67) &= 853513 = 67.12739,\\
P'(19) &= 1, & P'(71) &= 5472271 = 7.7.29.3851,\\
P'(23) &= 3, & P'(73) &= 11957417 = 89.134353,\\
P'(29) &= 8, & P'(79) &= 60087849 = 5.53.377911,\\
P'(31) &= 9, & P'(83) &= 838216959 = 3.279405653,\\
P'(37) &= 37, & P'(89) &= 13379363737 = 113.118401449,\\
P'(41) &= 121, & P'(97) &= 4113228230001 = 3457.1189825 93.
\end{aligned}$$

On voit que ces nombres vont en croissant avec une rapidité extraordinaire. La loi asymptotique des valeurs de ce premier facteur du nombre des classes H est exprimée par la formule

$$P'(\lambda) = \frac{P}{(2\lambda)^{\mu-1}} = \frac{\lambda^{\frac{\lambda+3}{4}}}{2^{\frac{\lambda-3}{2}}\cdot\pi^{\frac{\lambda-1}{2}}},$$

dont je me réserve la démonstration et les développements ultérieurs à une autre occasion.

§ IX.

Deux recherches spéciales concernant le nombre des classes des nombres complexes idéaux et les unités complexes.

En examinant les valeurs du premier facteur du nombre H, données dans le paragraphe précédent, on voit que, pour les trois nombres premiers de la première centaine

$$\lambda = 37, \quad \lambda = 59 \quad \text{et} \quad \lambda = 67,$$

le nombre H est divisible par λ. Pour de telles valeurs de λ, les nombres complexes sont doués de quelques propriétés singulières, de manière que ces valeurs de λ se présentent dans plusieurs recherches générales comme cas d'exception qui exigent des méthodes particulières. C'est pour cette raison que nous nous proposons ici le problème *de trouver tous les nombres premiers* λ *pour lesquels le nombre* H *des classes des nombres complexes idéaux est divisible par* λ.

Nous commençons par discuter le premier facteur $\frac{P}{(2\lambda)^{\mu-1}}$ du nombre

$$H = \frac{P}{(2\lambda)^{\mu-1}} \cdot \frac{D}{\Delta},$$

où nous avons posé

$$P = \varphi(\beta).\varphi(\beta^3).\varphi(\beta^5)\ldots\varphi(\beta^{\lambda-2}),$$

$$\varphi(\beta) = 1 + \gamma_1\beta + \gamma_2\beta^2 + \gamma_3\beta^3 + \ldots + \gamma_{\lambda-2}\beta^{\lambda-2}.$$

En multipliant par $\gamma\beta - 1$, on a la formule

$$(\gamma\beta-1)\varphi(\beta) = (\gamma\gamma_{\lambda-2} - 1) + (\gamma - \gamma_1)\beta + (\gamma\gamma_1 - \gamma_2)\beta^2 + \ldots + (\gamma\gamma_{\lambda-3} - \gamma_{\lambda-2})\beta^{\lambda-2},$$

dans laquelle tous les coefficients sont divisibles par λ; car, en substituant

$$\gamma_{k-1} \equiv \gamma^{k-1} \quad \text{et} \quad \gamma_k \equiv \gamma^k \pmod{\lambda},$$

on a

$$\gamma\gamma_{k-1} - \gamma_k \equiv \gamma\gamma^{k-1} - \gamma^k \equiv 0 \pmod{\lambda}.$$

Donc, en posant

$$\gamma\gamma_{k-1} - \gamma_k = \lambda b_k$$

et

$$b_0 + b_1\beta + b_2\beta^2 + \ldots + b_{\lambda-2}\beta^{\lambda-2} = \psi(\beta),$$

l'équation précédente donne

$$(\gamma\beta - 1)\varphi(\beta) = \lambda\psi(\beta).$$

En changeant β en β^3, β^5,..., $\beta^{\lambda-2}$ et multipliant, on trouve

$$(\gamma\beta-1).(\gamma\beta^3-1)\ldots(\gamma\beta^{\lambda-2}-1)\,P = \lambda^\mu\psi(\beta).\psi(\beta^3)\ldots\psi(\beta^{\lambda-2}),$$

et, comme on a

$$(\gamma\beta - 1).(\gamma\beta^3 - 1).(\gamma\beta^5 - 1)\dots(\gamma\beta^{\lambda-2} - 1) = \gamma^\mu + 1,$$

cette équation devient

$$(\gamma^\mu + 1)\,P = \lambda^\mu \psi(\beta).\psi(\beta^3)\dots\psi(\beta^{\lambda-2}).$$

Le nombre $\gamma^\mu + 1$, γ étant une racine primitive et $\mu = \frac{\lambda-1}{2}$, est toujours divisible par λ, on pourra donc poser $\gamma^\mu + 1 = \lambda G$, où G est un entier ; on pourra aussi toujours choisir la racine primitive γ, telle que $\gamma^\mu + 1$ ne soit pas divisible par λ^2, c'est-à-dire que G ne soit pas divisible par λ. Cela étant, on aura

$$2^{\mu-1} G.\frac{P}{(2\lambda)^{\mu-1}} = \psi(\beta).\psi(\beta^3)\dots\psi(\beta^{\lambda-2}),$$

et, puisqu'en substituant la racine primitive γ de la congruence

$$\gamma^{\lambda-1} \equiv 1 \pmod{\lambda}$$

à la racine de l'équation

$$\beta^{\lambda-1} = 1,$$

on a évidemment

$$\psi(\beta).\psi(\beta^3)\dots\psi(\beta^{\lambda-2}) \equiv \psi(\gamma).\psi(\gamma^3)\dots\psi(\gamma^{\lambda-2}) \pmod{\lambda},$$

cette équation donne la congruence

$$2^{\mu-1} G.\frac{P}{(2\lambda)^{\mu-1}} \equiv \psi(\gamma).\psi(\gamma^3)\dots\psi(\gamma^{\lambda-2}) \pmod{\lambda}.$$

Il suit de là que le premier facteur $\frac{P}{(2\lambda)^{\mu-1}}$ du nombre des classes H sera ou ne sera pas divisible par λ, selon que parmi les facteurs du produit $\psi(\gamma).\psi(\gamma^3)\dots\psi(\gamma^{\lambda-2})$ il y en a un ou il n'y en a aucun divisible par λ. Ainsi tout se réduit à examiner si la congruence

$$\psi(\gamma^{2n-1}) = b_0 + b_1\gamma^{2n-1} + b_2\gamma^{2(2n-1)} + \dots + b_{\lambda-2}\gamma^{(\lambda-2)(2n-1)} \equiv 0 \pmod{\lambda}$$

est ou n'est pas remplie pour une quelconque des valeurs de $n = 1, 2, 3, \dots, \mu$.

En divisant par γ^{2n-1}, puis changeant les exposants $1, 2, 3, \ldots, \lambda-1$ en indice, au moyen de la congruence $\gamma^k \equiv \gamma_k \pmod{\lambda}$, on aura la congruence équivalente

$$b_0\gamma_{\gamma-1}^{2n-1} + b_1 + b_2\gamma_1^{2n-1} + b_3\gamma_2^{2n-1} + \ldots + b_{\lambda-2}\gamma_{\lambda-3}^{3n-1} \equiv 0 \pmod{\lambda}.$$

Or il suit de la définition même des coefficients $\lambda b_k = \gamma\gamma_{k-1} - \gamma_k$ qu'on a $b_k = 0$, pour toutes les valeurs de γ_{k-1} comprises entre les limites 0 et $\frac{\lambda}{\gamma}$, $b_k = 1$ pour toutes les valeurs de γ_{k-1} comprises entre les limites $\frac{\lambda}{\gamma}$ et $\frac{2\lambda}{\gamma}$, et généralement $b_k = s$ pour toutes les valeurs comprises entre les limites $\frac{s\lambda}{\gamma}$ et $\frac{(s+1)\lambda}{\gamma}$. Donc, en comprenant tous les termes de cette congruence, pour lesquels les coefficients b_k ont la même valeur, et en désignant généralement par t_s le plus grand entier contenu dans $\frac{s\lambda}{\gamma}$, on pourra la mettre sous cette forme,

$$\begin{aligned}
&1[(t_1+1)^{2n-1} + (t_1+2)^{2n-1} + \ldots + t_2^{2n-1}],\\
&+2[(t_2+1)^{2n-1} + (t_2+2)^{2n-1} + \ldots + t_3^{2n-1}],\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&+(\gamma-1)[(t_{\gamma-1}+1)^{2n-1} + (t_{\gamma-1}+2)^{2n-1} + \ldots\\
&\qquad + (\lambda-1)^{2n-1}] \equiv 0 \pmod{\lambda}.
\end{aligned}$$

