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. 129-166.
<http://www.numdam.org/item?id=JMPA_1880_3_6__129_0>

Sur la théorie des nombres complexes

[SUITE];

PAR M. G. ZOLOTAREFF.

21. Maintenant nous allons considérer les nombres complexes qui dépendent des racines de l'équation

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

où n est un nombre premier impair.

Nous allons voir que les théorèmes de M. Kummer concernant ces nombres se déduisent très facilement de la théorie générale des nombres complexes exposée plus haut.

Soit α une racine de l'équation (1). Toutes les racines de cette équation sont alors

$$\alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}. \tag{2}$$

Soit encore p un nombre premier impair. Supposons d'abord $p = n$. La fonction $\frac{x^n - 1}{x - 1}$ est congrue à $(x - 1)^{n-1}$, suivant ce module.

Le nombre n est effectivement une puissance $(n - 1)^{\text{ième}}$ d'un nombre complexe. Nous avons

$$n = (1 - \alpha)(1 - \alpha^2)\ldots(1 - \alpha^{n-1}) = (1 - \alpha)^{n-1} \frac{1 - \alpha^2}{1 - \alpha} \frac{1 - \alpha^3}{1 - \alpha} \cdots \frac{1 - \alpha^{n-1}}{1 - \alpha},$$

et le produit $\frac{1-\alpha^2}{1-\alpha}\frac{1-\alpha^3}{1-\alpha}\cdots\frac{1-\alpha^{n-1}}{1-\alpha}$ est une unité complexe, comme il est facile de le voir.

Supposons maintenant que p ne soit pas égal à n et qu'il appartienne à l'exposant h suivant le module n, en sorte que

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

Désignant le nombre $\frac{n-1}{h}$ par k et une racine primitive quelconque de n par g, toutes les racines (2) se laissent distribuer en périodes :

$$\begin{aligned}
\beta &= \alpha + \alpha^{g^k} + \alpha^{g^{2k}} + \ldots + \alpha^{g^{(h-1)k}},\\
\beta_1 &= \alpha^g + \alpha^{g^{k+1}} + \alpha^{g^{2k+1}} + \ldots + \alpha^{g^{(h-1)k+1}},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
\beta_{k-1} &= \alpha^{g^{k-1}} + \alpha^{g^{2k-1}} + \alpha^{g^{3k-1}} + \ldots + \alpha^{g^{hk-1}}.
\end{aligned}$$

En vertu des liaisons connues entre les périodes, toute fonction rationnelle et entière à coefficients entiers des périodes peut être représentée sous la forme

$$a_0\beta + a_1\beta_1 + \ldots + a_{k-1}\beta_{k-1},$$

$a_0, a_1, \ldots, a_{k-1}$ étant des nombres entiers.

Cette fonction peut être considérée comme fonction d'une seule période β, et, par conséquent, on la désigne par $F(\beta)$.

Nous avons démontré que la fonction $\frac{x^n-1}{x-1}$ suivant le module p a la forme

$$\frac{x^n-1}{x-1} = PP_1\ldots P_{k-1} + p\,\psi(x), \tag{3}$$

$P, P_1, \ldots, P_{k-1}$ étant des fonctions irréductibles suivant le module p du degré h, et $\psi(x)$ un polynôme à coefficients entiers.

Nous avons vu encore que, en remplaçant dans les expressions des périodes α par x, les périodes obtenues $\eta, \eta_1, \ldots, \eta_{k-1}$ seront congrues suivant le module p et suivant chacune des fonctions $P, P_1, \ldots, P_{k-1}$ à des nombres constants.

Supposons que, suivant le module p et la fonction P, ces périodes soient congrues aux nombres $u, u_1, \ldots, u_{k-1}$. Alors, en remplaçant la fonction P par une autre de la suite $P_1, P_2, \ldots, P_{k-1}$, les nombres $u, u_1, \ldots, u_{k-1}$ seront permutés cycliquement, en sorte que les périodes seront congrues respectivement à $u_r, u_{r+1}, \ldots, u_{r+k-1}$, où l'on suppose $u_{\lambda+sk} = u_\lambda$.

Nous désignerons par $F(u)$ et $F(u_r)$ les valeurs des fonctions

$$F(\eta) = a_0\eta + a_1\eta_1 + \ldots + a_{k-1}\eta_{k-1},$$
$$F(\eta_r) = a_0\eta_r + a_1\eta_{r+1} + \ldots + a_{r-1}\eta_{r+k-1}$$

quand $\eta, \eta_1, \ldots, \eta_{k-1}$ seront remplacés respectivement par $u, u_1, \ldots, u_{k-1}$.

On voit, d'après l'équation (3), que le nombre p contient k facteurs idéaux appartenant respectivement aux fonctions $P, P_1, \ldots, P_{k-1}$.

Faisons voir maintenant comment on peut reconnaître si un nombre complexe quelconque $\varphi(\alpha)$ contient le facteur idéal appartenant à la fonction P.

Il est connu que α est une racine de l'équation

$$\alpha^k + A_1\alpha^{k-1} + A_2\alpha^{k-2} + \ldots = 0,$$

où $A_1, A_2, \ldots$ sont des fonctions des périodes $\beta, \beta_1, \ldots, \beta_{k-1}$; par conséquent, tout nombre complexe $\varphi(\alpha)$ peut être représenté sous la forme

$$\varphi(\alpha) = \varphi_1(\beta) + \varphi_2(\beta)\alpha + \varphi_3(\beta)\alpha^2 + \ldots + \varphi_k(\beta)\alpha^{k-1},$$

$\varphi_1(\beta), \varphi_2(\beta), \ldots, \varphi_k(\beta)$ étant des fonctions rationnelles entières des périodes $\beta, \beta_1, \ldots, \beta_{k-1}$.

Pour que le nombre $\varphi(\alpha)$ contienne le facteur idéal de p appartenant à la fonction P, il est nécessaire et il suffit que la fonction

$$\varphi(x) = \varphi_1(\eta) + \varphi_2(\eta)x + \varphi_3(\eta)x^2 + \ldots + \varphi_k(\eta)x^{k-1},$$

déduite de $\varphi(\alpha)$ en remplaçant α par x, soit divisible par P suivant le module p.

En vertu des propriétés des périodes, nous pouvons remplacer η,

$\eta_1, \ldots, \eta_{k-1}$ respectivement par les nombres entiers $u, u_1, \ldots, u_{k-1}$, et par conséquent la fonction $\varphi(x)$ par la suivante :

$$\varphi_1(u) + \varphi_2(u)x + \varphi_3(u)x^2 + \ldots + \varphi_h(u)x^{h-1}.$$

Cette dernière ne peut être divisible suivant le module p par la fonction P du degré h que dans le cas où l'on a

$$\varphi_1(u) \equiv 0, \ \varphi_2(u) \equiv 0, \ \ldots, \ \varphi_h(u) \equiv 0 \pmod{p}.$$

Ces congruences constituent les conditions données par M. Kummer pour que $\varphi(\alpha)$ contienne le facteur de p appartenant à la fonction P.

Il est aussi facile d'exprimer les conditions pour que le nombre complexe $\varphi(\alpha)$ contienne ce facteur λ fois.

En vertu de ce que nous avons dit au n° 7, dans ce cas aura lieu la congruence

$$(3) \qquad \varphi(x)\,\mathrm{P}(\mathrm{P}_1\mathrm{P}_2\ldots\mathrm{P}_{k-1})^{\lambda+1} \equiv 0 \quad \left(\mathrm{mod.}\ p^{\lambda+1}, \frac{x^n-1}{x-1}\right),$$

et cette autre,

$$(4) \qquad \varphi(x)\,\mathrm{P}(\mathrm{P}_1\mathrm{P}_2\ldots\mathrm{P}_{k-1})^{\lambda+2} \equiv 0 \quad \left(\mathrm{mod.}\ p^{\lambda+2}, \frac{x^n-1}{x-1}\right),$$

ne sera pas satisfaite.

Or on a

$$\frac{x^n-1}{x-1} = \mathrm{P}\,\mathrm{P}_1\ldots\mathrm{P}_{k-1} + p\,\psi(x),$$

où $\psi(x)$ peut être regardé comme non divisible par aucune des fonctions P, $\mathrm{P}_1, \ldots, \mathrm{P}_{k-1}$; par conséquent, on peut représenter les congruences (3) et (4) sous la forme

$$-\psi(x)\varphi(x)(\mathrm{P}_1\mathrm{P}_2\ldots\mathrm{P}_{k-1})^{\lambda} \equiv 0 \quad \left(\mathrm{mod.}\ p^{\lambda}, \frac{x^n-1}{x-1}\right),$$

$$-\psi(x)\varphi(x)(\mathrm{P}_1\mathrm{P}_2\ldots\mathrm{P}_{k-1})^{\lambda+1} \equiv 0 \quad \left(\mathrm{mod.}\ p^{\lambda+1}, \frac{x^n-1}{x-1}\right).$$

En remarquant que $\psi(x)$ n'est divisible par aucune des fonctions P,

$P_1, \ldots, P_{k-1}$, on peut remplacer ces congruences par les suivantes :

$$(I) \qquad \varphi(x)W^{\lambda} \equiv 0 \quad \left(\text{mod. } p^{\lambda}, \frac{x^n-1}{x-1}\right),$$

$$(II) \qquad \varphi(x)W^{\lambda+1} \equiv 0 \quad \left(\text{mod. } p^{\lambda+1}, \frac{x^n-1}{x-1}\right),$$

où $W = P_1 P_2 \ldots P_{k-1}$.

