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

G. ZOLOTAREFF

Sur la théorie des nombres complexes

Journal de mathématiques pures et appliquées 3^e série, tome 6 (1880), p. 51-84.
<http://www.numdam.org/item?id=JMPA_1880_3_6__51_0>

Sur la théorie des nombres complexes;

PAR M. G. ZOLOTAREFF.

Dans le Mémoire *Sur la méthode d'intégration de M. Tchebychef* (1), j'ai donné la démonstration des théorèmes énoncés par ce géomètre pour l'intégration de la différentielle

$$\frac{(x+\mathrm{A})\,dx}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}},$$

α, β, γ, δ étant des nombres rationnels. Depuis, en me fondant sur la théorie des nombres complexes, je suis parvenu à résoudre la même question dans le cas où α, β, γ, δ ont des valeurs réelles quelconques. Dans le Mémoire qu'on va lire, j'expose cette théorie des nombres complexes qui dépendent des racines de l'équation quelconque irréductible à coefficients entiers. Avant d'aborder cette théorie, je crois devoir signaler ici deux Mémoires qui ont pour sujet la généralisation de la théorie connue de M. Kummer. L'un d'eux appartient à M. Selling (2) et l'autre à M. Dedekind (3).

(1) *Mathematische Annalen*, Band V, série 560; *Journal de Mathématiques*, 2e série, t. XIX; 1874.

(2) *Zeitschrift für Mathematik und Physik*, 1865.

(3) LEJEUNE-DIRICHLET, *Zahlen Theorie*, zweite Auflage, 1871.

Mais, si je ne me trompe, jusqu'ici il n'y a pas de théorie des nombres complexes pour le cas des équations quelconques aussi satisfaisante que la théorie de M. Kummer pour le cas des équations binômes.

1. Soient

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

une équation irréductible de degré quelconque n à coefficients entiers, et $x_0, x_1, \ldots, x_{n-1}$ ses n racines.

Nous nommerons nombre complexe entier par rapport à l'équation (1) toute fonction entière à coefficients entiers d'une racine de cette équation. Il est clair que tous ces nombres peuvent être présentés sous la forme

$$\varphi(x_0) = b_0 + b_1 x_0 + \ldots + b_{n-1} x_0^{n-1},$$

$b_0, b_1, \ldots, b_{n-1}$ étant des nombres entiers ordinaires.

Dans la suite, nous donnerons une définition des nombres complexes plus générale, mais à présent nous nous bornons à la définition donnée ci-dessus.

Soient

$$\varphi(x_0),\ \psi(x_0),\ \chi(x_0),\ \ldots$$

des nombres complexes donnés. D'abord je vais faire voir comment on peut reconnaitre, sans effectuer les multiplications, si le produit

$$\varphi(x_0)\psi(x_0)\chi(x_0)\ldots$$

est divisible par un nombre premier p non complexe. Dans ce but, je décompose la fonction $F(x)$ en facteurs irréductibles (1) suivant le module p. Soit

$$(2) \qquad F(x) \equiv V^m V_1^{m_1} \ldots V_h^{m_h} \pmod{p},$$

(1) *Gauss Werke*, II Band, série 212. — SERRET, *Cours d'Algèbre supérieure*, t. II, chap. III.

$V, V_1, \ldots, V_h$ étant des fonctions irréductibles suivant le module p. Maintenant, si le nombre $\varphi(x_0)\psi(x_0)\chi(x_0)\ldots$ est divisible par p, la fonction $\varphi(x)\psi(x)\chi(x)\ldots$, étant divisée par $F(x)$, donnera le reste du degré inférieur à n, dont tous les coefficients seront divisibles par p.

En désignant donc par $\varpi(x)$ le quotient de cette division, nous aurons

$$\varphi(x)\psi(x)\chi(x)\ldots - \varpi(x)F(x) \equiv 0 \pmod{p}.$$

La fonction $F(x)$ étant divisible suivant le module p par $V^m V_1^{m_1}\ldots V_h^{m_h}$, la congruence ci-dessus montre que le produit $\varphi(x)\psi(x)\chi(x)\ldots$ doit contenir comme facteur la fonction $V^m V_1^{m_1}\ldots V_s^{m_s}$ suivant le module p.

Réciproquement, lorsque le produit $\varphi(x)\psi(x)\chi(x)\ldots$ est divisible par $V^m V_1^{m_1}\ldots V_h^{m_h}$ suivant le module p, le nombre complexe

$$\varphi(x_0)\psi(x_0)\chi(x_0)\ldots$$

sera divisible par p. En effet, nous avons par hypothèse la congruence

$$\varphi(x)\psi(x)\chi(x)\ldots \equiv \lambda(x)V^m V_1^{m_1}\ldots V_h^{m_h} \pmod{p},$$

$\lambda(x)$ étant une fonction entière à coefficients entiers, ou, ce qui est le même, la congruence

$$\varphi(x)\psi(x)\chi(x)\ldots \equiv \lambda(x)F(x) \pmod{p},$$

d'où l'on voit que les coefficients de tous les termes de la différence

$$\varphi(x)\psi(x)\chi(x)\ldots - \lambda(x)F(x),$$

seront divisibles par p; par conséquent, le nombre complexe

$$\varphi(x_0)\psi(x_0)\chi(x_0)\ldots$$

est divisible par p.

D'après cela, pour reconnaître si le nombre complexe

$$\varphi(x_0)\psi(x_0)\chi(x_0)\ldots$$

est ou non divisible par p, il faut décomposer les fonctions

$$\varphi(x),\ \psi(x),\ \chi(x),\ \ldots$$

en facteurs irréductibles suivant le module p.

Cela fait, nous verrons tout de suite si la fonction $V^m V_1^{m_1} \dots V_h^{m_h}$ entre comme facteur suivant le module p dans le produit $\varphi(x)\psi(x)\chi(x)\dots$

2. Le produit

$$\varphi(x_0)\varphi(x_1)\dots\varphi(x_{n-1}) = N\varphi(x_0),$$

$\varphi(x_0)$ étant un nombre complexe entier, sera dit la *norme du nombre complexe* $\varphi(x_0)$. Ce produit est évidemment un nombre entier ordinaire.

Faisons voir maintenant qu'au moyen de la décomposition d'une fonction entière quelconque $\varphi(x)$ à coefficients entiers en facteurs irréductibles suivant le module p, on reconnaîtra facilement si la norme $N\varphi(x_0)$ du nombre $\varphi(x_0)$ est divisible par p. Supposons que les fonctions

$$V,\ V_1,\ V_2,\ \dots,\ V_h$$

qui figurent dans la congruence (2) du n° 1 aient respectivement pour degrés les nombres $\nu, \nu_1, \nu_2, \dots, \nu_h$.

On voit aisément que les coefficients des plus hautes puissances de x dans $V, V_1, \dots, V_h$ peuvent être faits égaux à l'unité.

Je vais démontrer en premier lieu que les normes des nombres complexes

$$V(x_0),\ V_1(x_0),\ \dots,\ V_h(x_0)$$

sont respectivement divisibles par $p^\nu, p^{\nu_1}, \dots, p^{\nu_h}$.

Il suffit pour cela de considérer une des fonctions $V, V_1, \dots$, par exemple V. Soient

$$\alpha_1,\ \alpha_2,\ \dots,\ \alpha_\nu$$

les racines de l'équation

$$V = 0;$$

il s'ensuit

$$V(x) = (x_0 - \alpha_1)(x_0 - \alpha_2)\dots(x_0 - \alpha_\nu).$$

Ainsi l'on aura

$$(3)\qquad \begin{cases} NV(x_0) = (x_0 - \alpha_1)(x_0 - \alpha_2)\dots(x_0 - \alpha_\nu) \\ \qquad \times (x_1 - \alpha_1)(x_1 - \alpha_2)\dots(x_1 - \alpha_\nu) \\ \qquad \times \dots\dots\dots\dots\dots\dots\dots\dots \\ \qquad \times (x_{n-1} - \alpha_1)(x_{n-1} - \alpha_2)\dots(x_{n-1} - \alpha_\nu) \\ \qquad = (-1)^{n\nu} F(\alpha_1) F(\alpha_2)\dots F(\alpha_\nu). \end{cases}$$

D'ailleurs, la congruence (2) peut être écrite comme il suit :

$$F(x) = V^m V_1^{m_1} \dots V_h^{m_h} + p\,\psi(x),$$

$\psi(x)$ étant un polygone à coefficients entiers.

Remplaçant ici x successivement par

$$\alpha_1,\ \alpha_2,\ \dots,\ \alpha_\nu,$$

on aura, en multipliant les résultats,

$$F(\alpha_1)\,F(\alpha_2)\dots F(\alpha_\nu) = p^\nu \psi(\alpha_1)\,\psi(\alpha_2)\dots\psi(\alpha_\nu).$$

Par conséquent, en vertu de l'équation (3), il viendra

$$VN = (-1)^{n\nu} p^\nu \psi(\alpha_1)\,\psi(\alpha_2)\dots\psi(\alpha_\nu). \tag{4}$$

Le produit

$$\psi(\alpha_1)\,\psi(\alpha_2)\dots\psi(\alpha_\nu)$$

étant un nombre entier, on en conclut que la norme NV est divisible par p^ν. Pareillement, on prouvera que les normes NV_1, NV_2, ..., NV_h sont divisibles respectivement par p^{ν_1}, p^{ν_2}, ..., p^{ν_h}.