Nous nous servirons ici de la fonction rationnelle et entière de la variable x,

$$\chi(x) = \frac{x^{2n}}{\Pi_{2n}} - \frac{x^{2n-1}}{2\Pi_{2n-1}} + \frac{B_1 x^{2n}}{\Pi_{2n-2}\Pi_2} - \frac{B_2 x^{2n-2}}{\Pi_{2n-4}\Pi_4} + \ldots + \frac{(-1)^n B_{n-1} x^2}{\Pi_2 \Pi_{2n-2}},$$

dans laquelle $B_1, B_2, \ldots, B_{n-1}$ désignent les nombres bernoulliens, et Π_r le produit $1.2.3\ldots r$. Dans le cas où x est un nombre entier positif, la fonction $\chi(x)$ exprime la série des puissances $(2n-1)^{ièmes}$ des nombres naturels, car on a la formule connue

$$1^{2n-1} + 2^{2n-1} + 3^{2n-1} + \ldots + (x-1)^{2n-1} = \Pi_{2n-1}\chi(x).$$

Au moyen de cette formule, la congruence proposée se représente de la manière suivante :

$$\begin{aligned}&\chi(t_2+1)-\chi(t_1+1)\\&+2[\chi(t_3+1)-\chi(t_2+1)]+3[\chi(t_4+1)-\chi(t_3+1)]+\ldots\\&+(\gamma-1)[\chi(\lambda)-\chi(t_{\gamma-1}+1)]\equiv 0 \pmod{\lambda},\end{aligned}$$

ou, plus simplement,

$$\chi(t_1+1)+\chi(t_2+1)+\chi(t_3+1)+\ldots+\chi(t_{\gamma-1}+1)\equiv 0 \pmod{\lambda}$$

Le nombre t_s étant le plus grand entier contenu dans la fraction $\frac{s\lambda}{\gamma}$, pourra être mis sous la forme

$$t_s=\frac{s\lambda-r_s}{\gamma},$$

où r_s sera un nombre positif, moindre que γ, et la congruence proposée prendra la forme

$$\begin{aligned}&\chi\left(\frac{\lambda-r_1+\gamma}{\gamma}\right)+\chi\left(\frac{2\lambda-r_2+\gamma}{\gamma}\right)+\ldots\\&\qquad+\chi\left(\frac{(\gamma-1)\lambda-r_{\gamma-1}+\gamma}{\gamma}\right)\equiv 0 \pmod{\lambda},\end{aligned}$$

d'où, en négligeant les multiples du module λ, on aura la congruence simplifiée

$$\chi\left(\frac{\gamma-r_1}{\gamma}\right)+\chi\left(\frac{\gamma-r_2}{\gamma}\right)+\ldots+\chi\left(\frac{\gamma-r_{\gamma-1}}{\gamma}\right)\equiv 0 \pmod{\lambda},$$

dans laquelle on pourra faire disparaître les fractions en multipliant par les dénominateurs, dont aucun ne contient le facteur λ. Les nombres $r_1, r_2, \ldots, r_{\gamma-1}$ coïncident avec les nombres $1, 2, 3, \ldots, \gamma-1$, pris dans un ordre convenable; car on sait qu'ils sont tous positifs, moindres que γ, et l'on démontre aisément qu'ils sont tous différents entre eux. Donc, en mettant $1, 2, \ldots, \gamma-1$, au lieu de $r_1, r_2, \ldots, r_{\gamma-1}$, on obtient la congruence

$$\chi\left(\frac{1}{\gamma}\right)+\chi\left(\frac{2}{\gamma}\right)+\chi\left(\frac{3}{\gamma}\right)+\ldots+\chi\left(\frac{\gamma-1}{\gamma}\right)\equiv 0 \pmod{\lambda}.$$

Pour obtenir l'expression la plus simple de cette congruence, nous

développerons ici une formule nouvelle, contenant une propriété curieuse de la fonction $\chi(x)$. Pour cela, nous partons du développement en série, ordonnée suivant les cosinus des multiples de $2x\pi$,

$$\chi(x) = \frac{(-1)^n B_n}{\Pi_{2n}} - \frac{(-1)^n 2}{(2\pi)^{2n}}\left(\frac{\cos 2x\pi}{1^{2n}} + \frac{\cos 4x\pi}{2^{2n}} + \frac{\cos 6x\pi}{3^{2n}} + \ldots\right),$$

dans lequel x doit être pris entre les limites o et 1. En prenant successivement $x = 0, \frac{1}{\gamma}, \frac{2}{\gamma}, \ldots, \frac{\gamma-1}{\gamma}$, et ajoutant ces équations, en observant que la série

$$1 + \cos\frac{2k\pi}{\gamma} + \cos\frac{4k\pi}{\gamma} + \ldots + \cos\frac{2(\gamma-1)k\pi}{\gamma}$$

est égale à γ, si k est un multiple de γ, et qu'elle est égale à zéro dans tous les autres cas, on obtient

$$\chi\left(\frac{1}{\gamma}\right) - \chi\left(\frac{2}{\gamma}\right) + \chi\left(\frac{3}{\gamma}\right) + \ldots + \chi\left(\frac{\gamma-1}{\gamma}\right)$$
$$= \frac{(-1)^n \gamma B_n}{\Pi_{2n}} - \frac{(-1)^n 2\gamma}{(2\pi)^{2n}}\left[\frac{1}{\gamma^{2n}} + \frac{1}{(2\gamma)^{2n}} + \frac{1}{(3\gamma)^{2n}} + \ldots\right],$$

et puisqu'on a

$$1 + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \ldots = \frac{(2\pi)^{2n} B_n}{2\Pi_{2n}},$$

l'équation précédente se réduit à

$$\chi\left(\frac{1}{\gamma}\right) + \chi\left(\frac{2}{\gamma}\right) + \ldots + \chi\left(\frac{\gamma-1}{\gamma}\right) = \frac{(-1)^n(\gamma^{2n}-1)B_n}{\gamma^{2n-1}\Pi_{2n}}.$$

A cause de cette propriété de la fonction $\chi(x)$, la congruence de laquelle dépend la divisibilité par λ du premier facteur du nombre des classes H, prend la forme

$$\frac{(\gamma^{2n}-1)B_n}{\gamma^{2n-1}\Pi_{2n}} \equiv 0 \pmod{\lambda}.$$

Le dénominateur $\gamma^{2n-1}\Pi_{2n}$ peut être rejeté, parce qu'il ne contient pas le facteur λ; de même, le facteur $\gamma^{2n}-1$, qui n'est pas divisible par λ pour les valeurs de $n = 1, 2, 3, \ldots, \mu-1$, pourra être négligé dans tous ces cas, en sorte qu'on a simplement

$$B_n \equiv 0 \pmod{\lambda}.$$

Le cas de $n = \mu$, où $\gamma^{2\mu} - 1$ est divisible par λ, en sorte que B_μ contient le facteur λ en dénominateur, exige une discussion particulière. D'après une formule connue, le nombre bernoullien B_μ s'exprime au moyen des nombres bernoulliens précédents, de la manière suivante :

$$B_\mu = \frac{\Pi_{2\mu} B_{\mu-1}}{2^2 \Pi_3 \Pi_{2\mu-2}} - \frac{\Pi_{2\mu} B_{\mu-2}}{2^4 \Pi_5 \Pi_{2\mu-4}} + \ldots + \frac{(-1)^\mu}{2^{2\mu}(2\mu+1)} + \frac{(-1)^{\mu+1}}{2^{2\mu}},$$

où l'avant-dernier terme est le seul qui contienne le facteur $2\mu + 1 = \lambda$ en dénominateur. On aura donc

$$B_\mu = \frac{(-1)^\mu}{2^{2\mu}.\lambda} + \frac{M}{N},$$

où N n'est pas divisible par λ, et en multipliant par

$$\gamma^{2\mu} - 1 = (\gamma^\mu - 1)(\gamma^\mu + 1) = (\gamma^\mu - 1)\lambda G,$$

on obtient l'équation

$$\chi\left(\frac{1}{\gamma}\right) + \chi\left(\frac{2}{\gamma}\right) \cdots \chi\left(\frac{\gamma-1}{\gamma}\right) = \frac{(-1)^\mu G(\gamma^\mu - 1)}{\gamma^{2\mu-1} \Pi_{2\mu}} \left[\frac{(-1)^\mu}{2^{2\mu}} + \frac{\lambda M}{N}\right].$$