Ainsi, pour que le nombre complexe $\varphi(\alpha)$ contienne λ fois le facteur de p qui appartient à la fonction P, il est nécessaire et il suffit que la congruence (I) ait lieu et que la congruence (II) ne soit pas satisfaite. Il est facile de transformer ces conditions dans celles de M. Kummer. Nous allons chercher pour cela une fonction des périodes $\beta, \beta_1, \ldots, \beta_{k-1}$ qui ne contient qu'un facteur idéal de p appartenant, par exemple, à la fonction P et seulement une fois.

Dans le n° **20**, nous avons obtenu une congruence suivant le module p et la fonction P, à laquelle satisfont les fonctions x, x^{s^k}, $x^{s^{2k}}$, $\ldots$, $x^{s^{(h-1)k}}$. Cette congruence est de la forme

$$x^h + l_1 x^{h-1} + \ldots + l_h \equiv 0 \quad (\text{mod. } p, P),$$

$l_1, l_2, \ldots, l_h$ étant des entiers. Comme P est une fonction irréductible suivant le module p du degré h, on aura

$$P \equiv x^h + l_1 x^{h-1} + \ldots + l_h \quad (\text{mod. } p).$$

Il suit de là qu'en remplaçant, dans P, x successivement par x^{s^k}, $x^{s^{2k}}$, $\ldots$, $x^{s^{(h-1)k}}$, on obtiendra des fonctions divisibles par P suivant le module p. Il est évident que la même circonstance aura lieu relativement aux autres fonctions $P_1, P_2, \ldots, P_{k-1}$.

Soient maintenant A et B deux fonctions entières à coefficients entiers qui satisfont à la congruence

$$(5) \qquad AP - BW \equiv x + x^s + x^{s^2} + \ldots + x^{s^{k-1}} \quad (\text{mod. } p),$$

où, comme précédemment, $W = P_1 P_2 \ldots P_{k-1}$.

Comme P et W n'ont point de facteurs communs suivant le module p, on trouvera toujours des fonctions A et B qui satisferont à la

congruence (5). Cette dernière équivaut à l'équation

$$AP - BW = x + x^g + x^{g^2} + \ldots + x^{g^{k-1}} + pf(x),$$

$f(x)$ étant un polynôme à coefficients entiers.

Remplaçons dans cette équation x successivement par x^{g^k}, $x^{g^{2k}}$, ..., $x^{g^{(k-1)k}}$, et désignons par

$$\begin{aligned} &A', A'', \ldots, A^{(k-1)}, \\ &B', B'', \ldots, B^{(k-1)}, \\ &P', P'', \ldots, P^{(k-1)}, \\ &W', W'', \ldots, W^{(k-1)} \end{aligned}$$

les valeurs des fonctions A, B, P, W qui correspondent à ces remplacements; nous aurons les équations

$$\begin{aligned} A'P' - B'W' &= x^{g^k} + x^{g^{k+1}} + x^{g^{k+2}} + \ldots + x^{g^{2k-1}} + pf(x^{g^k}), \\ A''P'' - B''W'' &= x^{g^{2k}} + x^{g^{2k+1}} + \ldots + x^{g^{3k-1}} + pf(x^{g^{2k}}), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

En faisant donc

$$\begin{aligned} F(\eta) &= AP + A'P' + A''P'' + \ldots + A^{(k-1)}P^{(k-1)}, \\ F_1(\eta) &= BW + B'W' + B''W'' + \ldots + B^{(k-1)}W^{(k-1)}, \end{aligned}$$

où les seconds termes de ces équations sont évidemment des fonctions des périodes $\eta, \eta_1, \ldots, \eta_{k-1}$, il suit des équations précédentes

$$F(\eta) - F_1(\eta) \equiv -1 \quad \left(\text{mod. } p, \frac{x^n - 1}{x - 1}\right). \tag{6}$$

Nous avons vu que P', P'', ... sont divisibles par P suivant le module p; de même W', W'', ... sont divisibles par W suivant ce module; par suite, les fonctions $F(\eta)$ et $F_1(\eta)$ sont divisibles respectivement par P et W suivant le module p.

On voit par la congruence (6) que $F(\eta)$ n'est divisible suivant le module p par aucune des fonctions $P_1, P_2, \ldots, P_{k-1}$. Par conséquent, le nombre complexe $F(\beta)$ contient seulement le facteur idéal de p

appartenant à la fonction P. Si ce facteur est contenu dans $F(\beta)$ plusieurs fois, nous allons prendre le nombre complexe $F(\beta)+p$. Il est évident que ce nombre ne contient de tous les facteurs idéaux de p que celui qui appartient à la fonction P; de plus, comme p contient ce facteur au premier degré et $F(\beta)$ à un degré supérieur, la somme $F(\beta)+p$ contiendra le même facteur une seule fois. Cela se vérifie au moyen des congruences (I), (II).

Ainsi, on trouvera toujours un nombre complexe $\Phi(\beta)$ qui contiendra un seul facteur idéal de p, ou, ce qui est la même chose, on trouvera une fonction des périodes $\Phi(\eta)$, qui, suivant le module p, est représentée sous la forme

$$\Phi(\eta)\equiv P\,\varpi(x) \pmod{p},$$

$\varpi(x)$ étant un polynôme non divisible suivant ce module par aucune des fonctions $P, P_1, \ldots, P_{k-1}$.

Soit maintenant

$$\Psi(\eta)=\Phi(\eta_1)\Phi(\eta_2)\ldots\Phi(\eta_{k-1}).$$

Il suit de ce qui a été dit que $\Psi(\eta)$ suivant le module p est de la forme

$$\Psi(\eta)\equiv W\,\Omega(x) \pmod{p},$$

$\Omega(x)$ n'étant divisible par aucune des fonctions $P, P_1, \ldots, P_{k-1}$.

En vertu du n° 8, on peut remplacer, dans les congruences (I), (II), W par $W\,\Omega(x)$, et l'on aura, au lieu de ces congruences,

$$\varphi(x)[\Psi(\eta)]^{\lambda}\equiv 0 \quad \left(\text{mod. } p^{\lambda}, \frac{x^n-1}{x-1}\right),$$

$$\varphi(x)[\Psi(\eta)]^{\lambda+1}\equiv 0 \quad \left(\text{mod. } p^{\lambda+1}, \frac{x^n-1}{x-1}\right).$$

Ainsi, pour que le nombre complexe $\varphi(\alpha)$ contienne λ fois le facteur de p appartenant à la fonction P, il est nécessaire et il suffit que le nombre complexe $\varphi(\alpha)[\Psi(\beta)]^{\lambda}$ soit divisible par p^{λ} et que le nombre complexe $\varphi(\alpha)[\Psi(\beta)]^{\lambda+1}$ ne soit point divisible par $p^{\lambda+1}$. C'est dans cette forme que ces conditions sont données par M. Kummer.

Remarquons enfin qu'en appliquant au cas considéré, où les fonc-

tions P, P_1, ..., P_{k-1} sont toutes du degré h, ce qui a été démontré au n° **11**, on aura ce théorème :

Si la norme du nombre complexe $\varphi(\alpha)$ est divisible par un nombre premier p appartenant à l'exposant h suivant le module n, elle est divisible par p^h.

22. Jusqu'ici nous avons exclu de notre recherche (n° **5**) les équations

$$F(x) = X^n + a_1 X^{n-2} + a_2 X^{n-4} + \ldots + a_n = 0 \tag{1}$$

telles que la fonction $F(x)$ suivant le module premier p ait la forme

$$F(x) = V^m V_1^{m_1} \ldots V_s^{m_s} + p\,\varphi(x), \tag{2}$$

le polynôme $\varphi(x)$ étant divisible suivant ce module par l'une des fonctions V, dont l'exposant m surpasse l'unité.

Par le même numéro, on sait qu'il n'y a qu'un nombre fini de modules tels que p. Quant aux autres nombres premiers, leur décomposition en facteurs complexes qui dépendent des racines de l'équation (1) s'opère d'après les principes exposés plus haut.

Il nous reste maintenant à considérer les modules exceptionnels suivant lesquels la fonction $F(x)$ peut être présentée sous la forme (2). D'abord nous allons établir que la propriété des nombres complexes démontrée dans le n° **12** (corollaire I), savoir, *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*

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

$q_1, q_2, \ldots, q_n$ *étant des nombres entiers*, cesse d'avoir lieu s'il y a des modules exceptionnels.

En effet, supposons dans l'équation (2), pour fixer les idées, $m > 1$ et $\varphi(x)$ divisible par V suivant le module p.

En désignant par ζ le nombre complexe

$$\frac{V^{m-1} V_1^{m_1} \ldots V_s^{m_s}}{p},$$

nous allons démontrer qu'il satisfait à l'équation

$$(\alpha) \qquad \zeta^N + q_1\zeta^{N-1} + q_2\zeta^{N-2} + \ldots + q_N = 0,$$

à coefficients entiers.

En effet, l'équation (2) nous donne

$$(3) \qquad V^m V_1^{m_1} \ldots V_s^{m_s} = -p\varphi(x),$$

où $\varphi(x)$, en vertu de la supposition, est de la forme

$$\varphi(x) = AV + pB,$$

A et B étant des fonctions entières à coefficients entiers.