Je vais établir, en second lieu, que la norme du nombre complexe quelconque $W(x_0)$ n'est divisible par p que dans le cas où la fonction $W(x)$ contient comme facteurs une ou plusieurs des fonctions V, V_1, V_2, ..., V_h.

En effet, en supposant que $W(x)$ et $F(x)$ n'ont point de facteurs communs suivant le module p, on peut trouver deux polynômes A et B tels, qu'on aura

$$AW - BF(x) \equiv 1 \pmod{p}.$$

Il s'ensuit

$$NA \,.\, NW \equiv 1 \pmod{p},$$

et, par conséquent, la norme NW n'est pas divisible par p.

Donc la fonction $W(x)$ doit être nécessairement divisible par l'une des fonctions V, V_1, ..., V_h suivant ce module p pour que la norme $NW(x_0)$ soit divisible par p.

Démontrons maintenant que cette condition est suffisante. Supposons, en effet, que $W(x)$ soit divisible suivant le module p par l'une des fonctions $V, V_1, \ldots, V_h$, par exemple par V. On aura alors

$$W(x) = \varphi(x)V + pf(x),$$

$\varphi(x)$ et $f(x)$ étant des polynômes à coefficients entiers. Remplaçant ici x successivement par

$$x_0, x_1, \ldots, x_{n-1}$$

et multipliant les résultats, il viendra

$$NW(x_0) \equiv N\varphi(x_0)NV(x_0) \equiv 0 \pmod{p},$$

car $NV(x_0)$ est divisible par p, comme il a été démontré ci-dessus.

3. En s'appuyant sur les propositions précédentes, on prouvera que l'exposant de la plus haute puissance de p qui divise la norme $NV(x_0)$ est un multiple de ν.

En effet, on voit d'après l'équation (4) que l'exposant avec lequel p entre comme facteur dans NV ne peut surpasser ν que dans le cas où $\psi(\alpha_1)\psi(\alpha_2)\ldots\psi(\alpha_\nu)$ sera divisible par p.

Le nombre $\psi(\alpha_1)\psi(\alpha_2)\ldots\psi(\alpha_\nu)$ étant la norme du nombre complexe $\psi(\alpha_1)$ relativement à l'équation

$$V = 0,$$

et V étant irréductible suivant le module p, il s'ensuit que

$$\psi(\alpha_1)\psi(\alpha_2)\ldots\psi(\alpha_\nu)$$

n'est divisible par p que dans le cas où $\psi(x)$ est divisible par V suivant le module p.

Posons donc

$$\psi(x) = \psi_1(x)V + p\varpi(x),$$

$\psi_1(x)$ et $\varpi(x)$ étant des polynômes à coefficients entiers. Remplaçant ici x successivement par

$$\alpha_1, \alpha_2, \ldots, \alpha_\nu,$$

nous aurons facilement

$$\psi(\alpha_1)\psi(\alpha_2)\dots\psi(\alpha_\nu) = p^\nu \varpi(\alpha_1)\varpi(\alpha_2)\dots\varpi(\alpha_\nu),$$

d'où il vient

$$\mathrm{NV} = (-1)^{\nu n} p^{2\nu} \varpi(\alpha_1)\varpi(\alpha_2)\dots\varpi(\alpha_\nu),$$

c'est-à-dire que, lorsque la norme V contient comme facteur le nombre p avec l'exposant supérieur à ν, elle est divisible par $p^{2\nu}$.

Par la même analyse, on démontrera la proposition générale.

4. On peut toujours aisément déterminer, comme on va le voir, les modules suivant lesquels la fonction $\mathrm{F}(x)$ admet des facteurs multiples.

Soit Δ le discriminant de l'équation

$$\mathrm{F}(x) = 0, \tag{1}$$

savoir :

$$\Delta = (x_0 - x_1)^2 (x_0 - x_2)^2 \dots (x_{n-2} - x_{n-1})^2.$$

L'équation (1), étant irréductible, n'a pas de racines égales, et, par conséquent, Δ est différent de zéro. Posons

$$\Delta = \pm q_1^{\alpha_1}, \; q_2^{\alpha_2}, \; \dots, \; q_s^{\alpha_s},$$

$q_1, q_2, \dots, q_s$ étant des nombres premiers différents.

Nous allons démontrer que la fonction $\mathrm{F}(x)$ n'admet des facteurs multiples que suivant les modules $q_1, q_2, \dots, q_s$.

Considérons, en premier lieu, le nombre premier p, différent de $q_1, q_2, \dots, q_s$.

Supposant que suivant ce module $\mathrm{F}(x)$ a un facteur multiple V^k, il viendra

$$\mathrm{F}(x) = \varphi(x)\mathrm{V}^k + p\,\varpi(x),$$

$\varphi(x)$ et $\varpi(x)$ étant des polynômes à coefficients entiers.

La dérivée

$$\mathrm{F}'(x) = \varphi'(x)\mathrm{V}^k + k\varphi(x)\mathrm{V}^{k-1}\mathrm{V}' + p\,\varpi'(x)$$

sera divisible suivant le module p par V, et, par suite, la norme $\mathrm{N}F'(x_0)$, ou, en d'autres termes, le produit

$$F'(x_0)\,F'(x_1)\ldots F'(x_{n-1})$$

sera divisible par p.

Cette norme étant égale au signe près au discriminant Δ, p doit diviser ce discriminant, ce qui est contraire à la supposition. Il nous reste maintenant à démontrer que $F(x)$ a effectivement des facteurs multiples suivant chacun des nombres $q_1, q_2, \ldots, q_p$.

En effet, supposant que le contraire ait lieu par rapport au module q_i, on aura

$$F(x) = VV_1 \ldots V_h + q_i \varpi(x)$$

$V, V_1, \ldots, V_h$ désignant des polynômes irréductibles et distincts suivant le module q_i, et $\varpi(x)$ une fonction entière à coefficients entiers. Cela étant, la dérivée $F'(x)$ n'est divisible suivant le module q_i par aucune des fonctions $V, V_1, \ldots, V_h$.

D'après cela, la norme de nombre complexe $F'(x_0)$, ou, en d'autres termes, le discriminant Δ, ne sera pas divisible par q_i (2), contrairement à la supposition.

5. Je reprends maintenant la congruence

$$F(x) \equiv V^m V_1^{m_1} \ldots V_h^{m_h} \pmod{p}. \tag{2}$$

Elle peut être écrite comme il suit,

$$F(x) = V^m V_1^{m_1} \ldots V_h^{m_h} + p\varphi(x), \tag{3}$$

$\varphi(x)$ désignant un polynôme à coefficients entiers. Les fonctions $V, V_1, \ldots, V_h$ ne sont pas déterminées complètement, car leurs coefficients peuvent être remplacés par les nombres congrus à eux suivant le module p. En faisant usage de cette remarque, il est facile de démontrer que, si l'un des exposants

$$m,\ m_1,\ \ldots,\ m_h,$$

par exemple m, est l'unité, la fonction $\varphi(x)$ peut être supposée non

divisible suivant le module p par un polynôme V correspondant à cet exposant.

En effet, soit $m = 1$ et soit $\varphi(x)$ divisible par V suivant le module p. Cela étant, on peut prendre au lieu de V un polynôme

$$W = V + p\psi(x),$$

$\psi(x)$ désignant une fonction entière à coefficients entiers de degré inférieur à celui de V; W sera aussi une fonction irréductible suivant le module p, et son premier coefficient est égal à l'unité. Remplaçant maintenant dans l'équation (3) la fonction V par W et ayant égard à ce que $m = 1$, nous avons

$$F(x) = W V_1^{m_1} V_2^{m_2} \dots V_h^{m_h} + p\varphi_1(x),$$

où

$$\varphi_1(x) = \varphi(x) - \psi(x) V_1^{m_1} V_2^{m_2} \dots V_h^{m_h}.$$

La fonction $\varphi(x)$ est divisible, d'après l'hypothèse, par V ou, ce qui est le même, par W suivant le module p; quant à $\psi(x)$, qui reste arbitraire, on peut supposer qu'elle n'est pas divisible par p, et par conséquent, étant du degré inférieur à W, elle ne sera pas divisible par W suivant le module p. Alors la fonction $\varphi_1(x)$ ne sera pas divisible par W. De la même manière on démontrera que, si plusieurs des exposants $m, m_1, m_2, \dots, m_h$ sont égaux à l'unité, la fonction $\varphi(x)$ de l'équation (3) peut être supposée non divisible par des polynômes de la suite $V, V_1, \dots, V_h$ correspondant à ces exposants.