La congruence de condition, posée ci-dessus, devient donc, dans le cas de $n = \mu$,

$$\frac{G(\gamma^\mu - 1)}{2^{2\mu} \gamma^{2\mu-1} \Pi_{2\mu}} \equiv 0 \pmod{\lambda};$$

d'où, en ayant égard à l'hypothèse que G n'est pas divisible par λ, on voit qu'elle n'est satisfaite pour aucune valeur du nombre premier λ. Ainsi la divisibilité par λ du premier facteur du nombre H dépend de ce que la congruence $B_n \equiv 0 \pmod{\lambda}$ ait lieu pour une quelconque des valeurs de $n = 1, 2, 3, \ldots, \mu - 1$. Le résultat trouvé donne le théorème :

La condition nécessaire et suffisante pour que le premier facteur $\frac{P}{(2\lambda)^{\mu-1}}$ *du nombre des classes* H *soit divisible par* λ, *consiste en ce qu'un quelconque des* $\frac{\lambda-3}{2}$ *premiers nombres bernoulliens soit divisible par* λ.

Passons à la discussion du second facteur $\frac{D}{\Delta}$ du nombre H. En vertu d'un théorème démontré dans le § II de ce Mémoire, une certaine puissance de toute unité complexe s'exprime comme produit de puissances entières du système indépendant $e(\alpha)$, $e\left(\alpha^{\gamma}\right),\ldots, e\left(\alpha^{\gamma^{\mu-2}}\right)$; nous pouvons donc poser, comme à l'endroit cité,

$$\varepsilon_1(\alpha)^{n_1} = e\left(\alpha^{\gamma}\right)^{r_1^1}.e\left(\alpha^{\gamma}\right)^{r_2^1}\ldots e\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}^1},$$

$$\varepsilon_2(\alpha)^{n_2} = e\left(\alpha\right)^{r_1^2}.e\left(\alpha^{\gamma}\right)^{r_2^2}\ldots e\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}^2},$$

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

$$\varepsilon_{\mu-1}(\alpha)^{n_{\mu-1}} = e\left(\alpha\right)^{r_1^{\mu-1}}.e\left(\alpha^{\gamma}\right)^{r_2^{\mu-1}}\ldots e\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}^{\mu-1}},$$

en supposant que $\varepsilon_1(\alpha)$, $\varepsilon_2(\alpha),\ldots, \varepsilon_{\mu-1}(\alpha)$ désignent un système d'unités fondamentales, et que l'exposant n_h n'ait aucun facteur commun avec tous les exposants $r_1^h, r_2^h,\ldots, r_{\mu-1}^h$. Nous obtiendrons de là, comme dans le § II,

$$\frac{D}{\Delta} = \frac{n_1.n_2\ldots n_{\mu-1}}{R}.$$

d'où il suit que $\frac{D}{\Delta}$ ne pourra être divisible par λ, à moins qu'un des nombres $n_1, n_2,\ldots, n_{\mu-1}$ ne soit divisible par λ, c'est-à-dire qu'on ait une équation de la forme

$$\varepsilon(\alpha)^n = e\left(\alpha\right)^{r_1}.e\left(\alpha^{\gamma}\right)^{r_2}\ldots e\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}},$$

dans laquelle n soit divisible par λ, sans que les exposants $r_1, r_2,\ldots, r_{\mu-1}$ soient tous divisibles par λ.

Or, on démontre aisément que la $\lambda^{ième}$ puissance de tout nombre complexe existant est congrue à un nombre entier non complexe pour le module λ. En effet, en élevant à la $\lambda^{ième}$ puissance le polynôme

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha_{\lambda-2},$$

et négligeant tous les termes divisibles par λ, il ne restera que les $\lambda^{èmes}$

puissances des termes du polynôme, et l'on aura généralement

$$f(\alpha)^\lambda \equiv a^\lambda + a_1^\lambda + a_2^\lambda + \ldots + a_{\lambda-2}^\lambda$$
$$\equiv a + a_1 + a_2 + \ldots + a_{\lambda-2} \pmod{\lambda}.$$

La puissance $\varepsilon(\alpha)^n$, n étant divisible par λ, sera donc congrue à un nombre entier non complexe c. En le substituant dans l'équation précédente, on aura une condition nécessaire pour que le facteur $\frac{D}{\Delta}$ soit divisible par λ, exprimée par la congruence

$$e(\alpha)^{r_1} . e(\alpha')^{r_2} \ldots e\left(\alpha^{\nu^{\mu-2}}\right)^{r_{\mu-1}} \equiv c \pmod{\lambda},$$

laquelle doit avoir lieu pour des valeurs entières des exposants $r_1, r_2, \ldots, r_{\mu-1}$, qui ne sont pas tous divisibles par λ.

La recherche des valeurs du nombre premier λ pour lesquelles cette congruence puisse avoir lieu se fait au moyen d'une méthode générale, dont le point principal consiste en ce que, dans une équation contenant des nombres complexes, on introduit une variable continue x, au lieu de la racine α. Étant donnée une équation

$$f(\alpha) = \varphi(\alpha) \quad \text{ou} \quad f(\alpha) - \varphi(\alpha) = 0.$$

qui aura lieu pour toutes les valeurs de α qui satisfont à l'équation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

la fonction rationnelle et entière de la variable x, $f(x) - \varphi(x)$ sera égale à zéro pour toutes les valeurs de $x = \alpha$, $x = \alpha^2$, .., $x = \alpha^{\lambda-1}$, d'où l'on conclut qu'elle sera divisible par

$$(x - \alpha).(x - \alpha^2)\ldots(x - \alpha^{\lambda-1}) = 1 + x + x^2 + \ldots + x^{\lambda-1};$$

on pourra donc poser

$$f(x) - \varphi(x) = (1 + x + x^2 + \ldots + x^{\lambda-1})\psi(x),$$

ou

$$f(x) = \varphi(x) + (1 + x + x^2 + \ldots + x^{\lambda-1})\psi(x),$$

$\psi(x)$ étant une fonction rationnelle et entière de la variable x.