En multipliant les deux membres de l'équation (3) par $V^{m-2} V_1^{m} \ldots V_s^{m_s}$, on aura

$$V^{2m-2} V_1^{2m_1} \ldots V_s^{2m_s} = -pAV^{m-1} V_1^{m_1} \ldots V_s^{m_s} - p^2 BV^{m-2} V_1^{m_1} \ldots V_s^{m_s}$$

ou, ce qui revient au même,

$$\zeta^2 + A\zeta + BV^{m-2} V_1^{m_1} \ldots V_s^{m_s} = 0.$$

En remplaçant successivement, dans les coefficients A et BV^{m-2}, $V_1^{m_1} \ldots V_s^{m_s}$ de cette équation, x par toutes les racines de l'équation (1), et en multipliant les résultats, on aura une équation de la forme (α). A cause de cette propriété des modules exceptionnels, il nous faut généraliser la notion des nombres complexes entiers.

Chaque nombre complexe

$$y = a + bx + \ldots + lx^{n-1},$$

$a, b, \ldots, l$ étant des nombres rationnels, sera nommé nombre entier s'il satisfait à l'équation de la forme (α). D'ailleurs, y étant une fonction rationnelle à coefficients entiers, le degré de l'équation peut être évidemment supposé égal à n, savoir au degré de l'équation donnée $F(x) = 0$.

Le produit $\gamma_0\gamma_1\ldots\gamma_{n-1}$, où

$$\begin{aligned}\gamma_0 &= a + bx_0 + \ldots + lx_0^{n-1},\\ \gamma_1 &= a + bx_1 + \ldots + lx_1^{n-1},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ \gamma_{n-1} &= a + bx_{n-1} + \ldots + lx_{n-1}^{n-1},\end{aligned}$$

sera dit la *norme* du nombre complexe γ. Ce produit est évidemment un nombre entier ordinaire, et nous le désignerons toujours par $\mathrm{N}(\gamma)$.

Remarque. — Supposons que γ soit une fonction rationnelle à coefficients entiers d'une racine de l'équation $\mathrm{F}(x) = 0$ et, de plus, qu'il satisfasse à l'équation

$$\gamma^\mu + \mathrm{A}_1\gamma^{\mu-1} + \mathrm{A}_2\gamma^{\mu-2} + \ldots + \mathrm{A}_\mu = 0,$$

$\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_\mu$ étant des nombres complexes entiers. Alors γ sera un nombre entier.

En effet, soient

$$\begin{aligned}&\mathrm{A}'_1,\ \mathrm{A}'_2,\ \ldots,\ \mathrm{A}'_\mu,\\ &\mathrm{A}''_1,\ \mathrm{A}''_2,\ \ldots,\ \mathrm{A}''_\mu,\\ &\ldots\ldots\ldots\ldots\end{aligned}$$

les valeurs des coefficients $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_\mu$ lorsqu'on y remplace la racine de l'équation (1) par les autres racines de la même équation.

En multipliant les résultats

$$\begin{aligned}&\gamma^\mu + \mathrm{A}_1\gamma^{\mu-1} + \mathrm{A}_2\gamma^{\mu-2} + \ldots + \mathrm{A}_\mu,\\ &\gamma^\mu + \mathrm{A}'_1\gamma^{\mu-1} + \mathrm{A}'_2\gamma^{\mu-2} + \ldots + \mathrm{A}'_\mu,\\ &\gamma^\mu + \mathrm{A}''_1\gamma^{\mu-1} + \mathrm{A}''_2\gamma^{\mu-2} + \ldots + \mathrm{A}''_\mu,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\end{aligned}$$

on aura une équation de la forme

$$\gamma^{\mu n} + s_1\gamma^{\mu n-1} + s_2\gamma^{\mu n-2} + \ldots = 0,$$

$s_1, s_2, \ldots$ étant des entiers ordinaires. Donc γ est un nombre complexe entier.

23. Soit ξ un des nombres entiers complexes satisfaisant à l'équation

$$\xi^n + q_1\xi^{n-1} + q_2\xi^{n-2} + \ldots + q_n = 0,$$

$q_1, q_2, \ldots, q_n$ étant des entiers ordinaires. Il peut être présenté sous la forme

$$\xi = \frac{\alpha + \beta x + \gamma x^2 + \ldots + \lambda x^{n-1}}{N},$$

$\alpha, \beta, \gamma, \ldots, \lambda$, N étant des entiers qui n'ont pas de diviseurs communs.

Remarquons, en premier lieu, que N n'est divisible que par les modules exceptionnels.

En effet, soit p un autre nombre premier quelconque et supposons qu'il entre comme facteur dans N. Alors on en conclut, d'après le n° **15** (corollaire I), que tous les nombres $\alpha, \beta, \gamma, \ldots, \lambda$ sont divisibles par p, ce qui est contre l'hypothèse.

En second lieu, nous ferons voir que le discriminant Δ d'une équation donnée $F(x) = 0$ est divisible par N^2.

Soit, en effet,

$$N = p^{\mu} p_1^{\mu_1} p_2^{\mu_2} \ldots,$$

$p, p_1, p_2, \ldots$ étant des facteurs premiers et différents du nombre N.

La proposition dont il s'agit sera démontrée si l'on fait voir que le discriminant Δ est divisible par $p^{2\mu}$, par $p_1^{2\mu_1}, \ldots$.

A cet effet, considérons le nombre complexe entier

$$\eta = p_1^{\mu_1} p_2^{\mu_2} \ldots \xi = \frac{\alpha + \beta x + \gamma x^2 + \ldots + \lambda x^{n-1}}{p^{\mu}}.$$

Par hypothèse, un des nombres $\alpha, \beta, \gamma, \ldots, \lambda$ au moins n'est pas divisible par p. Désignons par εx^{μ} un des termes de la fonction

$$\alpha + \beta x + \gamma x^2 + \ldots + \lambda x^{n-1},$$

dont le coefficient ε n'est pas divisible par p.

De plus, soit E une racine de la congruence

$$\varepsilon E \equiv 1 \pmod{p^{\mu}}.$$

Donc

$$\varepsilon \mathrm{E} = 1 + p^{\mu} f,$$

f étant un nombre entier.

Nous considérons encore un nombre complexe

$$\zeta(x) = \mathrm{E}\eta - f x^{\mu} = \frac{x^{\mu} + \mathrm{E}\alpha + \mathrm{E}\beta x + \dots}{p^{\mu}}.$$

En premier lieu, il est aisé de voir que le déterminant

$$\mathrm{A} = \begin{vmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{\mu-1} & \zeta(x_0) & x_0^{\mu+1} & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{\mu-1} & \zeta(x_1) & x_1^{\mu+1} & \dots & x_1^{n-1} \\ \cdot & \dots & \dots & \dots & \dots\dots & \dots\dots & \dots\dots & \dots & \dots\dots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{\mu-1} & \zeta(x_{n-1}) & x_{n-1}^{\mu+1} & \dots & x_{n-1}^{n-1} \end{vmatrix}^2$$

est un nombre entier, car, d'une part, ce déterminant est évidemment une fonction symétrique des racines $x_0, x_1, \dots, x_{n-1}$, et par conséquent il est égal au nombre rationnel ordinaire; d'autre part, étant une fonction rationnelle des racines des équations

$$\mathrm{F}(\mathrm{X}) = \mathrm{X}^n + a_1 \mathrm{X}^{n-1} + a_2 \mathrm{X}^{n-2} + \dots = 0$$

et

$$\xi^n + q_1 \xi^{n-1} + q_2 \xi^{n-2} + \dots + q_n = 0,$$

il satisfait encore à une équation de la forme

$$\mathrm{A}^m + h_1 \mathrm{A}^{m-1} + h_2 \mathrm{A}^{m-2} + \dots = 0,$$

$h_1, h_2, \dots$ étant des entiers. Il suit de là que A est un nombre entier.

En second lieu, en remplaçant $\zeta(x_0), \zeta(x_1), \dots$ par leurs valeurs, on aura

$$\mathrm{A} = \frac{\Delta}{p^{2\mu}}.$$

Donc Δ est divisible par $p^{2\mu}$. On s'assure de la même manière que Δ est divisible par $p_1^{2\mu_1}, p_2^{2\mu_2}, \dots$.

D'où il suit que N ne surpasse pas $\sqrt{\Delta}$.

24. La notion des nombres complexes entiers étant établie, nous indiquons comment on doit concevoir leur division.

Un nombre complexe entier ξ sera dit divisible par un autre nombre α, si le quotient est encore un nombre entier.

Cela posé, nous allons démontrer une proposition qui nous sera utile dans ce qui suit.

Soient p un nombre premier ordinaire et α un nombre complexe dont la norme est divisible par p. Supposons $N(\alpha) = p^\lambda b$, b étant un entier non divisible par p.

Maintenant, s'il existe un autre nombre complexe ξ qui, étant multiplié par un nombre quelconque ordinaire H, premier avec p, devienne divisible par α, le produit $b\xi$ le sera aussi.