J'observe maintenant que dans le cas où $\varphi(x)$ est divisible suivant le module p par l'une des fonctions V, dont l'exposant m surpasse l'unité, la transformation que nous avons employée ci-dessus n'amène pas à la fonction $\varphi_1(x)$ non divisible suivant le module p par V. Alors, la fonction $F(x)$ ayant des facteurs multiples suivant le module p, ce dernier doit être un des nombres

$$q_1, q_2, \dots, q_s.$$

D'abord, pour plus de simplicité, nous excluons ces cas de notre recherche, puis nous les considérons à part.

6. En étudiant des nombres complexes qui dépendent des racines d'une équation

$$F(x) = 0,$$

nous posons les définitions suivantes :

I. Nous classerons parmi les nombres premiers complexes le nombre premier réel ordinaire p, si $F(x)$ est une fonction irréductible suivant le module p. Tous les autres nombres entiers ordinaires seront dits les *nombres complexes composés*.

La division des nombres complexes en deux classes, celle des nombres premiers et celle des nombres composés, que j'expose dans ce qui va suivre, n'est point basée sur la décomposition ordinaire des nombres en facteurs premiers.

Néanmoins, il est facile de démontrer que les nombres premiers ordinaires, que nous convenons de classer parmi les nombres premiers complexes, ne sont en effet divisibles par aucun nombre complexe distinct de p et des unités complexes.

En effet, supposons que p soit le produit de deux nombres complexes $\varphi(x_0)$ et $\psi(x_0)$. Le produit $\varphi(x_0)\,\psi(x_0)$ étant divisible par p et $F(x)$ une fonction irréductible suivant ce module, on en conclut (**1**) qu'une des fonctions $\varphi(x)$ et $\psi(x)$ est divisible par $F(x)$ suivant le module p. En ayant égard à ce que les degrés de ces fonctions peuvent être supposés inférieurs à celui de $F(x)$, on voit que tous les coefficients de l'une d'elles sont divisibles par p. Ainsi l'on aura

$$\varphi(x) = p\,\varphi_1(x),$$

$\varphi_1(x)$ étant un polynôme à coefficients entiers, d'où, en vertu de l'équation

$$p = \varphi(x_0)\,\psi(x_0),$$

il viendra

$$\varphi_1(x_0)\,\psi(x_0) = 1;$$

par conséquent, $\varphi_1(x_0)$ et $\psi(x_0)$ sont des unités complexes.

Le même raisonnement nous conduit au théorème en vertu duquel nous comptons le nombre p parmi les nombres premiers complexes. Voici ce théorème : *Si le produit de deux ou plusieurs nombres com-*

plexes est divisible par un nombre premier ordinaire p suivant lequel $F(x)$ *est une fonction irréductible, un des facteurs est divisible par p.*

II. Examinons maintenant les nombres premiers ordinaires p suivant lesquels $F(x)$ n'est plus irréductible. Dans ce cas, $F(x)$ est décomposable suivant p en facteurs irréductibles. Soit

$$(1) \qquad F(x) = V^m V_1^{m_1} \dots V_h^{m_h} + p\varphi(x),$$

$V, V_1, \dots, V_h$ étant ces facteurs, dont les degrés sont respectivement

$$\nu, \nu_1, \dots, \nu_h,$$

et $\varphi(x)$ un polynôme à coefficients entiers non divisible suivant le module p par aucune des fonctions $V, V_1, \dots, V_h$. Nous classerons ce nombre p parmi les nombres complexes composés et nous dirons qu'il contient m facteurs premiers idéaux égaux correspondant à V, m_1 facteurs premiers idéaux égaux correspondant à V_1. Soit $f(x_0)$ un nombre complexe; nous dirons que $f(x_0)$ est divisible par un facteur du nombre p appartenant à V, si $f(x)$ est divisible par V suivant le module p.

7. Maintenant nous allons donner le critérium au moyen duquel on peut toujours reconnaître quels facteurs du nombre p et combien de fois ces facteurs entrent dans un nombre donné $f(x_0)$. Désignons, pour abréger, par $W, W_1, \dots, W_h$ respectivement les produits

$$V_1^{m_1} V_2^{m_2} \dots V_h^{m_h}, \quad V^m V_2^{m_2} \dots V_h^{m_h}, \quad \dots, \quad V^m V_1^{m_1} \dots V_{h-1}^{m_{h-1}},$$

et soit λ un nombre entier ordinaire quelconque.

Posons

$$\lambda = km + r,$$

k étant le quotient et r le reste de la division de λ par m. Cela posé, nous dirons que le nombre complexe $f(x_0)$ contient un facteur idéal, appartenant à V, λ fois si la congruence

$$(\alpha) \qquad f(x) V^{m-r} W^{k+1} \equiv 0 \quad [\text{mod.} p^{k+1}, F(x)]$$

est satisfaite, mais la congruence

$$(\beta) \qquad f(x)\,V^{2m-r-1}\,W^{k+2} \equiv 0 \quad [\text{mod. } p^{k+2}, F(x)]$$

n'ayant pas lieu.

De la même manière on détermine les degrés de multiplicité des autres facteurs idéaux contenus dans $f(x_0)$. Maintenant nous allons établir quelques théorèmes qui feront ressortir toute la portée des facteurs idéaux dans la théorie des nombres complexes.

8. THÉORÈME. — *Si le nombre $f(x_0)$ contient le facteur idéal de p, appartenant à* V, λ *fois et que le nombre complexe $\psi(x_0)$ ne le contienne point, le produit $f(x_0)\psi(x_0)$ le contient λ fois.*

Soit, comme précédemment,

$$\lambda = km + r.$$

On aura, d'après l'hypothèse,

$$(1) \qquad f(x)V^{m-r}W^{k+1} = p^{k+1}f_1(x) + \varpi(x)F(x),$$

$f_1(x)$ et $\varpi(x)$ étant deux polynômes à coefficients entiers. On voit facilement que $f_1(x)$ n'est pas divisible par V suivant le module p. En effet, dans le cas contraire, le produit

$$p^{k+1}f_1(x)V^{m-1}W = f(x)V^{2m-r-1}W^{k+2} - F(x)\varpi(x)V^{m-1}W$$

serait divisible par p^{k+2}, en faisant abstraction des multiples de $F(x)$, savoir : $f(x_0)$ contiendrait le facteur de p appartenant à V plus de λ fois, ce qui est contraire à la supposition.

En multipliant l'équation (1) par $\psi(x)$, on aura

$$\psi(x)f(x)V^{m-r}W^{k+1} = p^{k+1}f_1(x)\,\psi(x) + \varpi(x)\,\psi(x)\,F(x).$$

Cela fait voir que le nombre complexe $\psi(x_0)f(x_0)$ contient le facteur de p appartenant à V au moins λ fois. D'ailleurs, en remarquant que la fonction $f_1(x)\,\psi(x)$ n'est pas divisible par V suivant le module p, on voit que la fonction

$$p^{k+1}f_1(x)\psi(x)V^{m-1}W,$$

ou, ce qui est le même produit,

$$f(x)\,\psi(x)\,V^{2m-r-1}\,W^{k+2},$$

n'est pas divisible par p^{k+2}, en faisant abstraction des multiples de $F(x)$.

Donc le nombre $f(x_0)\,\psi(x_0)$ contient le facteur idéal de p appartenant à V précisément λ fois.

9. THÉORÈME. — *Le produit $f(x_0)\,\psi(x_0)$ de deux nombres complexes contient le facteur idéal de p appartenant à* V *autant de fois que les deux nombres $f(x_0)$ et $\psi(x_0)$ ensemble.*

Supposons que $f(x_0)$ contienne ce facteur λ fois et $\psi(x_0)$ λ' fois. Soient, pour abréger,

$$\lambda = k\,m + r,$$
$$\lambda' = k'm + r';$$

k, k', r, r' sont respectivement les quotients et les restes des divisions de λ et λ' par m.

On a, par hypothèse,

$$(1)\qquad f(x)V^{m-r}\,W^{k+1} = p^{k+1}f_1(x) + \varpi(x)F(x),$$
$$(2)\qquad \psi(x)V^{m-r'}\,W^{k'+1} = p^{k'+1}\psi_1(x) + \varpi_1(x)F(x),$$

$f_1(x)$, $\psi_1(x)$, $\varpi(x)$ et $\varpi_1(x)$ étant des polynômes à coefficients entiers; chacune des fonctions $f_1(x)$ et $\psi_1(x)$ n'est pas divisible par V suivant le module p.

Les égalités (1) et (2) nous donnent la suivante,

$$(3)\quad f(x)\psi(x)V^{2m-r-r'}W^{k+k'+2} = p^{k+k'+2}f_1(x)\psi_1(x) + G(x)F(x),$$

$G(x)$ étant encore un polynôme à coefficients entiers.