Pour faire l'application à la congruence proposée, nous la réduirons d'abord à l'équation

$$e(\alpha)^{r_1}.e(\alpha^\gamma)^{r_2}\dots e\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}} \equiv c + \lambda\varphi(\alpha),$$

dans laquelle $\varphi(\alpha)$ désigne un nombre entier complexe. En substituant la variable x au lieu de la racine α, on aura

$$\begin{aligned} &e(x)^{r_1}.e(x^\gamma)^{r_2}\dots e\left(x^{\gamma^{\mu-2}}\right)^{r_{\mu-1}} \\ &\equiv c + \lambda\varphi(x) + (1 + x + x^2 + \dots + x^{\lambda-1})\psi(x). \end{aligned}$$

Si maintenant on prend les différentielles des logarithmes des deux membres de cette équation, et qu'après avoir multiplié par x, on restitue la valeur particulière $x = \alpha$, on en tire l'équation

$$\begin{aligned} &r_1\frac{\alpha e'(\alpha)}{e(\alpha)} + r_2\gamma\frac{\alpha^\gamma e'(\alpha^\gamma)}{e(\alpha)} + \dots + r_{\mu-1}\gamma^{\mu-2}\frac{\alpha^{\gamma^{\mu-2}} e'\left(\alpha^{\gamma^{\mu-2}}\right)}{e\left(\alpha^{\gamma^{\mu-2}}\right)} \\ &= \frac{\lambda\alpha\varphi'(\alpha) + [\alpha + 2\alpha^2 + 3\alpha^3 + \dots + (\lambda-1)\alpha^{\lambda-1}]\psi(\alpha)}{c + \lambda\varphi(\alpha)}, \end{aligned}$$

où, suivant la notation de Lagrange, $e'(x)$ et $\varphi'(x)$ désignent les premières dérivées de $e(x)$ et $\varphi(x)$. De là, en rejetant les multiples de λ, et faisant, pour abréger,

$$\frac{2e'(\alpha)}{e(\alpha)} = \mathrm{F}(\alpha),$$

on aura la congruence

$$\begin{aligned} &r_1\mathrm{F}(\alpha) + r_2\gamma\mathrm{F}(\alpha^\gamma) + \dots + r_{\mu-1}\gamma^{\mu-2}\mathrm{F}\left(\alpha^{\gamma^{\mu-2}}\right) \\ &\equiv \frac{2}{c}[\alpha + 2\alpha^2 + 3\alpha^3 + \dots + (\lambda-1)\alpha^{\lambda-1}]\psi(\alpha) \pmod{\lambda}. \end{aligned}$$

En mettant le nombre complexe $\psi(\alpha)$ sous la forme

$$\psi(\alpha) = a + (1-\alpha)\psi_1(\alpha),$$

où a est un entier non complexe, et observant qu'on a

$$(1-\alpha)[\alpha + 2\alpha^2 + 3\alpha^3 + \dots + (\lambda-1)\alpha^{\lambda-1}] = -\lambda,$$

puis faisant enfin

$$\mathrm{M} \equiv \frac{2a}{c} \pmod{\lambda},$$

on aura

$$r_1 F(\alpha) + r_2 \gamma F(\alpha^\gamma) + \ldots + r_{\mu-1} \gamma^{\mu-2} F\left(\alpha^{\gamma^{\mu-2}}\right) = M[\alpha + 2\alpha^2 + \ldots + (\lambda-1)\alpha^{\lambda-1}].$$

Développons actuellement le nombre entier complexe $F(\alpha)$. En prenant la différentielle logarithmique de l'expression

$$e(x) = \sqrt{\frac{(1-x^\gamma)(1-x^{-\gamma})}{(1-x)(1-x^{-1})}},$$

on obtient

$$\frac{2x e'(x)}{e(x)} = \frac{1+x}{1-x} - \frac{\gamma(1+x^\gamma)}{1-x^\gamma};$$

d'où, en restituant la valeur particulière $x = \alpha$,

$$F(\alpha) = \frac{1+\alpha}{1-\alpha} - \frac{\gamma(1+\alpha^\gamma)}{1-\alpha^\gamma}.$$

Le développement ultérieur se fait au moyen de l'équation

$$(1-\alpha)[\alpha + 2\alpha^2 + 3\alpha^3 + \ldots + (\lambda-1)\alpha^{\lambda-1}] = -\lambda,$$

de laquelle on tire

$$\frac{1}{1-\alpha} = -\frac{[\alpha + 2\alpha^2 + 3\alpha^3 + \ldots + (\lambda-1)\alpha^{\lambda-1}]}{\lambda},$$

et en multipliant par $1+\alpha$,

$$\frac{1+\alpha}{1-\alpha} = -\frac{[\lambda + 2\alpha + 4\alpha^2 + 6\alpha^3 + \ldots + 2(\lambda-1)\alpha^{\lambda-1}]}{\lambda}.$$

Lorsqu'on y remplace les coefficients $1, 2, 3, \ldots, \lambda-1$ par les nombres $1, \gamma_1, \gamma_2, \ldots, \gamma_{\lambda-2}$, qui, abstraction faite de l'ordre, sont absolument les mêmes, et qu'en même temps, au lieu des exposants correspondants, on met $1, \gamma, \gamma^2, \ldots, \gamma^{\lambda-2}$, cette équation prend la forme

$$\frac{1+\alpha}{1-\alpha} = -\frac{(\lambda + 2\alpha + 2\gamma_1\alpha^\gamma + 2\gamma_2\alpha^{\gamma^2} + \ldots + 2\gamma_{\lambda-2}\alpha^{\gamma^{\lambda-2}})}{\lambda}.$$

Si l'on change α en α^γ, et qu'on multiplie par γ, on aura aussi

$$\frac{\gamma(1-\alpha^\gamma)}{1-\alpha^\gamma} = -\frac{\left(\gamma + 2\gamma\gamma_{\lambda-2}\alpha + 2\gamma\alpha^\gamma + 2\gamma\gamma_1\alpha^{\gamma^2} + \ldots + 2\gamma\gamma_{\lambda-3}\alpha^{\gamma^{\lambda-3}}\right)}{\lambda};$$

enfin, en soustrayant cette équation de la précédente, on obtient le développement

$$F(\alpha) = \gamma - 1 + \frac{2(\gamma\gamma_{\lambda-2}-1)}{\lambda}\alpha + \frac{2(\gamma-\gamma_1)}{\lambda}\alpha^\gamma + \ldots + \frac{2(\gamma\gamma_{\lambda-3}-\gamma_{\lambda-2})}{\lambda}\alpha^{\gamma^{\lambda-2}},$$

dans lequel les coefficients sont les mêmes que ceux que nous avons désignés par b_k, dans la première partie de cette recherche. En adoptant les mêmes signes, nous avons

$$F(\alpha) = \gamma - 1 + 2b_0\alpha + 2b_1\alpha^\gamma + 2b_3\alpha^{\gamma^2} + \ldots + 2b_{\lambda-2}\alpha^{\gamma^{\lambda-2}}.$$

Substituons le développement trouvé de $F(\alpha)$, de même que ceux de $F(\alpha^\gamma)$, $F(\alpha^{\gamma^2})$, etc., qu'on en déduit par le changement de α en α^γ, α^{γ^2}, etc., dans la congruence proposée, dont le second membre pourra être mis dans la forme

$$M\left(\alpha + \gamma\alpha^\gamma + \gamma^2\alpha^{2\gamma^2} + \ldots + \gamma^{\lambda-2}\alpha^{\gamma^{\lambda-2}}\right).$$

Comparons séparément les coefficients des termes multipliés par α, $\alpha^\gamma, \alpha^{\gamma^2}, \ldots, \alpha^{\gamma^{\lambda-2}}$, et nous aurons ce système de congruences :

$$\left.\begin{array}{l}
r_1 b_0 + \gamma r_2 b_{\lambda-2} + \gamma^2 r_3 b_{\lambda-3} + \ldots + \gamma^{\mu-2} r_{\mu-1} b_{\lambda-\mu+1} - R \equiv M \\
r_1 b_1 + \gamma r_2 b_0 + \gamma^2 r_3 b_{\lambda-2} + \ldots + \gamma^{\mu-2} r_{\mu-1} b_{\lambda-\mu+2} - R \equiv \gamma M \\
r_1 b_2 + \gamma r_2 b_1 + \gamma^2 r_3 b_0 + \ldots + \gamma^{\mu-2} r_{\mu-1} b_{\lambda-\mu+3} - R \equiv \gamma^2 M \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_1 b_{\lambda-2} + \gamma r_2 b_{\lambda-2} + \gamma^2 r_3 b_{\lambda-4} + \ldots + \gamma^{\mu-2} r_{\mu-1} b_{\lambda-\mu} - R \equiv \gamma^{\lambda-2} M
\end{array}\right\} \pmod{\lambda},$$

où nous avons fait, pour abréger,

$$r_1 + \gamma r_2 + \gamma^2 r_3 + \ldots + \gamma^{\mu-2} r_{\mu-1} = R.$$

Ces congruences, multipliées respectivement par $1, \gamma^{2n-1}, \gamma^{2(2n-1)}, \ldots, \gamma^{(\lambda-2)(2n-1)}$, et ajoutées, donnent une somme qu'on décompose aisément en deux facteurs