En effet, H étant premier avec p, on peut toujours trouver deux nombres entiers P et Q tels qu'ils satisfassent à l'équation

$$PH - p^\lambda Q = 1.$$

De ce que le nombre $H\xi$ est divisible par α il suit que le nombre $\frac{HP\xi}{\alpha} = \frac{\xi}{\alpha} + \frac{p^\lambda Q\xi}{\alpha}$ et par conséquent le nombre $\frac{b\xi}{\alpha} + \frac{p^\lambda bQ\xi}{\alpha}$ sont des nombres entiers. Mais, en désignant par α', α'', ..., $\alpha^{(n-1)}$ les valeurs de α quand on y remplace x par les autres racines de l'équation (1) du n° **22**, on aura

$$\frac{p^\lambda bQ\xi}{\alpha} = \alpha'\alpha''\ldots\alpha^{(n-1)}Q\xi.$$

Or, $\frac{p^\lambda bQ\xi}{\alpha}$ est un nombre entier : donc $\frac{b\xi}{\alpha}$ le sera

25. Passons maintenant à la classification des nombres entiers par rapport au module premier p.

Remarquons que chaque nombre complexe entier est congru suivant un module p^m, m étant un exposant quelconque, bien entendu, positif et entier, au nombre $\frac{a + bx + cx^2 + \ldots + lx^{n-1}}{p^\mu}$, l'entier μ pouvant être égal à zéro.

En effet, soit $\zeta = \frac{A + Bx + Cx^2 + \ldots + Lx^{n-1}}{N}$ un nombre entier quel-

conque dont le dénominateur N se mettra toujours sous la forme

$$\mathrm{N} = p^{\mu}\mathrm{M},$$

M n'étant pas divisible par p.

Cela posé, on pourra trouver les entiers P et Q tels qu'on ait

$$\mathrm{PM} - \mathrm{Q}p^{m} = 1,$$

et, par conséquent, le nombre ζ pourra être présenté sous la forme

$$\zeta = \frac{\mathrm{P}(\mathrm{A} + \mathrm{B}x + \mathrm{C}x^2 + \ldots + \mathrm{L}x^{n-1})}{p^{\mu}} - \mathrm{Q}p^{m}\zeta.$$

Donc

$$\zeta \equiv \frac{\mathrm{P}(\mathrm{A} + \mathrm{B}x + \mathrm{C}x^2 + \ldots + \mathrm{L}x^{n-1})}{p^{\mu}} \pmod{p^{m}}.$$

Ainsi, pour faire une classification des nombres entiers suivant un module premier p, il suffit de considérer les nombres entiers

$$\alpha + \beta x + \gamma x^2 + \ldots + \lambda x^{n-1},$$
$$\frac{\alpha' + \beta' x + \gamma' x^2 + \ldots + \lambda' x^{n-1}}{p},$$
$$\frac{\alpha'' + \beta'' x + \gamma'' x^2 + \ldots + \lambda'' x^{n-1}}{p^2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Nous avons vu plus haut que les exposants du nombre p qui figure dans les dénominateurs ne surpassent pas la limite connue (n° **23**).

Considérons d'abord les nombres complexes entiers de la forme

$$\zeta = \frac{\alpha + \beta x + \gamma x^2 + \ldots + \lambda x^{n-1}}{p}.$$

On peut évidemment poser

$$\zeta = \frac{\varphi(x)}{p} + a + bx + cx^2 + \ldots + lx^{n-1},$$

$a, b, c, \ldots$ étant des entiers et $\varphi(x)$ une fonction entière dans laquelle

les coefficients des diverses puissances de x sont rabaissés au-dessous de p.

De tous les nombres complexes entiers $\frac{\varphi(x)}{p}$ nous choisirons celui pour lequel $\varphi(x)$ sera du moindre degré possible. Le coefficient de la plus haute puissance de x dans $\varphi(x)$ peut toujours être supposé égal à l'unité.

En effet, soit

$$\varphi(x) = A + Bx + Cx^2 + \ldots + Lx^\mu.$$

Si le coefficient L est différent de l'unité, on prendra un nombre g tel que l'on ait

$$gL \equiv 1 \pmod{p}.$$

Alors considérons le nombre complexe entier

$$g\frac{\varphi(x)}{p} = \frac{\alpha + \beta x + \gamma x^2 + \ldots + x^\mu}{p} + \alpha' + \beta' x + \ldots + \lambda' x^\mu,$$

et prenons, au lieu de $\frac{\varphi(x)}{p}$, le nombre complexe

$$\frac{\alpha + \beta x + \gamma x^2 + \ldots + x^\mu}{p},$$

ayant la forme désirée.

Cela posé, nous ferons voir qu'il n'existe qu'un seul nombre complexe entier

$$\frac{\alpha + \beta x + \gamma x^2 + x^\mu}{p}$$

pour lequel le degré μ sera le moindre possible.

En effet, soient au contraire

$$\frac{\varphi(x)}{p} = \frac{\alpha + \beta x + \gamma x^2 + \ldots + x^\mu}{p}$$

et

$$\frac{\varphi_1(x)}{p} = \frac{\alpha_1 + \beta_1 x + \gamma_1 x^2 + x^\mu}{p}$$

deux nombres entiers distincts et tels que le degré μ ait la moindre

valeur possible. Alors la différence $\frac{\varphi(x)-\varphi_1(x)}{p}$ sera encore un nombre complexe entier dont le numérateur est du degré inférieur à μ, ce qui est contre l'hypothèse. Donc il n'existe qu'un seul nombre complexe $\frac{\varphi(x)}{p}$ de la forme indiquée.

Maintenant nous ferons voir que tout nombre complexe entier de la forme

$$\frac{a+bx+cx^2+\ldots+lx^{n-1}}{p}$$

sera aussi de la forme

$$A\frac{\varphi(x)}{p}+B,$$

A et B étant deux polynômes à coefficients entiers.

En effet, en divisant la fonction $a+bx+cx^2+\ldots+lx^{n-1}$ par $\varphi(x)$, et en désignant par A le quotient et par R le reste, on aura

$$a+bx+cx^2+\ldots+lx^{n-1}=A\varphi(x)+R,$$

le degré de R étant inférieur à celui de $\varphi(x)$.

Le nombre complexe

$$\frac{R}{p}=\frac{a+bx+cx^2+\ldots+lx^{n-1}}{p}-A\frac{\varphi(x)}{p}$$

est évidemment un nombre entier; donc, en vertu de la propriété du nombre $\frac{\varphi(x)}{p}$, on en conclut que tous les coefficients de R sont divisibles par p.

Ainsi $R=pB$, B étant la fonction entière à coefficients entiers, et l'on aura

$$\frac{a+bx+cx^2+\ldots+lx^{n-1}}{p}=A\frac{\varphi(x)}{p}+B.$$

Passons maintenant aux nombres complexes entiers de la forme

$$\zeta=\frac{a+bx+cx^2+\ldots+lx^{n-1}}{p^2}.$$

On peut présenter ces nombres complexes sous la forme

$$\zeta = \frac{f(x)}{p^2} + \alpha + \beta x + \gamma x^2 + \ldots + \lambda x^{n-1},$$

α, β, γ, ..., λ étant des entiers et $f(x)$ un polynôme à coefficients entiers compris entre o et p^2. La fonction $f(x)$ consiste à son tour en deux parties,

$$f(x) = f_1(x) + p f_2(x)$$

$f_1(x)$ ne contenant pas de termes divisibles par p. En divisant $f_2(x)$ par $\varphi(x)$, $\varphi(x)$ étant le polynôme considéré ci-dessus, on aura

$$f_2(x) = \mathrm{A}\,\varphi(x) + \mathrm{B}.$$

De ce que $\frac{f_1(x)}{p} = \frac{f(x)}{p} - f_2(x)$ est un nombre entier, on en conclut que le degré de $f_1(x)$ n'est pas inférieur à celui de $\varphi(x)$.

En posant $f_1(x) + p\mathrm{B} = \varphi_1(x)$, on aura

$$\frac{f(x)}{p^2} = \frac{\varphi_1(x)}{p^2} + \mathrm{A}\frac{\varphi(x)}{p},$$

d'où l'on voit que le nombre complexe $\frac{\varphi_1(x)}{p^2}$ est un nombre entier. Il existe un nombre complexe entier, de la forme $\frac{\varphi_1(x)}{p^2}$, pour lequel $\varphi_1(x)$ sera du moindre degré possible. Le coefficient de la plus haute puissance de x dans la fonction $\varphi_1(x)$ peut être supposé égal à l'unité. En introduisant le nombre $\frac{\varphi_1(x)}{p^2}$, il est facile de faire voir que tous les nombres entiers complexes de la forme

$$\frac{a + bx + cx^2 + \ldots + lx^{n-1}}{p^2}$$

seront aussi de la forme

$$\mathrm{A}\frac{\varphi_1(x)}{p^2} + \mathrm{B}\frac{\varphi(x)}{p} + \mathrm{C},$$

A, B, C étant des fonctions entières à coefficients entiers.

En effet, la fonction $a + bx + cx^2 + \ldots + lx^{n-1}$ n'est pas de degré inférieur à celui de $\varphi_1(x)$. En la divisant par $\varphi_1(x)$, on aura le quotient A et le reste R, de degré inférieur à celui de $\varphi_1(x)$.

D'abord il suit de l'égalité

$$\frac{a + bx + cx^2 + \ldots + lx^{n-1}}{p^2} = A\frac{\varphi_1(x)}{p^2} + \frac{R}{p^2}$$

que $\frac{R}{p^2}$ est un nombre entier. Puis, le degré de R étant moindre que celui de $\varphi_1(x)$, on voit que tous les coefficients de R sont divisibles par p, et, par conséquent, $R = pR_1$.