Maintenant nous avons deux cas à distinguer :

1° $r + r' < m$. En substituant dans l'équation (3) au lieu de $V^m W$ sa valeur

$$-p\varphi(x) + F(x)$$

déduite de l'équation

$$F(x) = V^m V_1^{m_1} \dots V_h^{m_h} + p\varphi(x),$$

il vient

$$\varphi(x) f(x) \psi(x) V^{m-r-r'} W^{k+k'+1} = -p^{k+k'+1} f_1(x) \psi_1(x) + G_1(x) F(x),$$

$G_1(x)$ désignant aussi un polynôme à coefficients entiers. Il s'ensuit que le produit $f(x_0)\psi(x_0)\varphi(x_0)$ contient le facteur de p appartenant à V un nombre de fois qui est précisément

$$(k + k')m + r + r' = \lambda + \lambda';$$

$\varphi(x_0)$ n'étant pas divisible par ce facteur (n° 6, II), on voit que le produit $f(x_0)\psi(x_0)$ contient le facteur de p, appartenant à V, $\lambda + \lambda'$ fois.

2° $r + r' \geqq m$; d'ailleurs, bien entendu, $r + r' < 2m$. Supposant

$$r + r' = m + \rho,$$

on peut écrire l'égalité (3) comme il suit:

$$f(x) \psi(x) V^{m-\rho} W^{k+k'+2} = p^{k+k'+2} f_1(x) \psi_1(x) + G(x) F(x),$$

d'où l'on voit que le nombre $f(x_0)\psi(x_0)$ contient le facteur de p appartenant à V un nombre de fois qui est

$$(k + k' + 1)m + \rho = \lambda + \lambda'.$$

10. Théorème. — *Si le nombre complexe $f(x_0)$ contient le facteur idéal de p appartenant à* V *au moins sm fois, s étant un nombre entier, le facteur de p appartenant à* V_1 *au moins sm_1 fois et ainsi de suite, $f(x_0)$ est divisible par p^s.*

On a, d'après l'hypothèse,

$$f(x) V^m W^{s+1} = p^{s+1} \psi(x) + \varpi(x) F(x),$$

$\varpi(x)$ étant un polynôme à coefficients entiers.

Remarquant que

$$V^m W = -p\varphi(x) + F(x),$$

il vient

$$f(x)\,\varphi(x)W^s = p^s\psi(x) + \varpi_1(x)\,F(x),$$

$\varpi_1 x$ étant encore un polynôme à coefficients entiers.

Pareillement, il viendra

$$\begin{aligned}
f(x)\varphi(x)W_1^s &= -p^s\psi_1(x) + \varpi_2(x)Fx,\\
f(x)\varphi(x)W_2^s &= -p^s\psi_2(x) + \varpi_3(x)Fx,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
f(x)\varphi(x)W_h^s &= -p^s\psi_3(x) + \varpi_{s+1}(x)\,F(x).
\end{aligned}$$

Par conséquent, le nombre complexe

$$f(x_0)\,\varphi(x_0)\,[W^s(x_0) + W_1^s(x_0) + \ldots + W_h^s(x_0)]$$

est divisible par p^s. La fonction

$$\varphi(x)\,(W^s + W_1^s + \ldots + W_h^s)$$

n'est divisible suivant le module p par aucune des fonctions

$$V,\ V_1,\ \ldots,\ V_h;$$

donc (**1**) le nombre $f(x_0)$ doit être divisible par p. Soit

$$f(x_0) = pf_1(x_0).$$

Par le même raisonnement, nous ferons voir que $f_1(x_0)$ est aussi divisible par p, savoir $f(x_0)$ divisible par p^2. Ainsi l'on démontrera, en définitive, que $f(x_0)$ est divisible par p^s.

11. Supposons que le nombre complexe $f(x_0)$ contienne le facteur de p, appartenant à V, λ fois; le facteur de p, appartenant à V_1, λ_1 fois, etc. Nous allons démontrer que, dans ce cas, la norme du nombre complexe $f(x_0)$ contient p précisément $\lambda\nu + \lambda_1\nu_1 + \ldots + \lambda_h\nu_h$ fois, $\nu, \nu_1, \ldots, \nu_h$ étant des degrés des fonctions V, $V_1, \ldots, V_h$.

Dans ce but, considérons le nombre complexe

$$f(x_0)\,\mathrm{V}^{mk-\lambda}(x_0)\,\mathrm{V}_1^{m_1k-\lambda_1}(x_0)\ldots\,\mathrm{V}_h^{m_hk-\lambda_h}(x_0),$$

k désignant un entier positif satisfaisant aux inégalités

$$mk>\lambda,\ m_1k>\lambda_1,\ \ldots,\ m_hk>\lambda_h.$$

Ce nombre complexe contient le facteur idéal de p, appartenant à V, mk fois; le facteur idéal de p, appartenant à V_1, m_1k fois, etc.; par conséquent, il sera de la forme

$$p^k, f_1(x_0),$$

le nombre complexe $f_1(x_0)$ n'étant divisible par aucun des facteurs idéaux de p, ou, ce qui est le même, $f_1(x)$ n'est divisible suivant le module p par aucune des fonctions $\mathrm{V}, \mathrm{V}_1,\ldots,\mathrm{V}_h$. Cela posé, on aura

$$\begin{aligned}&\mathrm{N}f(x_0)(\mathrm{NV})^{mk-\lambda}(\mathrm{NV}_1)^{m_1k-\lambda_1}\ldots(\mathrm{NV}_h)^{m_hk-\lambda_h}\\&\quad=p^{kn}\mathrm{N}f_1(x_0)=p^{k(m\nu+m_1\nu_1+\ldots+m_h\nu_h)}\mathrm{N}f_1(x_0).\end{aligned}$$

Remarquant que les normes

$$\mathrm{NV},\ \mathrm{NV}_1,\ \ldots,\ \mathrm{NV}_h$$

contiennent le facteur p respectivement avec les exposants (2)

$$\nu,\ \nu_1,\ \ldots,\ \nu_h,$$

et que la norme $\mathrm{N}f_1(x_0)$ n'est pas divisible par p, on voit que $\mathrm{N}f(x_0)$ contient le facteur p avec l'exposant

$$\lambda\nu+\lambda\nu_1+\ldots+\lambda_h\nu_h.$$

Il suit de là que tout nombre complexe contient les facteurs idéaux de nombres premiers ordinaires qui divisent sa norme, chaque facteur un nombre fini de fois, et il ne contient point d'autres facteurs idéaux.

Décomposition des nombres complexes en facteurs premiers idéaux.

12. Les résultats du numéro précédent permettent toujours de reconnaître les nombres ordinaires dont les facteurs idéaux entrent dans le nombre complexe quelconque $\varphi(x_0)$.

On peut les reconnaître encore en opérant comme il suit.

Faisons avec les deux fonctions $\varphi(x)$ et $F(x)$ les divisions successives pour trouver leur plus grand commun diviseur. Comme l'équation

$$F(x) = 0$$

est irréductible, nous allons parvenir au reste constant égal à une fraction rationnelle, car les coefficients de $\varphi(x)$ et $F(x)$ sont des nombres entiers. Il est connu comment on obtient de cette manière deux fonctions entières, à coefficients entiers A et B, telles que la différence

$$A F(x) - B \varphi(x)$$

est égale à un nombre entier. En désignant ce nombre par M, on aura

$$A F(x) - B \varphi(x) = M.$$

Si $\varphi(x)$ est divisible par un facteur idéal du nombre premier ordinaire p, les fonctions $\varphi(x)$ et $F(x)$ ont un diviseur commun suivant ce module (**6**). Ce diviseur doit diviser M. Or, comme M est un nombre entier ordinaire, il doit être divisible par p. Il résulte de là que, pour trouver les facteurs idéaux du nombre complexe $\varphi(x_0)$, nous décomposons d'abord $F(x)$ en facteurs premiers suivant tous les nombres premiers p qui divisent M. Ensuite, en ayant ces décompositions, au moyen du critérium (**7**), nous trouverons quels facteurs idéaux et combien de fois ces facteurs sont contenus dans $\varphi(x_0)$. Soient $d_1, d_2, \ldots, d_e$ les différents facteurs premiers idéaux du nombre $\varphi(x_0)$, et $\lambda_1, \lambda_2, \ldots, s\lambda_e$ leurs degrés de multiplicité. Nous écrirons

$$\varphi(x_0) = d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_e^{\lambda_e} \varphi_1(x_0), \tag{1}$$

$\varphi_1(x_0)$ étant une unité complexe quelconque.

Cette équation est, bien entendu, symbolique, car $d_1, d_2, \ldots, d_e$ n'ont pas de valeurs.

L'équation (1) exprime la composition intérieure du nombre complexe $\varphi(x_0)$ et dans la théorie de ces nombres elle représente la généralisation de la décomposition ordinaire des nombres de la forme $a + bi$ en facteurs premiers.

13. De la décomposition des nombres complexes en facteurs idéaux on peut déduire une règle par laquelle on reconnaîtra la divisibilité d'un nombre complexe $\varphi(x_0)$ par un autre $\psi(x_0)$. Supposons que ces nombres, étant décomposés en facteurs idéaux, aient la forme

$$\varphi(x_0) = d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_e^{\lambda_e} \varphi_1(x_0),$$
$$\psi(x_0) = e_1^{\mu_1} e_2^{\mu_2} \ldots e_k^{\mu_k} \psi_1(x_0),$$

$\varphi_1(x_0)$ et $\psi_1(x_0)$ désignant deux unités complexes.