$$\left(\begin{matrix} r_1 + \gamma^{2n} r_2 + \gamma^{4n} r_3 + \ldots \\ + \gamma^{2(\mu-2)n} r_{\mu-1} \end{matrix}\right) \cdot \left(\begin{matrix} b_0 + b_1 \gamma^{2n-1} + b_2 \gamma^{2(2n-1)} + \ldots \\ + b_{\lambda-2} \gamma^{(\lambda-2)(2n-1)} \end{matrix}\right) \equiv 0,$$

pour le module λ et pour les valeurs de $n = 1, 2, 3, \ldots, \mu - 1$. Il suit de cette congruence, que dans les cas où le second facteur

$$b_0 + b_1 \gamma^{2n-1} + b_2 \gamma^{2(2n-1)} + \ldots + b_{\lambda-2} \gamma^{(\lambda-2)(2n-1)}$$

n'est divisible par λ pour aucune des valeurs de $n = 1, 2, 3, \ldots, \mu - 1$, le premier facteur sera nécessairement congru à zéro pour toutes ces valeurs de n. Dans ce cas, on aura le système des congruences :

$$\left.\begin{aligned} & r_1 + \gamma^2 r_2 + \gamma^4 r_3 + \ldots + \gamma^{2(\mu-2)} r_{\mu-1} \equiv 0, \\ & r_1 + \gamma^4 r_2 + \gamma^8 r_3 + \ldots + \gamma^{4(\mu-2)} r_{\mu-1} \equiv 0, \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & r_1 + \gamma^{2(\mu-1)} r_2 + \gamma^{4(\mu-1)} r_3 + \ldots + \gamma^{(\mu-2)(\mu-1)} r_{\mu-1} \equiv 0, \end{aligned}\right\} \pmod{\lambda}.$$

Le déterminant de ce système de congruences linéaires n'est pas congru à zéro, car on sait qu'il est composé de facteurs de la forme $\gamma^{2k} - \gamma^{2h}$, où k et h sont différents entre eux et moindres que $\mu - 1$. Par cette raison, il n'y a pas d'autres valeurs des inconnues de ce système, que

$$r_1 \equiv 0, \quad r_2 \equiv 0, \quad r_3 \equiv 0, \ldots, \quad r_{\mu-1} \equiv 0 \pmod{\lambda},$$

et puisque ces exposants ne doivent pas être tous divisibles par λ, on en conclut que, dans le cas où

$$b_0 + b_1 \gamma^{2n-1} + b_2 \gamma^{2(2n-1)} + \ldots + b_{\lambda-2} \gamma^{(\lambda-2)(2n-1)}$$

n'est divisible par λ pour aucune des valeurs $n = 1, 2, 3, \ldots, \mu - 1$, le second facteur $\frac{D}{\Delta}$ du nombre des classes H ne sera pas divisible par λ. La condition

$$b_0 + b_1 \gamma^{2n-1} + b_2 \gamma^{2(2n-1)} + \ldots + b_{\lambda-2} \gamma^{(\lambda-2)(2n-1)} \equiv 0 \pmod{\lambda}.$$

nécessaire pour que le facteur $\frac{D}{\Delta}$ soit divisible par λ, étant la même que nous avons trouvée comme condition nécessaire et suffisante pour que le premier facteur $\frac{P}{(2\lambda)^{\mu-1}}$ soit divisible par λ, on voit que le second facteur du nombre des classes H ne sera jamais divisible par λ, à moins que le premier facteur ne le soit en même temps. Nous voilà donc arrivés au résultat suivant :

Pour que le nombre H *des classes diverses des nombres complexes idéaux soit divisible par* λ, *il faut et il suffit que le nombre premier* λ *soit facteur du numérateur d'un quelconque des* $\frac{\lambda-3}{2}$ *premiers nombres bernoulliens.*

Nous passons au second problème de ce paragraphe, qui consiste dans la recherche des valeurs du nombre premier λ pour lesquelles une unité complexe puisse être congrue à un nombre entier non complexe, sans être une puissance du degré λ.

Soit $E(\alpha)$ une unité complexe qui satisfasse à la condition

$$E(\alpha) \equiv c \pmod{\lambda},$$

où c est un entier non complexe. Cette unité, exprimée par le système des unités indépendantes

$$e(\alpha), \quad e\left(\alpha^{\gamma}\right), \ldots, \quad e\left(\alpha^{\gamma^{\mu-2}}\right),$$

prendra la forme

$$E(\alpha) = \pm \alpha^{k} e(\alpha)^{\frac{r_1}{n}} . e\left(\alpha^{\gamma}\right)^{\frac{r_2}{n}} \ldots e\left(\alpha^{\gamma^{\mu-2}}\right)^{\frac{r_{\mu-1}}{n}},$$

où les exposants rationnels $\frac{r_1}{n}, \frac{r_2}{n}, \ldots, \frac{r_{\mu-1}}{n}$ sont réduits au même dénominateur le plus petit possible, en sorte qu'il n'y ait pas de facteur commun de tous les numérateurs avec le dénominateur n. En changeant α en α^{-1} dans la congruence posée, on a aussi

$$E(\alpha^{-1}) \equiv c \pmod{\lambda},$$

d'où

$$E(\alpha) \equiv E(\alpha^{-1}) \pmod{\lambda},$$

et, par conséquent,

$$\alpha^k = \alpha^{-k}, \quad \alpha^k = 1, \quad k \equiv 0 \pmod{\lambda}.$$

En substituant cette valeur de $\alpha^k = 1$, élevant à la puissance n et prenant $E(\alpha) \equiv c$, on aura

$$\pm c^n \equiv e(\alpha)^{r_1} \cdot e\left(\alpha^{\gamma}\right)^{r_2} \ldots e\left(\alpha^{\gamma^{\mu-2}}\right)^{r_{\mu-1}} \pmod{\lambda}.$$

Voilà la même congruence que nous avons discutée dans la recherche précédente. Nous y avons trouvé qu'à l'exception des cas où λ se trouve comme facteur du numérateur d'un des $\frac{\lambda-3}{2}$ premiers nombres bernoulliens, cette congruence exige nécessairement que tous les exposants soient divisibles par λ. Alors $E(\alpha)^n$ sera égal à une puissance du degré λ; on pourra donc poser

$$E(\alpha)^n = F(\alpha)^{\lambda},$$

et comme tous les nombres $r_1, r_2, \ldots, r_{\mu-1}$ n'ont aucun facteur commun avec n, cet exposant n ne sera pas divisible par λ. Par cette raison, on pourra toujours trouver deux nombres entiers s et t, tels qu'on ait

$$ns - \lambda t = 1 \quad \text{ou} \quad ns = \lambda t + 1,$$

et, en élevant l'équation précédente à la puissance s, on aura

$$E(\alpha)^{ns} = E(\alpha)^{\lambda t + 1} = F(\alpha)^{\lambda s},$$

d'où, en divisant par $E(\alpha)^{\lambda t}$,

$$E(\alpha) = \left[\frac{F(\alpha)^s}{E(\alpha)^t}\right]^{\lambda}.$$

Ainsi $E(\alpha)$ est une $\lambda^{ième}$ puissance, et nous avons le théorème :

Si le nombre premier λ n'est contenu dans aucun des $\frac{\lambda-3}{2}$ premiers nombres bernoulliens comme facteur du numérateur, toute unité complexe, congrue à un nombre complexe pour le module λ, sera une $\lambda^{ième}$ puissance d'une autre unité complexe.

§ X.

Application à la démonstration du dernier théorème de Fermat.