Par ce qui précède, on sait que le nombre entier $\frac{R_1}{p}$ doit être de la forme $B\frac{\varphi(x)}{p} + C$. Donc

$$\frac{a + bx + cx^2 + \ldots + lx^{n-1}}{p^2} + A\frac{\varphi(x)}{p^2} = B\frac{\varphi(x)}{p} + C.$$

En considérant de la même manière les nombres complexes entiers de la forme

$$\frac{a + bx + \ldots + lx^{n-1}}{p^3} \cdots \frac{a + bx + \ldots + lx^{n-1}}{p^m},$$

m étant le plus haut degré de p qui figure dans les dénominateurs de nombres entiers complexes, nous choisirons parmi eux les nombres $\frac{\varphi_2(x)}{p^3}, \ldots, \frac{\varphi_{m-1}(x)}{p^m}$, semblables à $\frac{\varphi(x)}{p}$ et $\frac{\varphi_1(x)}{p^2}$.

Le coefficient de la plus haute puissance de x dans chacune des fonctions $\varphi_2(x), \ldots, \varphi_{m-1}(x)$ peut être supposé égal à l'unité.

Soient respectivement $\mu, \mu_1, \ldots, \mu_{m-1}$ les degrés des fonctions $\varphi(x)$, $\varphi_1(x), \ldots, \varphi_{m-1}(x)$. On aura

$$\mu \leq \mu_1 \leq \mu_2 \leq \ldots \leq \mu_{m-1}.$$

En effet, si l'on a, par exemple,

$$\mu_i > \mu_{i+1},$$

il en résultera une contradiction, car, le nombre $\frac{\varphi_{i+1}(x)}{p^{i+1}}$ étant entier, $\frac{\varphi_{i+1}(x)}{p^i}$ le sera aussi, et la fonction $\varphi_{i+1}(x)$ est de degré inférieur à celui de $\varphi_i(x)$, ce qui est en contradiction avec la définition de la fonction $\varphi_i(x)$.

De plus, si l'on a

$$\mu_i = \mu_{i+1},$$

on peut toujours faire $\varphi_i(x) = \varphi_{i+1}(x)$, car $\frac{\varphi_{i+1}(x)}{p^i}$ est un nombre entier, et $\varphi_{i+1}(x)$ est du même degré que $\varphi_i(x)$.

Posons, en général,

$$\begin{aligned}
&\mu \quad = \mu_1 \quad = \ldots = \mu_k,\\
&\mu_{k+1} = \mu_{k+2} = \ldots = \mu_{k_1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\mu_{k_k+1} = \mu_{k_k+2} = \ldots = \mu_{m-1}.
\end{aligned}$$

Alors, en suivant la même marche que plus haut, il est aisé de faire voir que tout nombre complexe entier ζ est congru suivant le module p au nombre

$$(1) \qquad A\frac{\varphi_{m-1}(x)}{p^m} + B\frac{\varphi_{k_k}(x)}{p^{k_k+1}} + C\frac{\varphi_{k_{k-1}}(x)}{p^{k_{k-1}+1}} + \ldots + K\frac{\varphi_k(x)}{p^{k+1}} + L,$$

A, B, C, ..., L étant des fonctions entières à coefficients entiers.

Les degrés de A, B, ..., K, L seront respectivement

$$\begin{aligned}
&A \text{ du degré } n - 1 - \mu_{m-1},\\
&B \quad » \quad \mu_{m-1} - \mu_{k_k} - 1,\\
&C \quad » \quad \mu_{k_k} - \mu_{k_{k-1}} - 1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&L \text{ du degré } \mu_k - 1.
\end{aligned}$$

Réciproquement, tout nombre complexe ayant la forme (1) est évidemment un nombre entier.

Remarquons maintenant que, lorsque les deux nombres complexes

$$A\frac{\varphi_{m-1}(x)}{p^m}+B\frac{\varphi_{k_h}(x)}{p^{k_h+1}}+C\frac{\varphi_{k_{h-1}}(x)}{p^{k_{h-1}+1}}+\cdots,$$
$$A'\frac{\varphi_{m-1}(x)}{p^m}+B'\frac{\varphi_{k_h}(x)}{p^{k_h+1}}+C'\frac{\varphi_{k_{h-1}}(x)}{p^{k_{h-1}+1}}+\cdots$$

sont congrus suivant le module p, on aura

$$A'\equiv A,\quad B'\equiv B,\quad \ldots,\quad K'\equiv K,\quad L'\equiv L\pmod p,$$

de sorte que tous les coefficients dans les différences

$$A'-A,\ B'-B,\ \ldots,\ L'-L$$

seront divisibles par p.

En effet, la différence

$$\frac{(A'-A)\varphi_{m-1}(x)}{p^{m+1}}+\frac{(B'-B)\varphi_{k_h}(x)}{p^{k_h+2}}+\frac{(C'-C)\varphi_{k_{h-1}}(x)}{p^{k_{h-1}+2}}+\cdots$$

étant, par hypothèse, un nombre entier, et p^m la plus haute puissance de p qui puisse figurer dans les dénominateurs des nombres complexes entiers, s'ils sont réduits à leurs plus simples expressions, on voit que les coefficients de toutes puissances de x dans la fonction

$$(A'-A)\varphi_{m-1}(x)+(B'-B)(p^{m-k_h}\varphi_{k_h}(x)+(C'-C)p^{m-k_{h-1}}\varphi_{k_{h-1}}(x)+\cdots$$

doivent être divisibles par p, ou, ce qui revient au même

$$A'-A\equiv 0\pmod p.$$

Donc

$$\frac{(A'-A)\varphi_{m-1}(x)}{p^{m+1}}$$

est un nombre entier.

Il résulte de là que le nombre $\frac{(B'-B)\varphi_{k_h}(x)}{p^{k_h+2}}+\frac{(C'-C)\varphi_{k_{h-1}}(x)}{p^{k_{h-1}+2}}+\cdots$ le sera aussi. Mais, la fonction

$$(B'-B)\varphi_{k_h}(x)+(C'-C)p^{k_h-k_{h-1}}\varphi_{k_{h-1}}(x)+\cdots$$

étant du degré inférieur à celui de $\varphi_{m-1}(x)$, on voit que les coefficients de toutes les puissances de x dans cette fonction doivent être divisibles par p. Donc

$$B' - B \equiv 0 \pmod{p}.$$

On s'assurera de la même manière que $C' - C \equiv 0 \pmod{p}$, etc. On en conclut que la quantité des nombres complexes entiers incongrus entre eux suivant le module p et non divisibles par p est égale à $p^n - 1$.

En effet, les coefficients des fonctions A, B, C, ..., L sont respectivement en nombres

$$n - \mu_{m-1},\ \mu_{m-1} - \mu_{kk},\ \mu_{k_k} - \mu_{kk-1},\ \ldots,\ \mu_k;$$

chacun d'eux a, suivant le module p, p valeurs distinctes. Si l'on exclut le nombre pour lequel tous les coefficients des A, B, ..., L s'annulent, on aura $p^n - 1$ nombres incongrus suivant le module p.

Remarque. — La formule générale (1), pour les nombres complexes entiers pris suivant le module p, suppose que les nombres $\frac{\varphi_{m-1}(x)}{p^m}$, $\frac{\varphi_{k_k}(x)}{p^{k_k+1}}$, ... soient connus.

Tous les nombres pourront effectivement être déterminés après un nombre fini d'opérations. En effet, considérons des nombres complexes de la forme

$$\frac{a + bx + cx^2 + \ldots + lx^{n-1}}{p^i},$$

en supposant l'exposant i donné et les coefficients $a, b, c, \ldots, l$ compris entre zéro et p^i. Ces nombres étant en nombre fini, on peut toujours reconnaître parmi eux ceux qui sont entiers et choisir celui pour lequel la fonction $a + bx + cx^2 + \ldots + lx^{n-1}$ aura le moindre degré possible.

Il existe des méthodes pour trouver ces nombres $\frac{\varphi_{m-1}(x)}{p^m}$, $\frac{\varphi_{k_k}(x)}{p^{k_k+1}}$, ... plus promptement; mais je ne m'arrête pas sur ce point, n'y voyant rien d'essentiel.

26. D'après ce qui a été établi dans le numéro précédent, on

peut toujours reconnaître si un nombre complexe donné

$$y = \frac{f(x)}{\varphi(x)},$$

f et φ désignant des fonctions entières à coefficients entiers, est un nombre entier.

En effet, ce nombre peut être représenté sous la forme

$$y = \frac{\psi(x)}{N},$$

$\psi(x)$ étant un polynôme à coefficients entiers qui n'ont pas avec N de diviseur commun.

Cela posé, si N est divisible par un nombre premier qui n'appartient pas aux modules exceptionnels pour l'équation $F(x) = 0$, on en conclut que y ne sera pas un nombre entier.

Maintenant supposons

$$N = p^m p_1^{m_1} \dots p_s^{m_s},$$

$p, p_1, \dots, p_s$ étant des modules exceptionnels.

Alors $\frac{\psi(x)}{p^m}, \frac{\psi(x)}{p_1^{m_1}}, \dots, \frac{\psi(x)}{p_s^{m_s}}$ doivent être des nombres entiers si $\frac{\psi(x)}{N}$ en est un.