Nous allons démontrer que pour la divisibilité de $\varphi(x_0)$ par $\psi(x_0)$ il faut et il suffit que les facteurs

$$e_1, e_2, \ldots, e_k$$

soient contenus parmi les facteurs

$$d_1, d_2, \ldots, d_e$$

et qu'ils entrent dans $\varphi(x_0)$ avec des exposants non inférieurs respectivement à

$$\mu_1, \mu_2, \ldots, \mu_k.$$

En effet, si $\varphi(x_0)$ est divisible par $\psi(x_0)$, on aura

$$\varphi(x_0) = \psi(x_0)\, \varpi(x_0),$$

$\varpi(x_0)$ étant un nombre entier complexe.

Il est évident que, dans ce cas, $\varphi(x_0)$ contient tous les facteurs premiers idéaux de $\psi(x_0)$,

$$e_1, e_2, \ldots, e_k,$$

avec les exposants non inférieurs à

$$\mu_1,\ \mu_2,\ \ldots,\ \mu_k \quad (9).$$

Réciproquement, si $\varphi(x_0)$ contient tous les facteurs

$$e_1,\ e_2,\ \ldots,\ e_k$$

et si leurs degrés de multiplicité ne sont pas inférieurs respectivement à

$$\mu_1,\ \mu_2,\ \ldots,\ \mu_k,$$

$\varphi(x_0)$ est divisible par $\psi(x_0)$.

En effet, on a

$$\frac{\varphi(x_0)}{\psi(x_0)} = \frac{\varphi(x_0)\Psi(x_0)}{\mathrm{N}\psi(x_0)},$$

$\Psi(x_0)$ étant un nombre complémentaire de $\psi(x_0)$, savoir

$$\Psi(x_0) = \psi(x_1)\psi(x_2)\ldots\psi(x_{n-1}).$$

En outre, tout facteur idéal de $\mathrm{N}\psi(x_0)$ entre dans le produit $\varphi(x_0)\Psi(x_0)$ avec un exposant plus grand que dans $\mathrm{N}\psi(x_0)$. Il résulte de là que $\frac{\varphi(x_0)}{\psi(x_0)}$ est un nombre entier complexe (**10**).

Corollaire I. — Si le rapport de deux nombres complexes $\frac{\varphi(x_0)}{\psi(x_0)}$ n'est pas un nombre entier (complexe), aucune puissance $\frac{\varphi^m(x_0)}{\psi^m(x_0)}$ ne peut être un tel nombre. En effet, dans ce cas, $\psi(x_0)$ contient au moins un facteur premier idéal avec un exposant supérieur à celui du même facteur dans $\varphi(x_0)$. La même circonstance aura lieu par rapport aux nombres $\varphi^m(x_0)$ et $\psi^m(x_0)$, et, par conséquent, $\frac{\varphi^m(x_0)}{\psi^m(x_0)}$ n'est point un nombre entier complexe.

On peut établir une propriété des nombres complexes entiers plus générale.

Soit

$$\varphi(x_0) = a_0 + a_1x_0 + a_2x_0^2 + \ldots + a_{n-1}x_0^{n-1}$$

un nombre complexe entier quelconque. Les nombres

$$\varphi(x_0),\ \varphi(x_1),\ \ldots,\ \varphi(x_{n-1}),$$

$x_0, x_1, \ldots, x_{n-1}$ étant n racines d'une équation fondamentale

$$F(x)=0,$$

satisfont évidemment à l'équation de la forme

$$z^n + q_1 z^{n-1} + \ldots + q_n = 0, \tag{1}$$

$q_1, q_2, \ldots, q_n$ étant des nombres entiers ordinaires.

Maintenant il est facile de démontrer que, si le rapport $\frac{\varphi(x_0)}{\psi(x_0)}$ de deux nombres complexes entiers n'est pas un nombre entier, il ne peut satisfaire à aucune équation de la forme (1). En effet, désignons par d un des facteurs idéaux de $\psi(x_0)$ qui entrent dans $\psi(x_0)$ avec exposant supérieur à celui du même facteur dans $\varphi(x_0)$.

En supposant que la quantité $\frac{\varphi(x_0)}{\psi(x_0)}$ satisfasse à l'équation (1), il vient

$$\varphi^m(x_0) = -q_1\varphi^{m-1}(x_0)\,\psi(x_0) - q_2\varphi^{m-2}(x_0)\,\psi^2(x_0) - \ldots - q_n\psi^n(x_0)$$

Le premier terme de cette équation contient le facteur d moins de fois que le second, ce qui est évidemment impossible.

Corollaire II. — Il suit de la proposition établie dans ce numéro que chaque nombre complexe n'est décomposable que d'une seule manière en facteurs premiers idéaux. Supposons, en effet, qu'il existe pour un nombre complexe $\varphi(x_0)$ deux décompositions en facteurs premiers idéaux :

$$\varphi(x_0) = d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_c^{\lambda_c}\varphi_1(x_0),$$
$$\varphi(x_0) = e_1^{\mu_1} e_2^{\mu_2} \ldots e_k^{\mu_k}\varphi_2(x_0),$$

$\varphi_1(x_0)$ et $\varphi_2(x_0)$ étant des unités complexes.

On voit que les rapports

$$\frac{d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_c^{\lambda_c}}{e_1^{\mu_1} e_2^{\mu_2} \ldots e_k^{\mu_k}},\quad \frac{e_1^{\mu_1} e_2^{\mu_2} \ldots e_k^{\mu_k}}{d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_c^{\lambda_c}}$$

sont des unités complexes. Il en résulte que tous les facteurs idéaux

$$e_1,\ e_2,\ \ldots,\ e_k$$

sont renfermés parmi les facteurs

$$d_1,\ d_2,\ \ldots,\ d_e$$

et *vice versa*. Par conséquent, deux suites de facteurs

$$e_1,\ e_2,\ \ldots,\ e_k,$$
$$d_1,\ d_2,\ \ldots,\ d_e$$

doivent être identiques. Donc on peut supposer

$$d_1 = e_1, \quad d_2 = e_2, \quad \ldots, \quad d_e = e_k, \quad e = k.$$

Cela étant, les exposants

$$\lambda_1,\ \lambda_2,\ \ldots,\ \lambda_e$$

ne sont pas inférieurs respectivement à

$$\mu_1,\ \mu_2,\ \ldots,\ \mu_k,$$

parce que le nombre

$$\frac{d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_e^{\lambda_e}}{e_1^{\mu_1} e_2^{\mu_2} \ldots e_k^{\mu_k}}$$

est un nombre entier.

Réciproquement, les exposants

$$\mu_1,\ \mu_2,\ \ldots,\ \mu_k$$

ne sont pas inférieurs respectivement à

$$\lambda_1,\ \lambda_2,\ \ldots,\ \lambda_e,$$

car le nombre

$$\frac{e_1^{\mu_1} e_2^{\mu_2} \ldots e_k^{\mu_k}}{d_1^{\lambda_1} d_2^{\lambda_2} \ldots d_e^{\lambda_e}}$$

est aussi un nombre entier. Ainsi, nous aurons

$$\lambda_1 = \mu_1, \quad \lambda_2 = \mu_2, \quad \ldots,$$

et les deux décompositions ne diffèrent entre elles ni par les facteurs idéaux ni par leurs exposants.

14. On déduit de la décomposition des nombres en facteurs premiers idéaux des théorèmes complètement analogues à ceux qui ont lieu pour les nombres entiers ordinaires.

Nous les indiquerons seulement, car leurs démonstrations ne présentent aucune difficulté. Deux nombres complexes sont nommés premiers entre eux s'ils n'ont point de facteurs idéaux communs.

THÉORÈME. — *Si le nombre complexe* $\psi(x_0)$ *premier à* $\varphi(x_0)$ *divise le produit* $\varphi(x_0)\,\varphi_1(x_0)$, *il divise le nombre* $\varphi_1(x_0)$.

THÉORÈME. — *Si le nombre complexe* $\psi(x_0)$ *est premier par rapport à chacun des nombres complexes* $\varphi(x_0)$, $\varphi_1(x^0)$, $\varphi_2(x_0)$, ..., *il est premier par rapport à leur produit.*

Il est nécessaire maintenant de définir comment on doit concevoir le produit de deux ou de plusieurs facteurs idéaux. Nous avons vu que tout nombre premier idéal tient lieu d'une certaine congruence. L'ensemble des congruences qui se rapportent à deux nombres premiers idéaux est remplacé par un nouveau nombre idéal qui s'appelle le produit de ces deux nombres. Le produit de tous les facteurs premiers idéaux communs à deux nombres s'appelle *leur plus grand commun diviseur.*

Quelques cas particuliers des nombres complexes.