Dans tout ce qui précède, la théorie des nombres complexes est avancée à un point où la démonstration du fameux théorème de Fermat se fait avec facilité pour toutes les puissances dont les exposants satisfont à la condition qui se trouve dans les théorèmes du paragraphe précédent : que le nombre λ ne soit pas contenu comme facteur dans un des premiers $\frac{\lambda-3}{2}$ nombres bernoulliens. Comme la démonstration pour les nombres complexes est aussi facile que pour les nombres entiers non complexes, nous supposerons que, dans l'équation

$$u^\lambda + v^\lambda + w^\lambda = 0,$$

u, v, w soient des nombres complexes existants de la forme

$$a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-2}\alpha^{\lambda-2},$$

sans aucun facteur commun deux à deux. Nous supposerons aussi que λ soit un nombre premier qui ne se trouve pas comme facteur du numérateur d'un des $\frac{\lambda-3}{2}$ premiers nombres bernoulliens.

Cela posé, nous savons qu'en vertu d'un théorème du paragraphe précédent, le nombre H des classes des nombres complexes idéaux n'est pas divisible par λ. De plus, nous avons trouvé dans le § VI, qu'en supposant $f(\alpha)$ idéal, $f(\alpha)^\lambda$ ne pourra être existant à moins que λ et H n'aient un facteur commun différent de l'unité, ce qui n'a pas lieu. Donc, si λ est un nombre tel que nous l'avons supposé, *la $\lambda^{ième}$ puissance d'un nombre complexe idéal ne sera pas égale à un nombre complexe existant, et de ce que $f(\alpha)^\lambda$ est un nombre complexe existant, il suivra nécessairement que $f(\alpha)$ est un nombre existant.*

Rappelons encore expressément le théorème démontré à la fin du paragraphe précédent, que pour les valeurs de λ, que nous considérons ici, *chaque unité complexe qui est congrue à un nombre non complexe pour le module λ est égale à une $\lambda^{ième}$ puissance d'une autre unité.*

La démonstration de l'impossibilité de l'équation proposée consistera en deux parties distinctes, dont la première traitera le cas où aucun des trois nombres u, v, w n'est divisible par $1-\alpha$, l'autre le cas où un de ces nombres aura le facteur $1-\alpha$.

Soit donc proposée en premier lieu l'équation

$$u^\lambda + v^\lambda + w^\lambda = 0,$$

dans laquelle aucun des trois nombres complexes u, v, w ne soit divisible par $1-\alpha$. Observons d'abord que les nombres u, v, w pourront être multipliés par des unités simples de la forme α^k sans que l'équation proposée change de forme. En posant donc $\alpha^k u$ au lieu de u, on pourra toujours déterminer le nombre k tel, que $\alpha^k u$ prenne la forme

$$a + (1-\alpha)^2 \mathrm{P},$$

dans laquelle a est un entier non complexe et P un entier complexe. En effet, le nombre complexe u, ordonné suivant les puissances $1-\alpha$, prendra la forme

$$u = \mathrm{A} + \mathrm{A}_1(1-\alpha) + \mathrm{A}_2(1-\alpha)^2 + \ldots + \mathrm{A}_{\lambda-2}\alpha^{\lambda-2};$$

de même, en prenant

$$\alpha = 1 - (1-\alpha),$$

on aura

$$\alpha^k = 1 - k(1-\alpha) + \frac{k(k-1)}{1.2}(1-\alpha)^2 - \ldots,$$

d'où, en multipliant et comprenant dans un seul tous les termes multipliés par $(1-\alpha)^2$,

$$\alpha^k u = \mathrm{A} + (\mathrm{A}_1 - \mathrm{A}k)(1-\alpha) + (1-\alpha)^2 \mathrm{P}.$$

Enfin, en prenant le nombre k tel qu'on ait

$$\mathrm{A}k \equiv \mathrm{A}_1 \pmod{\lambda},$$

ce qui est toujours possible, puisque A n'est pas divisible par λ, on voit que $\alpha^k u$ prend la forme proposée. En opérant de même sur les

nombres v et w, on pourra mettre

$$u = a + (1-\alpha)^2 P,$$
$$v = b + (1-\alpha)^2 Q,$$
$$w = c + (1-\alpha)^2 R,$$

où les nombres a, b, c ne sont pas divisibles par λ, à cause de la supposition que u, v, w ne sont pas divisibles par $1-\alpha$.

Maintenant, en décomposant la forme $u^\lambda + v^\lambda$, on obtient l'équation

$$(u+v).(u+\alpha v).(u+\alpha^2 v)\ldots(u+\alpha^{\lambda-1} v) = -w^\lambda,$$

et je dis que deux quelconques de ces facteurs sont premiers entre eux. En effet, si $u+\alpha^r v$ et $u+\alpha^s v$ avaient un facteur commun, il est clair que $(\alpha^r-\alpha^s)u$ et $(\alpha^r-\alpha^s)v$ auraient le même facteur commun, et comme u et v sont premiers entre eux et $\alpha^r-\alpha^s$, ou, ce qui est au fond le même, $1-\alpha$ ne peut diviser un de ces facteurs sans diviser également le nombre w, on voit que ces facteurs sont premiers entre eux.

Cela étant, mettons à profit le théorème démontré à la fin du § V, que lorsqu'une puissance d'un nombre complexe est décomposée en facteurs premiers entre eux, ces facteurs doivent être séparément des puissances semblables multipliées par des unités complexes. Nous en concluons qu'on doit avoir généralement pour toutes les valeurs de $r = 0, 1, 2, \ldots, \lambda-1$,

$$u + \alpha^r v = \alpha^\rho E_r(\alpha)\, t_r^\lambda,$$

t_r étant un nombre complexe, facteur de w, et $\alpha^\rho E_r(\alpha)$ une unité complexe quelconque, dans laquelle $E_r(\alpha)$ soit égal à $E_r(\alpha^{-1})$. On se rappellera que toute unité complexe consiste de deux facteurs tels que nous venons de les établir. Dans cette équation, t_r^λ est donné comme nombre complexe existant; d'où nous concluons que t_r sera aussi un nombre existant; la $\lambda^{ième}$ puissance t_r^λ sera donc congrue à un nombre entier non complexe pour le module λ, et l'on aura la congruence

$$u + \alpha^r v \equiv \alpha^\rho E_r(\alpha).m \pmod{\lambda}.$$

En désignant par u', v', w' les nombres complexes réciproques de u, v, w, qu'on en déduit en changeant α en α^{-1}, on aura de même

$$u' + \alpha^{-r} v' \equiv \alpha^{-\rho} \mathrm{E}_r(\alpha) . m \pmod{\lambda};$$

d'où, en éliminant $\mathrm{E}_r(\alpha) . m$,

$$\alpha^{-\rho}(u + \alpha^r v) \equiv \alpha^{\rho}(u' + \alpha^{-r} v') \pmod{\lambda}.$$

Cette congruence, prise par rapport au module $(1 - \alpha)^2$, diviseur du module λ, donne

$$\alpha^{-\rho}(a + \alpha^r b) \equiv \alpha^{\rho}(a + \alpha^{-r} b) \quad [\mathrm{mod.}\ (1 - \alpha)^2],$$

car on a, en vertu des expressions de u, v, w données ci-dessus,

$$u \equiv a, \quad v \equiv b, \quad u' \equiv a, \quad v' \equiv b \quad [\mathrm{mod.}\ (1 - \alpha)^2]:$$

et, comme on a généralement

$$\alpha^h \equiv 1 - h(1 - \alpha) \quad [\mathrm{mod.}\ (1 - \alpha)^2],$$

cette congruence donne

$$(\alpha + b)\rho \equiv br \quad [\mathrm{mod.}\ (1 - \alpha)].$$

Or on sait qu'un nombre entier non complexe divisible par $1 - \alpha$ sera toujours divisible par λ; d'où il suit que deux entiers non complexes congrus pour le module $1 - \alpha$ seront aussi congrus pour le module λ. On aura donc

$$(a + b)\rho \equiv br \pmod{\lambda},$$

ce qui fait voir que $a + b$ n'est pas divisible par λ. En déterminant le nombre k par la congruence

$$(a + b)k \equiv b \pmod{\lambda},$$

on aura

$$\rho \equiv kr \pmod{\lambda},$$

et, en substituant cette valeur de ρ dans la congruence plus générale donnée ci-dessus, on obtient la congruence

$$\alpha^{-kr}(u + \alpha^r v) \equiv \alpha^{kr}(u' + \alpha^{-r} v') \pmod{\lambda},$$

qui subsiste pour toutes les valeurs de $r = 0, 1, 2, \ldots, \lambda - 1$. Lors-

qu'on y prend $r = 0$, on trouve

$$u + v \equiv u' + v' \pmod{\lambda},$$

et, puisque les lettres u, v, w, et en même temps les lettres u', v', w' peuvent être échangées entre elles, on aura aussi

$$\left.\begin{aligned} u + w &\equiv u' + w' \\ v + w &\equiv v' + w' \end{aligned}\right\} \pmod{\lambda};$$

enfin, de ces trois congruences, on déduit les congruences plus simples

$$\left.\begin{aligned} u &\equiv u' \\ v &\equiv v' \\ w &\equiv w' \end{aligned}\right\} \pmod{\lambda}.$$