Réciproquement, si $\frac{\psi(x)}{p^m}, \frac{\psi(x)}{p_1^{m_1}}, \dots, \frac{\psi(x)}{p_s^{m_s}}$ sont des nombres entiers, le nombre $\frac{\psi(x)}{N}$ le sera.

Effectivement, la somme $\frac{\psi(x)}{p^m} + \frac{\psi(x)}{p_1^{m_1}} + \dots + \frac{\psi(x)}{p_s^{m_s}}$ est égal à $\frac{M\psi(x)}{N}$, M étant un nombre ordinaire premier avec N. Donc on pourra trouver deux nombres P et Q tels qu'on ait

$$PM - QN = 1.$$

En remarquant que $\frac{PM\psi(x)}{N} = \frac{\psi(x)}{N} + Q\psi(x)$ est un nombre entier, on conclut que $\frac{\psi(x)}{N}$ le sera.

Nous sommes donc amené à reconnaître si les nombres $\frac{\psi(x)}{p^m}$,

$\frac{\psi(x)}{p_1^{n_1}}, \cdots$ sont entiers. Cela se fait au moyen de la formule (1) du numéro précédent et des formules analogues pour les autres nombres premiers $p_1, p_2, \ldots$.

27. Dans ce numéro et dans les suivants, nous allons démontrer quelques théorèmes qui nous seront indispensables pour décomposer les nombres complexes en facteurs idéaux.

Désignons par

$$\alpha_1, \alpha_2, \ldots, \alpha_\sigma, \tag{1}$$

σ étant égal à $p^n - 1$, les $p^n - 1$ nombres incongrus suivant le module p. Si l'on exclut les nombres complexes qui sont multiples de p, chaque nombre sera congru à l'un des termes de la suite (1).

Nous nommerons le nombre complexe α *premier avec le module* p si le produit $\alpha\beta$ n'est pas divisible par p, quel que soit le nombre de la suite (1) que l'on prend au lieu de β.

Dans le cas contraire, les nombres α et β ont des *facteurs communs*.

Nous dirons que deux nombres α et β n'ont pas de *diviseurs communs avec* p ou qu'ils *sont premiers entre eux suivant le module* p si les nombres $\alpha\gamma$ et $\beta\gamma$ ne sont pas divisibles par p ensemble, quel que soit le nombre γ de la suite (1). Remarquons maintenant que la norme du nombre α ne sera pas divisible par p si α est premier avec p.

En effet, soit au contraire $\mathrm{N}(\alpha)$ divisible par p. Alors on pourra trouver, comme nous allons voir, un nombre β non divisible par p et tel que $\alpha\beta \equiv 0 \pmod{p}$.

Désignons par $\alpha', \alpha'', \ldots, \alpha^{(n-1)}$ les valeurs du nombre α correspondant aux autres racines de l'équation fondamentale $\mathrm{F}(x) = 0$ et par A le produit $\alpha'\alpha'' \ldots \alpha^{(n-1)}$.

Supposons A divisible par p^ν et non divisible par $p^{\nu+1}$ (ν peut être égal à zéro). Donc $\frac{\mathrm{A}}{p^\nu}$ sera un nombre complexe non divisible par p. Le produit $\mathrm{B} = \alpha\frac{\mathrm{A}}{p^\nu}$ sera un nombre entier ordinaire, divisible par p, car $\mathrm{B}^n = \mathrm{N}(\alpha)\,\mathrm{N}\left(\frac{\mathrm{A}}{p^\nu}\right)$. Il résulte de là qu'on peut prendre au lieu de

β le nombre congru à $\frac{A}{p^r}$ suivant le module p. Donc le nombre α ne sera pas premier avec p, comme nous avons supposé.

Réciproquement, si la norme $N(\alpha)$ du nombre complexe α n'est pas divisible par p, il n'existe aucun nombre β non divisible par p, et tel que le produit $\alpha\beta$ soit divisible par p.

En effet, supposons au contraire que β soit un tel nombre. On a

$$\alpha\beta = p\gamma,$$

γ étant un nombre complexe entier.

Le nombre α, comme on sait, est la racine de l'équation

$$\alpha^n + q_1\alpha^{n-1} + q_2\alpha^{n-2} + \ldots + q_n = 0,$$

à coefficients entiers, dont le dernier, q_n, n'est pas divisible par p, car il est égal à la norme $N(\alpha)$.

Il suit de là que le nombre β est la racine de l'équation

$$(I) \qquad q_n\left(\frac{\beta}{p}\right)^n + q_{n-1}\gamma\left(\frac{\beta}{p}\right)^{n-1} + \ldots + \gamma^n = 0.$$

Mais le nombre β, comme un nombre entier, satisfait encore à l'équation

$$(II) \qquad p^n\left(\frac{\beta}{p}\right)^n + g_1p^{n-1}\left(\frac{\beta}{p}\right)^{n-1} + \ldots + g_n = 0,$$

$g_1, g_2, \ldots, g_n$ étant des nombres entiers ordinaires.

Le nombre q_n étant premier avec p, on pourra trouver deux entiers M et N tels qu'on ait

$$q_nM + Np^n = 1.$$

En multipliant l'équation (I) par M et l'équation (II) par N, on aura, après l'addition,

$$\left(\frac{\beta}{p}\right)^n + (q_{n-1}\gamma M + g_1p^{n-1}N)\left(\frac{\beta}{p}\right)^{n-1} + \ldots = 0,$$

d'où l'on voit que $\frac{\beta}{p}$ est un nombre complexe entier, et, par conséquent, β est divisible par p, ce qui est contraire à la supposition.

THÉORÈME. — *Si les nombres complexes* A *et* B *n'ont pas de diviseurs communs avec p, ainsi que les nombres* A *et* C, *les nombres* A *et* BC *n'auront pas aussi de diviseurs communs avec p.*

En effet, supposons au contraire que les nombres A et BC ne soient pas des nombres premiers entre eux suivant le module p; alors, par conséquent, on pourrait trouver un nombre complexe R tel que AR et BCR soient divisibles par p; mais CR n'est pas divisible par p, car autrement A et C auraient des diviseurs communs avec p. En remarquant maintenant que le produit ACR est encore divisible par p, car p divise le facteur AR, on voit qu'il existe un nombre complexe CR non divisible par p et tel que les produits $A \times CR$ et $B \times CR$ soient les multiples de p.

Donc A et B ont des diviseurs communs avec p, ce qui est contraire à la supposition.

28. THÉORÈME. — *Si le nombre complexe* A *n'a pas de diviseurs communs avec p, il existe dans la suite* (1) (n° **27**) *un nombre* M *tel qu'on ait*

$$AM \equiv 1 \pmod{p}.$$

En effet, considérons la suite des nombres

$$A\alpha_1,\ A\alpha_2,\ \ldots,\ A\alpha_\sigma. \tag{I}$$

Ces nombres sont congrus suivant le module p aux nombres (1) (n° **27**), abstraction faite de l'ordre. En effet, aucun des nombres (I) n'est divisible par p, car autrement A ne serait pas un nombre premier avec p. Par la même raison, tous les nombres de la suite (I) sont incongrus suivant le module p. Donc l'un d'eux est congru à l'unité, qui est congru à l'un des termes de la suite (I).

29. THÉORÈME. — *Soient* A *et* B *deux nombres complexes premiers*

entre eux suivant le module p. On peut toujours trouver deux nombres complexes entiers M *et* N *tels qu'on ait*

$$AM - BN \equiv 1 \pmod{p}.$$

Considérons deux nombres complexes quelconques μ et ν, dont chacun est premier avec le module p.

Soit

$$A\mu - B\nu \equiv \xi \pmod{p}. \tag{1}$$

Supposons, en premier lieu, que ξ soit un nombre premier avec le module p.

On pourra alors trouver (n° **28**) un nombre Q tel qu'on ait

$$Q\xi \equiv 1 \pmod{p}.$$

Par conséquent, en posant

$$M \equiv Q\mu, \quad N \equiv Q\nu \pmod{p},$$

on aura

$$AM - BN \equiv 1 \pmod{p}$$

et le théorème sera démontré.

Considérons, en second lieu, le cas dans lequel ξ n'est pas premier avec le module p.

Alors les nombres A et ξ, ainsi que B et ξ, n'auront pas de diviseurs communs avec le module p. En effet, supposons, par exemple, les nombres B et ξ ayant des facteurs communs avec le module p. Il résulte de là qu'il existe un nombre Q non divisible par p et tel qu'on ait

$$BQ \equiv 0 \quad \text{et} \quad \xi Q \equiv 0 \pmod{p}.$$

On voit par la congruence (1) que $A\mu Q$ sera aussi divisible par p. En multipliant ce nombre par un nombre μ' satisfaisant à la congruence

$$\mu\mu' \equiv 1 \pmod{p},$$

on trouve que le nombre AQ est divisible par p. Mais ce résultat est

contre l'hypothèse, car les deux nombres AQ et BQ ne peuvent être divisibles l'un et l'autre par p. Donc les nombres A et ξ, ainsi que B et ξ, n'ont pas de diviseurs communs avec p.