15. Dans les numéros précédents, nous avons considéré les nombres complexes qui dépendent d'une racine de l'équation irréductible

$$F(x) = 0,$$

à coefficients entiers. Dans la théorie de ces nombres, sont contenus,

comme cas particuliers, la théorie de Gauss pour les nombres de la forme $a + bi$ et celle de M. Kummer pour les nombres complexes qui dépendent des racines d'un degré quelconque de l'unité. Nous allons nous arrêter un peu sur ces cas.

Considérons séparément ces deux cas particuliers.

Soient d'abord

$$F(x) = x^2 + 1,$$

et p un nombre premier ordinaire quelconque.

La fonction $x^2 + 1$ peut être irréductible suivant le module p, ou elle est le produit des deux fonctions irréductibles du premier degré.

Dans le dernier cas, la congruence $x^2 + 1 \equiv 0 \pmod{p}$ aura deux racines, et, par conséquent, p doit être égal à 2 ou être de la forme $4n + 1$.

Les nombres premiers de la forme $4n + 3$ sont donc encore premiers dans la suite des nombres $a + bi$.

De plus, en remarquant que $2 = (1 + i)(1 - i)$, et que tout nombre premier $4n + 1$ se représente dans la forme

$$a^2 + b^2 = (a + bi)(a - bi),$$

on voit que ces nombres sont composés dans l'ensemble des nombres complexes de la forme $a + bi$.

Dans le cas de ces nombres il n'y a point de facteurs idéaux; tous les facteurs premiers sont réels.

16. Avant de considérer les nombres complexes qui dépendent des racines de l'équation

$$\frac{x^n - 1}{x - 1} = 0,$$

nous démontrons quelques théorèmes qui se rapportent à la fonction $\frac{x^n - 1}{x - 1}$, prise suivant le module premier p.

Si n est divisible par p, on aura, en supposant $n = p^\mu \nu$,

$$x^n - 1 \equiv (x^\nu - 1)^{p^\mu} \pmod{p};$$

par conséquent, il suffit d'examiner la fonction $x^n - 1$ dans la supposition n non divisible par p.

Si $n = p$, il vient

$$x^p - 1 \equiv (x-1)^p \pmod{p}.$$

Donc la fonction $x^p - 1$ est congrue suivant le module p à la puissance p du facteur $x - 1$.

Maintenant, supposant n non divisible par p, nous allons établir les propositions suivantes.

Remarquons, en premier lieu, que la fonction $x^n - 1$ n'a pas de facteurs multiples suivant le module p.

THÉORÈME I. — *Tout facteur irréductible suivant le module p de la fonction* $x^n - 1$ *divise aussi la fonction* $x^{\lambda n} - 1$, λ *étant un nombre entier positif.*

En effet, la fonction $x^n - 1$ divise algébriquement la fonction $x^{\lambda n} - 1$, et, par conséquent, tous les facteurs suivant le module quelconque de la fonction $x^n - 1$ divisent aussi la fonction $x^{\lambda n} - 1$.

THÉORÈME II. — *Chaque diviseur commun des fonctions* $\frac{x^n-1}{x-1}$ *et* $\frac{x^\lambda - 1}{x-1}$, *suivant le module p, divise aussi la fonction* $\frac{x^\delta - 1}{x-1}$, δ *étant le plus grand commun diviseur des nombres n et* λ.

Soient s et t deux nombres entiers positifs satisfaisant à l'équation

$$sn - t\lambda = \delta.$$

Le diviseur commun des fonctions $\frac{x^n-1}{x-1}$, $\frac{x^\lambda-1}{x-1}$ suivant le module p divisera encore, suivant ce module, les fonctions $\frac{x^{sn}-1}{x-1}$ et $\frac{x^{t\lambda}-1}{x-1}$, et par conséquent leur différence

$$\frac{x^{sn} - x^{t\lambda}}{x-1} = x^{s\lambda}\frac{x^\delta - 1}{x-1}.$$

Donc il divisera, suivant le module p, la fonction $\frac{x^\delta - 1}{x-1}$.

THÉORÈME III. — *Si n est un nombre premier et si p appartient à l'exposant h suivant le module n, h étant, comme on sait, un diviseur de* $n-1$, *la fonction* $\frac{x^n-1}{x-1}$ *est congrue suivant le module p au produit de* $\frac{n-1}{h}$ *fonctions irréductibles de degré h.*

Remarquons en premier lieu que la fonction $\frac{x^n-1}{x-1}$ ne peut avoir aucun diviseur suivant le module p qui ne serait pas du degré h ou de degré multiple de h.

En effet, supposons que la fonction soit divisible suivant le module p par une fonction irréductible de degré ν. Cette fonction divisera aussi suivant le module p la fonction (1)

$$x^{p^\nu} - x = x(x^{p^\nu - 1} - 1),$$

et, par conséquent, $p^\nu - 1$ est divisible par n, ou, en d'autres termes,

$$p^\nu \equiv 1 \pmod{n}.$$

Mais p appartient à l'exposant h; donc ν est divisible par h.

En second lieu, nous allons démontrer que la fonction $\frac{x^n-1}{x-1}$ ne renferme point comme facteur suivant le module p des fonctions irréductibles dont les degrés sont multiples de h et non égaux à h.

A cet effet, remarquons que la fonction $\frac{x^n-1}{x-1}$ divise algébriquement la fonction $x^{p^h} - x = x(x^{p^h-1} - 1)$. D'après cela, si une fonction de degré $\nu = \lambda h, \lambda > 1$, divise suivant le module p la fonction $x^n - 1$, elle divisera aussi la fonction $x^{p^h} - x$. Mais, h étant inférieur à ν, cela est impossible.

17. On peut, comme nous allons le voir, par un procédé très simple, obtenir des facteurs irréductibles de la fonction $\frac{x^n-1}{x-1}$ suivant le module p. Deux fonctions entières A et B, à coefficients entiers, seront dites

(1) SERRET, *Cours d'Algèbre supérieure*, t. II, p. 139.

congrues suivant la fonction entière U, dont les coefficients sont aussi des nombres entiers, si la différence A — B est divisible algébriquement par U. Pour exprimer cette congruence, nous écrivons

$$A \equiv B\ (U).$$

Cela posé, soit

$$U = \frac{x^n - 1}{x - 1},$$

n étant un nombre premier.

Nous allons démontrer que dans la suite de fonctions

$$(1) \qquad 1,\ x,\ x^2,\ \ldots,\ x^{n-1},\ x^n,\ x^{n+1},\ \ldots$$

les n premiers termes sont incongrus entre eux suivant la fonction U. En effet, la différence

$$x^m - x^\nu,$$

m et ν étant inférieurs à n, n'est pas divisible algébriquement par U.

De plus, chaque terme de la suite (1) est congru suivant la fonction U à une des fonctions $1, x, x^2, \ldots, x^{n-1}$.

En effet, soit x^m un terme de la suite (1), m étant supérieur à $n - 1$.

Désignant par s le quotient et par r le reste de la division de m par n, on aura

$$m = sn + r.$$

La différence

$$x^m - x^r = x^r(x^{sn} - 1)$$

est évidemment divisible par U. Donc

$$x^m \equiv x^r\ (U).$$

Les fonctions $x, x^2, \ldots, x^{n-1}$ peuvent être distribuées *en périodes* (1) comme il suit. Soit

$$n - 1 = ef,$$

e et f étant deux diviseurs de $n - 1$, et désignons par g une racine primitive de nombre n.

---

(1) *Gauss Werke*, Band II, *Solutio congruentiæ* $x^m - 1 \equiv 0$.

Comme nous avons à considérer les congruences suivant la fonction U, on peut prendre, au lieu des fonctions

$$x,\ x^2,\ \ldots,\ x^{n-1},$$

les fonctions

$$(2) \qquad x^g,\ x^{g^2},\ \ldots,\ x^{g^{n-1}},$$

car les deux suites se sont composées de termes congrus suivant la fonction U. Désignons maintenant par

$$\xi,\ \xi_1,\ \ldots,\ \xi_{e-1}$$

les fonctions suivantes :

$$(U) \qquad \begin{cases} \xi \equiv x + x^{g^e} + x^{g^{2e}} + \ldots + x^{g^{(f-1)e}}, \\ \xi_1 \equiv x^g + x^{g^{e+1}} + x^{g^{2e+1}} + \ldots + x^{g^{(f-1)e+1}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \xi_{e-1} \equiv x^{g^{e-1}} + x^{g^{2e-1}} + x^{g^{3e-1}} + \ldots + x^{g^{fe-1}}. \end{cases}$$

Ces fonctions seront dites les *périodes*. Les fonctions $\xi, \xi_1, \ldots, \xi_{e-1}$ ne sont pas tout à fait déterminées, parce qu'on les obtient au moyen des congruences suivant le module U.

Par rapport aux périodes nous ferons les remarques suivantes :

1° Les périodes

$$\xi,\ \xi_1,\ \ldots,\ \xi_{e-1}$$

se déduisent l'une de l'autre par changement de x en x^g ; si l'on fait la même substitution dans la période ξ_{e-1}, on aura $\xi_e \equiv \xi\,(U)$. Puis, en appliquant la même substitution, on reproduira les périodes $\xi_1, \xi_2, \ldots, \xi_{e-1}$.