En substituant ces valeurs congrues de u, v, w, au lieu de u', v', w', on aura

$$\alpha^{-kr}(u + \alpha^r v) \equiv \alpha^{kr}(u + \alpha^{-r} v) \pmod{\lambda},$$

ou, ce qui est le même

$$(\alpha^{-kr} - \alpha^{kr})\, u + [\alpha^{-(k-1)r} - \alpha^{(k-r)r}]\, v \equiv 0 \pmod{\lambda}.$$

Maintenant, si l'on prend les deux valeurs déterminées $r = 1$ et $r = 2$, on aura

$$\left.\begin{aligned} (\alpha^{-k} - \alpha^{k})\, u + [\alpha^{-(k-1)} - \alpha^{k-1}]\, v &\equiv 0 \\ (\alpha^{-2k} - \alpha^{2k})\, u + [\alpha^{-2(k-1)} - \alpha^{2(k-1)}]\, v &\equiv 0 \end{aligned}\right\} \pmod{\lambda};$$

d'où, en multipliant la première par $\alpha^{-k} + \alpha^{k}$, soustrayant la seconde et divisant par v, qui est premier par rapport au module, on obtient la congruence

$$(\alpha^{-k} + \alpha^{k})[\alpha^{-k(k-1)} - \alpha^{k-1}] - [\alpha^{-2(k-1)} - \alpha^{2(k-1)}] \equiv 0 \pmod{\lambda},$$

qu'on peut mettre sous la forme

$$(\alpha^{k-1} - \alpha^{-k+1})(\alpha^{-k} - \alpha^{k-1})(\alpha - 1) \equiv 0 \pmod{\lambda}.$$

Maintenant, si aucun de ces trois facteurs n'est égal à zéro, leur produit contient le facteur $1 - \alpha$ trois fois; mais, pour être divisible par λ, il fallait qu'il contînt ce facteur $(\lambda - 1)$ fois. Donc, excepté le

seul cas $\lambda = 3$, que nous excluons de notre discussion, cette congruence ne peut subsister, à moins que des deux facteurs $\alpha^{k-1} - \alpha^{-k+1}$ et $\alpha^{-k} - \alpha^{k-1}$, l'un ou l'autre soit égal à zéro, ce qui revient à

$$k \equiv 1 \quad \text{ou} \quad 2k \equiv 1 \pmod{\lambda}.$$

Le premier de ces deux cas ne peut avoir lieu; car, d'après la congruence $(a+b)k \equiv b$, il s'ensuivrait

$$a \equiv 0 \pmod{\lambda},$$

ce qui est contre l'hypothèse. Le second cas $2k \equiv 1$ donne, en vertu de la même congruence,

$$a \equiv b \pmod{\lambda},$$

comme conséquence nécessaire de l'équation

$$u^\lambda + v^\lambda + w^\lambda = 0,$$

en supposant qu'aucun des trois nombres u, v, w ne soit divisible par $1 - \alpha$. En échangeant les nombres u, v, w, ce qui change les nombres a, b, c en même temps, on obtient

$$a \equiv c \quad \text{et} \quad b \equiv c \pmod{\lambda}.$$

Or, en développant la $\lambda^{ième}$ puissance du binôme

$$u = a + (1-\alpha)^2 \mathrm{P},$$

et en négligeant tous les termes divisibles par λ, on obtient

$$u^\lambda \equiv a^\lambda \equiv a \pmod{\lambda}.$$

De la même manière, on aura aussi

$$\left.\begin{aligned} v^\lambda &\equiv b^\lambda \equiv b \\ w^\lambda &\equiv c^\lambda \equiv c \end{aligned}\right\} \pmod{\lambda};$$

et, en ajoutant,

$$u^\lambda + v^\lambda + w^\lambda \equiv a + b + c \pmod{\lambda}.$$

Il faut donc qu'on ait

$$a + b + c \equiv 0 \pmod{\lambda};$$

et, comme ces trois nombres a, b, c sont congrus entre eux, on aura

enfin les congruences

$$3a \equiv 0, \quad 3b \equiv 0, \quad 3c \equiv 0 \pmod{\lambda},$$

qui ne peuvent subsister que dans le seul cas $\lambda = 3$.

Donc l'équation proposée

$$u^\lambda + v^\lambda + w^\lambda = 0$$

ne peut être satisfaite par des nombres complexes u, v, w dont aucun n'a le facteur $1 - \alpha$.

Passons maintenant à la seconde partie de notre démonstration, dans laquelle nous supposons qu'un des trois nombres u, v, w soit divisible par $1 - \alpha$. Soit w ce nombre divisible par $1 - \alpha$, qui pourra contenir ce facteur plusieurs fois, et mettons $(1 - \alpha)^m w$ au lieu de w, en sorte que l'équation proposée soit

$$u^\lambda + v^\lambda + (1 - \alpha)^{m\lambda} w^\lambda = 0.$$

Mais nous préférons discuter l'équation plus générale

$$u^\lambda + v^\lambda = E(\alpha)(1 - \alpha)^{m\lambda} w^\lambda,$$

dans laquelle les nombres complexes u, v, w, premiers entre eux, ne sont pas divisibles par $1 - \alpha$, et où $E(\alpha)$ désigne une unité complexe quelconque.

En décomposant l'expression $u^\lambda + v^\lambda$, on a

$$(u + v).(u + \alpha v).(u + \alpha^2 v)\ldots(u + \alpha^{\lambda-1} v) = E(\alpha)(1 - \alpha)^{m\lambda} w^\lambda.$$

Ici les facteurs de ce produit ont tous le facteur commun $1 - \alpha$; car, en faisant, comme ci-dessus,

$$u = a + (1 - \alpha)^2 P,$$
$$v = b + (1 - \alpha)^2 Q,$$

on aura

$$u + \alpha^r v \equiv a + b - rb(1 - \alpha) \quad [\text{mod. } (1 - \alpha)^2] :$$

et comme le facteur $u + \alpha^r v$ doit être divisible par $1 - \alpha$, pour une certaine valeur de r du moins, on voit que $a + b$ doit être divisible

par $1-\alpha$, et conséquemment par λ. Cette congruence devient donc

$$u+\alpha^r v \equiv -rb(1-\alpha) \quad [\text{mod. } (1-\alpha)^2];$$

d'où l'on voit que tous ces facteurs ont le facteur commun $1-\alpha$, et qu'ils ne le contiennent qu'une seule fois, excepté le cas de $r=0$, où l'on a

$$u+v \equiv 0 \quad [\text{mod. } (1-\alpha)^2].$$

Cela étant, il suit immédiatement de l'équation précédente, que $u+v$ contient $(m\lambda-\lambda+1)$ fois précisément le facteur $(1-\alpha)$; on pourra donc poser

$$u+v=(1-\alpha)^{m\lambda-\lambda+1}.\varphi$$

et

$$u+\alpha^r v=(1-\alpha^r)\varphi_r,$$

et, en substituant ces expressions dans l'équation où $u^\lambda+v^\lambda$ est décomposé en λ facteurs, on aura

$$\varphi.\varphi_1.\varphi_2\cdots\varphi_{\lambda-1}=\mathrm{E}(\alpha)w^\lambda.$$