Remarquons encore que le nombre ξ peut toujours être supposé non divisible par p. En effet, soit

$$A\mu \equiv B\nu \pmod{p}. \tag{2}$$

Cette congruence ne peut être satisfaite qu'en supposant chacun des nombres A et B premier avec le module p. En effet, si par exemple B a des facteurs communs avec p, on pourra déterminer un nombre Q tel qu'on ait

$$BQ \equiv 0 \pmod{p}.$$

Alors la congruence (2) nous donne

$$A\mu Q \equiv 0 \pmod{p},$$

d'où l'on déduit, comme ci-dessus, que

$$AQ \equiv 0 \pmod{p},$$

ce qui ne peut avoir lieu, A et B étant deux nombres premiers entre eux suivant le module p.

Donc la congruence (2) suppose chacun des nombres A et B premier avec p. Mais, cela étant, il est facile de déduire notre théorème du théorème du n° **28**. En effet, on peut prendre $N = 0$ et déterminer M par la congruence

$$AM \equiv 1 \pmod{p}.$$

Ainsi nous supposons ξ non divisible par p.

Comme les nombres A et B sont premiers entre eux suivant le module p, l'un des deux nombres $A\xi$, $B\xi$ au moins ne sera pas divisible par p.

Supposons, pour fixer les idées, $A\xi$ non divisible par p. D'après le théorème du n° **27**, on voit que les nombres $A\xi$ et B sont premiers entre eux suivant le module p.

Considérons maintenant le nombre

$$A\xi\mu - B\nu \equiv \xi_1 \pmod{p}.$$

Dans le cas où ξ_1 est un nombre premier avec le module p, on démontre notre théorème tout de suite; mais, si ξ n'est pas un nombre premier avec p, les nombres ξ_1 et B, ainsi que ξ_1 et $A\xi$, sont premiers entre eux suivant le module p. Il suit de là que ξ_1 et ξ ne sont pas des nombres congrus suivant le module p. Dans ce cas, on peut passer du nombre ξ_1 au nombre ξ_2 de la même manière que de ξ à ξ_1, etc.

Remarquons que la série de nombres $\xi, \xi_1, \xi_2, \ldots$ est toujours finie, car ils sont tous incongrus suivant le module p. On voit donc que nous arrivons enfin à une congruence

$$A\mu' - B\nu' \equiv \eta \pmod{p},$$

η étant un nombre premier avec le module p. Mais de cette congruence il résulte, comme nous avons vu, notre théorème.

Remarque. — En poursuivant la même marche, il est facile de déduire le théorème plus général :

Soient A *et* B *deux nombres complexes premiers entre eux suivant le module p. On peut toujours trouver deux nombres complexes entiers* M *et* N *tels qu'on ait*

$$AM - BN \equiv 1 \pmod{p^m},$$

m étant un nombre entier et positif.

30. Nous compterons parmi les nombres complexes premiers un nombre réel p si tous les nombres

$$\alpha_1, \alpha_2, \ldots, \alpha\sigma \tag{1}$$

sont premiers avec p.

Pour décomposer les autres nombres premiers ordinaires en facteurs

premiers idéaux, nous supposons que les termes de la suite (1) ne sont pas pris arbitrairement, mais qu'ils satisfont à une certaine condition que nous allons connaître.

Soit α un des nombres de la suite (1), dont la norme est divisible par p.

De tous les nombres complexes entiers $\alpha + p\xi$ congrus à α suivant le module p, nous choisirons un de ceux dont les normes contiennent comme facteur le moindre degré possible du nombre p.

Voici comment on peut trouver ce nombre.

Supposons que

$$N(\alpha) = p^h P,$$

P étant un nombre non divisible par p.

Soit

$$\alpha,\ \beta,\ \gamma,\ \ldots \tag{2}$$

la suite composée de tous les nombres congrus à α suivant le module p et telle qu'il n'y en ait que deux congrus suivant le module p^h.

On sait par le n° **25** comment cette suite (2) peut être trouvée.

Soit maintenant A un nombre complexe quelconque congru à α suivant le module p. Il sera congru suivant le module p^h à un nombre de la suite (2).

Supposant, par exemple,

$$A \equiv \beta \pmod{p^h},$$

on aura

$$N(A) \equiv N(\beta) \pmod{p^h}.$$

Donc, si la norme N(A) contient p comme facteur moins de h fois, il en contient le même nombre de fois que la norme Nβ.

Il suit de là que parmi les termes de la suite (2) on pourra toujours trouver au moins un nombre dont la norme contient comme facteur le moindre degré possible du nombre p.

Supposons que ce nombre soit le nombre α lui-même qui figure dans la suite (1) et que tous les nombres de cette suite non premiers avec p satisfassent à la même condition que le nombre α.

Cela posé, nous allons établir une propriété importante des nombres contenus dans la suite (1).

Chaque nombre α de la suite (1) *ayant la norme divisible par p^μ satisfait à l'équation*

$$\alpha^n + b_1\alpha^{n-1} + b_2\alpha^{n-2} + \ldots + b_{n-1}\alpha + b_n = 0, \tag{3}$$

dans laquelle le coefficient b_n est divisible par p^μ par hypothèse et les autres coefficients b_{n-1}, b_{n-2}, ... sont respectivement divisibles par $p^{\mu-1}$, $p^{\mu-2}$, ...

Pour démontrer cette proposition, considérons un nombre $\alpha - \lambda p$, λ étant un entier ordinaire.

Les nombres α, α', α'', ... désignant toutes les racines de l'équation (3), la norme du nombre complexe $\alpha - \lambda p$ se présente sous la forme

$$\begin{aligned}\mathrm{N}(\alpha - \lambda p) &= (\alpha - \lambda p)(\alpha' - \lambda p)\ldots(\alpha^{(n-1)} - \lambda p)\\ &= \pm(p^n\lambda^n + b_1p^{n-1}\lambda^{n-1} + b_2p^{n-2}\lambda^{n-2} + \ldots + b_n).\end{aligned}$$

Cette norme doit être divisible par p^μ, quel que soit λ, car p^μ divise $\mathrm{N}(\alpha)$, contenant comme facteur le moindre degré du nombre p.

En posant $b_n = p^\mu c_n$, on voit que le nombre

$$p^{n-1}\lambda^n + b_1p^{n-2}\lambda^{n-1} + \ldots + b_{n-1}\lambda + p^{\mu-1}c_n$$

doit être divisible par $p^{\mu-1}$, quel que soit λ. Donc b_{n-1} est divisible par p, et l'on peut poser $b_{n-1} = pc_{n-1}$, c_{n-1} étant un nombre entier. Puis on voit que le nombre

$$p^{n-2}\lambda^n + b_1p^{n-3}\lambda^{n-1} + \ldots + b_{n-2}\lambda^2 + c_{n-1}\lambda + p^{\mu-2}c_n$$

doit être divisible par $p^{\mu-2}$, λ étant quelconque. Donc les coefficients b_{n-2} et c_{n-1} doivent être divisibles par p.

Il est clair que l'on peut poursuivre de cette manière jusqu'à ce que l'on ait démontré la divisibilité du nombre b_{n-1} par $p^{\mu-1}$, b_{n-2} par $p^{\mu-2}$, ... Cette démonstration peut être en défaut dans quelques cas particuliers si p est inférieur à n.

En voici une autre qui ne souffre aucune exception.

Soient

$$b_n = p^{\mu} c_n, \quad b_{n-1} = p^{\mu_1} c_{n-1} \ldots,$$
$$b_{n-k} = p^{\mu_k} c_{n-k}, \quad \ldots\ldots\ldots\ldots,$$
$$\ldots\ldots\ldots\ldots, \quad \ldots\ldots\ldots\ldots,$$

c_n, c_{n-1}, ..., c_{n-k} étant des entiers non divisibles par p. Désignons par $\lambda = \frac{r}{s}$, r et s étant des nombres entiers, la plus grande valeur des fractions

$$\mu - \mu_1', \quad \frac{\mu - \mu_2}{2}, \quad \ldots, \quad \frac{\mu - \mu_k}{k}, \quad \ldots.$$

Cela posé, nous ferons voir que le nombre $\frac{p^r c_n^s}{\alpha^s}$ est un nombre entier.

En effet, le nombre $\frac{p^{\lambda} c_n}{\alpha}$ est une racine de l'équation

$$\xi^n + c_{n-1} p^{\mu_1 + \lambda - \mu} \xi^{n-1} + c_{n-2} c_n p^{\mu_2 + 2\lambda - \mu} \xi^{n-2} + \ldots = 0.$$

Les exposants $\mu_1 + \lambda - \mu$, $\mu_2 + 2\lambda - \mu$, ... peuvent être fractionnaires, mais aucun d'eux ne peut être négatif, car $\mu_i + i\lambda - \mu \geq 0$ ou, ce qui est le même, $\lambda \geq \frac{\mu - \mu_i}{i}$. Cela est d'accord avec la définition de λ.

Il résulte de là que le nombre $\frac{p^r c_n^s}{\alpha^s}$ est un nombre entier.

Considérons maintenant un nombre complexe entier

$$\zeta = \alpha - \frac{p^{ri+1} c_n^{si}}{\alpha^{si}},$$

congru à α suivant le module p, i étant un entier quelconque ordinaire et positif.