En général, on aura

$$\xi_{\lambda e+h} \equiv \xi_h \quad (U).$$

Il suit de là que si l'on remplace x par x^μ, μ satisfaisant à la congruence

$$\mu \equiv g^{\lambda e} \pmod{n},$$

les périodes restent invariables, et, si μ satisfait à la congruence

$$\mu \equiv g^{\lambda e+h} \pmod{n},$$

les périodes $\xi, \xi_1, \ldots, \xi_{e-1}$ se transforment respectivement en

$$\xi_h, \ \xi_{h+1}, \ \ldots, \ \xi_{h+e-1}.$$

En remplaçant enfin, dans la période ξ, x par $x^{\lambda n}$, λ étant un nombre entier positif, on aura la fonction A :

$$(\mathrm{U}) \qquad \mathrm{A} \equiv x^{\lambda n} + x^{\lambda n g^e} + \ldots.$$

La fonction $x^{kn} - 1$ étant divisible par U, il vient

$$\mathrm{A} \equiv f(\mathrm{U}).$$

Donc, en désignant par $[f, \lambda]$ la somme

$$x^{\lambda} + x^{\lambda g^e} + x^{\lambda g^{2e}} + \ldots + x^{\lambda g^{(f-1)e}},$$

on aura

$$(\mathrm{U}) \qquad \xi \equiv [f, 1], \quad \xi_1 \equiv [f, g], \quad \ldots, \quad \xi_{e-1} \equiv [f, g^{e-1}].$$

2° La somme de périodes

$$(\mathrm{U}) \qquad \xi + \xi_1 + \xi_2 + \ldots + \xi_{e-1} \equiv x + x^2 + \ldots + x^{n-1} \equiv -1.$$

3° Si f est le produit de deux nombres entiers b et c, chacune des périodes $[f, 1]$, $[f, g]$, ... contenant f termes se compose de c périodes dont chacune contient b termes, savoir :

$$[f, 1] = [b, 1] + [b, g^e] + [b, g^{2e}] \ldots [b, g^{(c-1)e}],$$
$$[f, g] = [b, g] + [b, g^{e+1}] + [b, g^{2e+1}] \ldots [b, g^{(c-1)e+1}],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

4° Maintenant il est aisé de voir que l'ensemble des périodes ne dépend pas de la racine primitive g, choisie arbitrairement.

En effet, soit G une autre racine primitive du nombre n.

Cela posé, nous aurons, comme on sait,

$$\mathrm{G} \equiv g^{\mu} \pmod{n},$$

μ étant un nombre premier avec $n - 1$.

Il suit de là que les résidus minima des nombres $1, g^e, g^{2e}, \ldots, g^{(f-1)e}$ suivant le module n ne sont distincts que par l'ordre des résidus minima des nombres $1, G^e, G^{2e}, \ldots, G^{(f-1)e}$. De plus, les nombres $g^\alpha, g^{e+\alpha}, g^{2e+\alpha}, \ldots, g^{(f-1)e+\alpha}$ sont congrus suivant le module n, en faisant abstraction de l'ordre, aux nombres $G^\beta, G^{e+\beta}, G^{2e+\beta}, \ldots, G^{(f+1)e+\beta}$, lorsque $g^\alpha \equiv G^\beta \pmod{n}$.

De tout cela il résulte que, si l'on change dans les périodes

$$[f, 1], [f, g], \ldots, [f, g^{e-1}]$$

g en G, on ne variera que leur ordre.

18. Démontrons maintenant le théorème fondamental par rapport aux périodes.

THÉORÈME. — *Le produit de deux périodes* $[f, \lambda]$ *et* $[f, \mu]$ *égales ou distinctes est congru, suivant la fonction* (U), *à une fonction linéaire des périodes* $[f, 1], [f, g], \ldots, [f, g^{e-1}]$, *à coefficients entiers.*

En multipliant chaque terme de la période $[f, \mu]$ par la période

$$(U) \qquad [f, \lambda] \equiv [f, \lambda g^e] \equiv [f, \lambda g^{2e}],$$

on aura

$$(U) \quad \left\{ \begin{aligned} [f, \lambda][f, \mu] &\equiv [f, \lambda] x^\mu + [f, \lambda g^e] x^{\mu g^e} + \ldots \\ &\quad + [f, \lambda g^{(f-1)e}] x^{\mu g^{(f-1)e}} \\ &\equiv x^{\lambda+\mu} + x^{\lambda g^e + \mu} + \ldots + x^{\lambda g^{(f-1)e} + \mu} \\ &\quad + x^{(\lambda+\mu) g^e} + x^{\lambda g^{2e} + \mu g^e} + \ldots + x^{\lambda g^{fe} + \mu g^e} + \ldots \\ &\quad + x^{(\lambda+\mu) g^{(f-1)e}} + x^{\lambda g^{fe} + \mu g^{(f-1)e}} + \ldots \\ &\quad + x^{\lambda g^{(2f-2)e} + \mu g^{(f-1)e}}, \end{aligned} \right.$$

et par conséquent

$$(1) \quad [f, \lambda][f, \mu] \equiv [f, \lambda + \mu] + [f, \lambda g^e + \mu] + \ldots + [f, \lambda g^{(f-1)e} + \mu].$$

Quelques-unes des périodes $[f, \lambda + \mu], [f, \lambda g^e + \mu], \ldots$ peuvent être congrues entre elles suivant la fonction U; en outre, si

$$\lambda g^{he} + \mu \equiv 0 \pmod{n},$$

il vient

$$(U) \qquad [f, \lambda g^{ke} + \mu] \equiv f.$$

Donc, en général, on aura

$$(2)\quad (U) \qquad [f, \lambda]\,[f, \mu] \equiv af + b\xi + c\xi_1 + \ldots + l\xi_{e-1},$$

$a, b, c, \ldots, l$ étant des nombres entiers.

En multipliant maintenant les deux termes de la congruence (2) par $[f, \nu]$, on aura, à cause de la même formule (2),

$$(U) \qquad [f, \lambda]\,[f, \mu]\,[f, \nu] \equiv a'f + b'\xi + c'\xi_1 + \ldots + l'\xi_{e-1},$$

$a', b', c', \ldots$ étant des nombres entiers.

Par conséquent, si V désigne une fonction entière à coefficients entiers des périodes $\xi, \xi_1, \ldots, \xi_{e-1}$, on peut toujours supposer

$$(U) \qquad V \equiv A + B\xi + C\xi_1 + \ldots + L\xi_{e-1},$$

A, B, C, ... étant des nombres entiers.

En attribuant dans la congruence (2) aux nombres λ et μ les différentes valeurs, on aura les congruences qui suivent :

$$(3)\ (U)\quad \begin{cases} \xi^2 \equiv sf + m\xi + m_1\xi_1 + \ldots + m_{e-1}\xi_{e-1} \\ \xi\xi_1 \equiv s^{(1)}f + m^{(1)}\xi + m_1^{(1)}\xi_1 + \ldots + m_{e-1}^{(1)}\xi_{e-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \xi\xi_{e-1} \equiv s^{(e-1)}f + m^{(e-1)}\xi + m_1^{(e-1)}\xi_1 + \ldots + m_{e-1}^{(e-1)}\xi_{e-1} \end{cases}$$

$$\begin{array}{lllll} s, & m, & m_1, & \ldots, & m_{e-1}, \\ s^{(1)}, & m^{(1)}, & m_1^{(1)}, & \ldots, & m_{e-1}^{(1)}, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots, & \ldots\ldots \\ s^{(e-1)}, & m^{(e-1)}, & m_1^{(e-1)}, & \ldots, & m_{e-1}^{(e-1)}, \end{array}$$

étant des nombres entiers égaux respectivement à ceux qui figurent dans les formules analogues pour les équations binômes.

De ces congruences on déduit la suivante,

$$(4)\quad (U) \qquad \xi^e + p_1\xi^{e-1} + p_2\xi^{e-2} + \ldots + p_e \equiv 0,$$

$p_1, p_2, \ldots, p_e$ étant des nombres entiers.

Cette congruence, étant convertie en équation, sera identique à celle dont on se sert pour obtenir les périodes à f termes formées avec des racines de l'équation $\frac{x^n-1}{x-1}=0$. La congruence (4) est satisfaite par toutes les périodes $\xi, \xi_1, \ldots, \xi_{e-1}$.

De plus, en procédant comme dans la théorie des équations binômes, on aura la congruence

$$(U) \qquad N\xi_\lambda \equiv a^{(\lambda)} + a_1^{(\lambda)}\xi + a_2^{(\lambda)}\xi^2 + \ldots + a_{e-1}^{(\lambda)}\xi^{e-1},$$

$N, a^{(\lambda)}, a_1^{(\lambda)}, \ldots$ étant des entiers.

19. Maintenant, soient p un nombre premier appartenant à l'exposant h suivant le module n, et f un nombre entier divisible par h ou, en d'autres termes, tel qu'on ait $p^f \equiv 1 \pmod 1$. Nous allons étudier les propriétés des périodes par rapport au module p et une fonction P irréductible et divisant la fonction U suivant ce module.