Les nombres complexes $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{\lambda-1}$ sont premiers entre eux; car tout facteur commun de φ_r et φ_s, ou de $u+\alpha^r v$ et $u+\alpha^s v$, diviserait également les nombres $(\alpha^r-\alpha^s)u$ et $(\alpha^r-\alpha^s)v$, dont le plus grand diviseur commun est $1-\alpha$. De là on conclut, par la même raison que dans la première partie de notre démonstration, que les facteurs $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{\lambda-1}$, premiers entre eux, dont le produit est égal à une $\lambda^{ième}$ puissance multipliée par une unité, seront séparément des puissances du degré λ multipliées par des unités. Donc on peut poser

$$\varphi=e_0(\alpha)w_1^\lambda,$$

$$\varphi_r=e_r(\alpha)t_r^\lambda,$$

ce qui donne

$$u+v=e_0(\alpha)(1-\alpha)^{m\lambda-\lambda+1}.w_1^\lambda,$$

$$u+\alpha^k v=e_r(\alpha)(1-\alpha^r)t_r^\lambda,$$

pour toutes les valeurs de $r = 1, 2, 3, \ldots, (\lambda - 1)$. En changeant la valeur de r en s, on aura aussi

$$u + \alpha^s v = e_s(\alpha)(1 - \alpha^s) t_s^\lambda,$$

et, en éliminant u et v de ces trois équations, on trouve

$$t_r^\lambda - \frac{e_s(\alpha)}{e_r(\alpha)} t_s^\lambda = \frac{e_0(\alpha)(\alpha^r - \alpha^s)(1-\alpha)}{e_r(\alpha)(1-\alpha^r)(1-\alpha^s)} (1-\alpha)^{(m-1)\lambda} . w_1^\lambda;$$

lorsqu'on y fait, pour abréger,

$$\frac{e_s(\alpha)}{e_r(\alpha)} = -\varepsilon(\alpha),$$

$$\frac{e_0(\alpha)(\alpha^r - \alpha^s)(1-\alpha)}{e_r(\alpha)(1-\alpha^r)(1-\alpha^s)} = \mathrm{E}_1(\alpha),$$

où $\varepsilon(\alpha)$ et $\mathrm{E}_1(\alpha)$ sont aussi unités complexes, on aura

$$t_r^\lambda + \varepsilon(\alpha) t_s^\lambda = \mathrm{E}_1(\alpha)(1-\alpha^s)^{(m-1)\lambda} w_1^\lambda.$$

Les nombres complexes t_r, t_s et w_1, dont les $\lambda^{ièmes}$ puissances sont données comme nombres complexes existants, doivent être nombres existants eux-mêmes; les $\lambda^{ièmes}$ puissances de ces nombres existants seront donc congrues à des entiers non complexes pour le module λ, et l'on aura

$$t_r^\lambda \equiv k, \quad t_s^\lambda \equiv k' \pmod{\lambda},$$

et, comme la puissance $(1-\alpha)^{(m-1)\lambda}$ est divisible par λ, si le nombre entier m est plus grand que l'unité, cette équation donne la congruence

$$k + \varepsilon(\alpha) k' \equiv 0 \pmod{\lambda}.$$

En déterminant le nombre c par la congruence

$$k + ck' \equiv 0 \pmod{\lambda},$$

on aura

$$\varepsilon(\alpha) \equiv c \pmod{\lambda},$$

et l'unité $\varepsilon(\alpha)$, congrue à un nombre entier non complexe pour le module λ, doit être égale à une $\lambda^{ième}$ puissance d'une autre unité. Donc,

en posant

$$\varepsilon(\alpha) = \varepsilon_1(\alpha)^\lambda, \quad \varepsilon_1(\alpha)\, t_s = v_1 \quad \text{et} \quad t_r = u_1,$$

l'équation précédente devient

$$u_1^\lambda + v_1^\lambda = \mathrm{E}_1(\alpha)\,(1-\alpha)^{(m-1)\lambda} w_1.$$

Voilà une équation qui ne diffère de l'équation proposée, dont elle dérive, qu'en ce que le nombre m est diminué d'une unité. En appliquant la même méthode à la nouvelle équation, on obtiendra une équation entièrement semblable, dans laquelle le nombre m sera diminué de deux unités; et, en continuant cette réduction, on parviendra nécessairement à une équation semblable, dans laquelle m est réduit à la valeur $m = 1$. La même méthode de réduction, dans laquelle m était supposé plus grand que l'unité, n'est plus applicable à l'équation

$$u^\lambda + v^\lambda = \mathrm{E}(\alpha)\,(1-\alpha)^r w^r,$$

mais il est facile de démontrer que cette équation ne peut jamais avoir lieu. Pour cela, il suffit de démontrer que *la forme* $u^\lambda + v^\lambda$, *étant divisible par* $1-\alpha$, *doit nécessairement contenir ce facteur* $(\lambda+1)$ *fois au moins.*

En effet, en prenant, comme ci-dessus,

$$u = a + (1-\alpha)^2 \mathrm{P}, \quad v = b + (1-\alpha)^2 \mathrm{Q},$$

on aura

$$u + \alpha^r v \equiv a + b - rb(1-\alpha) \quad [\text{mod. } (1-\alpha)^2],$$

et comme, pour une certaine valeur de r, le facteur $u + \alpha^r v$ de la forme $v^\lambda + v^\lambda$ doit être divisible par $1-\alpha$, on aura nécessairement $a+b$ divisible par $1-\alpha$, et conséquemment divisible par λ, ce qui donne

$$u + \alpha^r v \equiv -rb(1-\alpha) \quad [\text{mod. } (1-\alpha)^2],$$

et, pour le cas $r = 0$,

$$u + v \equiv 0 \quad [\text{mod. } (1-\alpha)^2].$$

On voit donc que tous les facteurs du produit

$$u^\lambda + v^\lambda = (u+v).(u+\alpha v).(u+\alpha^2 v)\ldots(u+\alpha^{\lambda-1} v)$$

sont divisibles par $1-\alpha$, et que le premier facteur $u+v$ est divisible par $(1-\alpha)^2$. Ainsi le nombre des facteurs $1-\alpha$ contenus dans la forme $u^\lambda + v^\lambda$ sera égal à $\lambda + 1$ au moins.

Il suit de là que l'équation

$$u^\lambda + v^\lambda = E(\alpha).(1-\alpha)^\lambda w^\lambda,$$

dans laquelle la forme $u^\lambda + v^\lambda$, divisible par $(1-\alpha)^\lambda$, n'est pas divisible par $(1-\alpha)^{\lambda+1}$, ne pourra jamais subsister, et nous en concluons que l'équation

$$u^\lambda + v^\lambda = E(\alpha).(1-\alpha)^{m\lambda}.w^\lambda$$

dont elle dérive est aussi impossible.

Le théorème de Fermat, en tant qu'il est rigoureusement démontré dans ce qui précède, pourra donc s'énoncer comme il suit :

Si λ est un nombre premier, qui n'est contenu dans aucun des $\frac{\lambda-3}{2}$ premiers nombres bernoulliens comme facteur du numérateur, l'équation

$$u^\lambda + v^\lambda + w^\lambda = 0$$

ne peut avoir lieu, ni pour des valeurs entières non complexes des nombres u, v, w, ni pour des valeurs complexes de ces nombres formées avec les racines de l'équation $\alpha^\lambda = 1$.

D'après les valeurs calculées du premier facteur du nombre des classes H, que nous avons données à la fin du § VIII de ce Mémoire, dans la première centaine, il n'y a que les trois nombres premiers $\lambda = 37$, $\lambda = 59$ et $\lambda = 67$, qui sont exceptés de notre démonstration, parce qu'ils se trouvent respectivement comme facteurs du seizième, du vingt-deuxième et du vingt-neuvième nombre bernoullien. Pour de telles puissances qui se présentent comme cas exceptionnels de notre démonstration, il reste encore à démontrer que le théorème de Fermat a lieu en vérité, ou à trouver les solutions de l'équation

$$u^\lambda + v^\lambda + w^\lambda = 0.$$