Il est clair que toutes les congruences précédentes suivant la fonction U auront lieu aussi suivant le module p et la fonction P, car U est divisible suivant ce module par P.

Cela posé, on aura le théorème suivant :

THÉORÈME. — *Les périodes* $\xi, \xi_1, \ldots, \xi_{e-1}$ *sont congrues aux nombres entiers suivant le module p et la fonction* P.

En effet, d'après ce qui précède, on aura

$$\xi \equiv x + x^{g^e} + x^{g^{2e}} + \ldots \pmod{p, P},$$

d'où il résulte

$$\xi^p \equiv (x + x^{g^e} + x^{g^{2e}} + \ldots)^p \equiv x^p + x^{g^e p} + x^{g^{2e} p} + \ldots \pmod{p, P}.$$

D'ailleurs, il suit de la congruence $p^f \equiv 1 \pmod n$ que p est congru suivant le module n au nombre $g^{\lambda e}$, λ désignant un nombre entier, et, par conséquent

$$(U) \qquad \xi^p \equiv x^p + x^{g^e p} + \ldots \equiv \xi.$$

Donc il viendra

$$\xi^p \equiv \xi \pmod{p, P},$$

ou, en d'autres termes, le produit $\xi(\xi-1)\dots(\xi-p+1)$ est divisible par P suivant le module p.

Mais, P étant une fonction irréductible, l'un des facteurs de ce produit est divisible par P suivant le module p, savoir : ξ est congru à l'un des nombres $0, 1, 2, \dots, p-1$ suivant le module p et la fonction P.

Cela aura lieu encore par rapport aux autres périodes $\xi_1, \xi_2, \dots, \xi_{e-1}$.

Soient $u, u_1, \dots, u_{e-1}$ des nombres entiers congrus aux périodes $\xi, \xi_1, \dots, \xi_{e-1}$ suivant le module p et la fonction P.

Ces nombres peuvent être déterminés comme il suit.

Nous avons déduit dans le numéro précédent la congruence

$$(U) \qquad \xi^e + p_1\xi^{e-1} + p_2\xi^{e-2} + \dots + p_e \equiv 0.$$

Les nombres entiers $p_1, p_2, \dots, p_e$ satisfont aux congruences

$$(U) \qquad \begin{cases} -p_1 \equiv \xi + \xi_1 + \dots + \xi_{e-1}, \\ p_2 \equiv \xi\xi_1 + \xi\xi_2 + \dots + \xi_{e-2}\xi_{e-1}, \\ -p_3 \equiv \xi\xi_1\xi_2 + \dots, \\ \dots\dots\dots\dots\dots \end{cases}$$

Ces congruences nous donnent les suivantes :

$$\left.\begin{array}{l} -p_1 \equiv u_1 + u_2 + \dots + u_{e-1}, \\ p_2 \equiv uu_1 + uu_2 + \dots + u_{e-2}u_{e-1}, \\ -p_3 \equiv uu_1u_2 + \dots, \\ \dots\dots\dots\dots\dots \end{array}\right\} \pmod{p}$$

Il résulte de là que la congruence

$$u^e + p_1u^{e-1} + \dots + p_e \equiv 0 \pmod{p}$$

est satisfaite par tous les nombre $u, u_1, \dots, u_{e-1}$.

Ainsi, nous sommes parvenu au théorème de M. Kummer : *L'équation de degré e au moyen de laquelle se trouvent les périodes à f termes formées avec des racines de l'équation* $\frac{x^n-1}{x-1} = 0$, *n étant un nombre*

premier, a e racines égales ou inégales, si on la considère comme une congruence suivant le module p tel qu'on ait $p^f \equiv 1 \pmod{n}$.

Des congruences (3) du numéro précédent on déduit les suivantes :

$$\left.\begin{array}{lllll} u^2 & \equiv sf & + mu & + m_1 u_1 & + \ldots + m_{e-1} u_{e+1} \\ uu_1 & \equiv s^{(1)} f & + m^{(1)} u & + m_1^{(1)} u & + \ldots + m_{e-1}^{(1)} u_{e-1} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ uu_{e-1} & \equiv s^{(e-1)} f & + m^{(e-1)} u & + m_1^{(e-1)} u_1 & + \ldots + m_{e-1}^{(e-1)} u_{e-1} \end{array}\right\} \pmod{p}$$

Il suit de la définition des nombres $u, u_1, \ldots, u_{e-1}$ que toute fonction entière $\varphi(\xi, \xi_1, \ldots, \xi_{e-1})$ des périodes $\xi, \xi_1, \ldots, \xi_{e-1}$, à coefficients entiers, satisfait à la congruence

$$\varphi(\xi, \xi_1, \ldots, \xi_{e-1}) \equiv \varphi(u, u_1, \ldots, u_{e-1}) \pmod{p, \mathrm{P}}.$$

Donc $\varphi(\xi, \xi_1, \ldots, \xi_{e-1})$ sera divisible par P suivant le module p si l'on a

$$\varphi(u, u_1, \ldots, u_{e-1}) \equiv 0 \pmod{p}.$$

20. Maintenant nous allons voir comment on obtient les facteurs irréductibles de la fonction U suivant le module premier p.

Supposons que p appartienne à l'exposant h par rapport au module n, et soit $n - 1 = kh$. Désignons par

$$(1)\ (\mathrm{U}) \quad \left\{\begin{array}{llll} [h, 1] & = \eta & \equiv x & + x^{s^k} + x^{s^{2k}} + \ldots + x^{s^{(h-1)k}} \\ [h, g] & = \eta_1 & \equiv x^s & + x^{s^{k+1}} + x^{s^{2k+1}} + \ldots + x^{s^{(h-1)k+1}} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ [h, g^{k-1}] & = \eta_{k-1} & \equiv x^{s^{k-1}} & + x^{s^{2k-1}} + x^{s^{3k-1}} + \ldots + x^{s^{hk-1}} \end{array}\right.$$

les périodes à h termes. Soit encore P un des facteurs irréductibles de la fonction U suivant le module p.

D'après ce qui précède, les périodes $\eta, \eta_1, \ldots, \eta_{k-1}$ sont congrues suivant la fonction P et le module p aux nombres entiers

$$\nu, \nu_1, \ldots, \nu_{k-1},$$

satisfaisant à la congruence

$$\nu^k + q_1 \nu^{k-1} + q_2 \nu^{k-2} + \ldots \equiv 0 \pmod{q},$$

$q_1, q_2, \ldots, q_k$ étant des nombres entiers.

Maintenant nous allons former la congruence de degré hk suivant le

module p et la fonction P qui aura pour ses racines les fonctions x, x^{s^k}, $x^{s^{2k}}$, ..., $x^{s^{(h-1)k}}$. Cette congruence peut être représentée sous la forme

$$(2)\quad (X-x)(X-x^{s^k})(X-x^{s^{2k}})\ldots(X-x^{s^{(h-1)k}}) \equiv 0 \pmod{p, P}.$$

Afin de déterminer les coefficients de cette congruence, on cherche d'abord les sommes de puissances semblables des racines.

En vertu des formules (1) on aura

$$\left.\begin{aligned} &x + x^{s^k} + x^{s^{2k}} + \ldots + x^{s^{(h-1)k}} \equiv [h, 1] \\ &x^2 + x^{2s^k} + x^{2s^{2k}} + \ldots + x^{2s^{(h-1)k}} \equiv [h, 2] \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &x^k + x^{ks^k} + x^{ks^{2k}} + \ldots + x^{ks^{(h-1)k}} \equiv [h, k] \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \pmod{p, P}.$$

Les périodes $[h, 1]$, $[h, 2]$, ..., comme nous avons vu plus haut, sont congrues suivant le module p et la fonction P aux nombres v, v_1, ..., v_{k-1}. Comme nous avons désigné par P un facteur irréductible quelconque de U, le nombre v, congru à la première période $[h, 1]$, peut être choisi arbitrairement dans la suite v, v_1, ..., v_{k-1}. Le nombre v étant déterminé, on cherche le nombre v_i congru à la période $[h, g^i]$ au moyen de la liaison qui existe entre les périodes; v_i dépend de v tout à fait de la même manière, comme $[h, g^i]$ de $[h, 1]$.

Ainsi on pourra toujours déterminer les sommes de puissances semblables de racines de la congruence (2). Soit

$$X^h + l_1 X^{h-1} + \ldots + l_h \equiv 0 \pmod{p, P}$$

cette congruence, l_1, l_2, ..., l_h étant des nombres entiers. En remarquant que cette congruence est satisfaite par la fonction $X = x$, on voit que la fonction $x^h + l_1 x^{h-1} + l_2 x^{h-2} + \ldots + l_h$ est divisible par P suivant le module p.

P étant une fonction irréductible de degré h, on peut toujours prendre

$$P = x^h + l_1 x^{h-1} + l_2 x^{h-2} + \ldots + l_h.$$

En remplaçant v par d'autres valeurs v_1, v_2, ..., v_{k-1}, on aura les autres fonctions P.

(A suivre.)