On aura évidemment

$$\mathrm{N}(\zeta) = \frac{\mathrm{N}(\alpha^{si+1} - p^{ri+1} c_n^{si})}{\mathrm{N}(\alpha^{si})}.$$

Afin de savoir quelle puissance de p est contenue comme facteur

dans la norme $\mathbf{N}\zeta$, nous remarquons que

$$\mathbf{N}(\alpha^{si+1} - p^{ri+1} c_n^{si}) = \mathbf{N}\left(\alpha - p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \mathbf{N}\left(\alpha - \omega p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \mathbf{N}\left(\alpha - \omega^2 p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \ldots,$$

ω étant une racine primitive $si+1^{\text{ième}}$ de l'unité, et $\mathbf{N}\left(\alpha - \omega^k p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right)$ désignant le produit

$$\left(\alpha - \omega^k p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right)\left(\alpha' - \omega^k p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right)\left(\alpha'' - \omega^k p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \ldots,$$

où α, α', α'', ... sont toutes les racines de l'équation (3).

En posant

$$\Phi(z) = (z-\alpha)(z-\alpha')(z-\alpha'')\ldots = z^n + b_1 z^{n-1} + b_2 z^{n-2} + \ldots + b_n,$$

il vient

$$\mathbf{N}(\alpha^{si+1} - p^{ri+1} c_n^{si}) = \pm \Phi\left(p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \Phi\left(\omega p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \Phi\left(\omega^2 p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) \ldots,$$

où

$$\Phi\left(p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right) = p^{\mu} c_n + p^{\mu_1 + \frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}} c_{n-1} + p^{\mu_1 + 2\frac{ri+1}{si+1}} c_n^{\frac{si2}{si+1}} c_{n-2} + \ldots.$$

On pourra assigner un nombre i de telle manière, que parmi les exposants μ, $\mu_1 + \frac{ri+1}{si+1}$, $\mu_2 + 2\frac{ri+1}{si+1}$, $\cdots$ il n'y en ait pas deux égaux entre eux. Soit Δ celui des exposants qui a la valeur moindre.

Maintenant il y a deux cas à distinguer : $\lambda > 1$ et $\lambda \leq 1$.

Supposons d'abord $\lambda > 1$. On va voir que Δ est inférieur à μ.

En effet, soit $\lambda = \frac{\mu - \mu_f}{f}$; on aura

$$\mu_f + \lambda f = \mu.$$

Mais, $\lambda = \frac{r}{s}$ étant supérieur à l'unité, on a

$$\lambda > \frac{ri+1}{si+1},$$

et par conséquent

$$\mu_f + f\frac{ri+1}{si+1} < \mu.$$

Donc, *a fortiori*, $\Delta < \mu$.

Cela posé, on s'assure aisément que le nombre entier égal au produit

$$\Phi\left(p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right)\Phi\left(\omega p^{\frac{ri+1}{si+1}} c_n^{\frac{si}{si+1}}\right)\ldots$$

contient $(si+1)\Delta$ fois le facteur p. Il résulte de là que la norme ζ le contient $(si+1)\Delta - si\mu < \mu$ fois, ce qui est absurde, en vertu du choix des nombres α, car ζ est congru à α suivant le module p.

Ainsi $\lambda \leq 1$, et par conséquent

$$\frac{\mu - \mu_h}{h} \leq 1,$$

quel que soit h, d'où

$$\mu_h \geq \mu - h.$$

Donc le théorème est démontré.

Corollaire I. — Le nombre complexe $\frac{pc_n}{\alpha}$ est un nombre entier.

En effet, l'équation (3) multipliée par $\frac{c_n^{\mu-1}}{\alpha^\mu}$ nous donne la suivante,

$$\left(\frac{pc_n}{\alpha}\right)^\mu + \frac{b_{n-1}}{p^{\mu-1}}\left(\frac{pc_n}{\alpha}\right)^{\mu-1} + \frac{b_{n-2}c_n}{p^{\mu-2}}\left(\frac{pc_n}{\alpha}\right)^{\mu-2} + \ldots = 0;$$

$\frac{b_{n-1}}{p^{\mu-1}}, \frac{b_{n-2}c_n}{p^{\mu-2}}, \ldots$ étant des nombres entiers. On en conclut que $\frac{pc_n}{\alpha}$ est un nombre entier. Donc, pour chaque nombre α de la suite (1), il existe un nombre ordinaire H non divisible par p, et tel que le produit Hp soit divisible par α.

Corollaire II. — Soit β un nombre complexe non compris dans la suite

$$(1) \qquad \alpha_1, \alpha_2, \ldots, \alpha_\sigma$$

et non divisible par p.

Nous ferons voir qu'il existe alors dans cette suite un nombre α tel que le produit $H\beta$ soit divisible par α, H étant un nombre ordinaire premier avec p.

En effet, supposant β congru au nombre α de la suite (1), on aura

$$\beta = \alpha + p\gamma,$$

γ étant un nombre entier complexe. Désignons maintenant par H un nombre non divisible par p et tel que le produit Hp soit divisible par α (corollaire I). Alors il vient

$$H\beta = \alpha(H + \delta\gamma),$$

δ étant égal à $\frac{Hp}{\alpha}$. C. Q. F. D.

31. Nous dirons, pour abréger, que le nombre β contient tous les facteurs du nombre p appartenant au nombre α s'il existe un nombre A premier avec p et tel que $A\beta$ soit divisible par α.

Désignons par H la norme $N(A)$, H étant un nombre ordinaire non divisible par p. On voit que $H\beta$ est divisible par α. Ainsi, lorsque β contient tous les facteurs de p appartenant à α, il existe un nombre ordinaire H non divisible par p et tel que $H\beta$ soit divisible par α.

Théorème. — *Si le produit $\beta\gamma$ de deux nombres complexes contient tous les facteurs de p appartenant à α et si les nombres α et β n'ont aucun facteur commun avec p, le nombre γ contient tous les facteurs de p appartenant à α.*

Posons, pour abréger,

$$N(\alpha) = p^\lambda b,$$

b n'étant pas divisible par p.

Il existe, par hypothèse, un nombre ordinaire H non divisible par p et tel que le produit $H\beta\gamma$ soit divisible par α. On peut prendre b au lieu de H (n° **24**), et soit $\frac{b\beta\gamma}{\alpha} = \delta$, δ étant un nombre entier complexe. Mais, α et β n'ayant point de facteurs communs avec p, on pourra trouver deux nombres complexes ξ, η tels qu'on ait (n° **29**)

$$\beta\xi - \alpha\eta \equiv 1 \pmod{p^\lambda}$$

ou, ce qui est la même chose,

$$\beta\xi = \alpha\eta + 1 + p^{\lambda}\varepsilon,$$

ε étant encore un nombre entier. Donc

$$\xi\delta = \frac{b\gamma}{\alpha} + b\eta\gamma + \frac{bp^{\lambda}\varepsilon\gamma}{\alpha}.$$

En ayant égard à ce que $\frac{bp^{\lambda}}{\alpha}$ est un nombre entier, on voit que $\frac{b\gamma}{\alpha}$ le sera aussi; par conséquent, γ contient tous les facteurs de p appartenant à α.

32. THÉORÈME. — *Si les deux nombres complexes β et γ ont des diviseurs communs avec p, et si aucun de ces deux nombres ne contient tous les facteurs de p appartenant à l'autre, il existe un tel nombre α que chacun d'eux contienne tous les facteurs de p appartenant à α.*

En effet, les nombres β et γ ayant des diviseurs communs avec p, on pourra toujours trouver dans la suite

$$(1) \qquad \alpha_1, \ \alpha_2, \ \ldots, \ \alpha_\sigma,$$

que nous avons considérée dans le n° **30**, un nombre M tel que les nombres $M\beta$ et $M\gamma$ soient divisibles par p (n° **27**). Soient

$$M\beta = p\beta_1, \quad M\gamma = p\gamma_1.$$

D'ailleurs, on sait par le n° **30** qu'il existe toujours un nombre ordinaire H, non divisible par p, tel que $\frac{Hp}{M}$ soit un nombre entier.

En désignant $\frac{Hp}{M}$ par α, on aura

$$(2) \qquad H\beta = \alpha\beta_1, \quad H\gamma = \alpha\gamma_1.$$

Donc les nombres β, γ contiennent l'un et l'autre tous les facteurs de p appartenant à α.

D'après le corollaire II (n° **30**), il est permis de supposer que α

soit encore un terme de la suite (1). De plus, aucun des nombres β_1 et γ_1 ne sera premier avec le module p.

En effet, supposons, par exemple, β_1 premier avec le module p. Alors (n° **31**) α contiendra tous les facteurs de p appartenant à β. Donc γ les contient aussi, ce qui est contraire à la supposition.

Les équations (2) nous donnent, en prenant les normes,

$$\mathrm{H}^n \mathrm{N}(\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta_1),$$
$$\mathrm{H}^n \mathrm{N}(\gamma) = \mathrm{N}(\alpha)\mathrm{N}(\gamma_1).$$

En ayant égard à ce que $\mathrm{N}(\beta_1)$ et $\mathrm{N}(\gamma_1)$ sont divisibles par p (n° **27**), on en conclut que p rentre comme facteur dans la norme $\mathrm{N}(\alpha)$ moins de fois que dans les normes $\mathrm{N}(\beta)$ et $\mathrm{N}(\gamma)$.

33. Je reprends maintenant la suite des nombres

$$(1) \qquad \alpha_1, \ \alpha_2, \ \ldots, \ \alpha_\sigma$$

incongrus suivant le module p.

Nous dirons que le nombre α de cette suite ne contient qu'un facteur premier idéal du nombre p si chaque nombre non premier avec α suivant le module p contient tous les facteurs de p appartenant à α (n° **31**).

Le corollaire II (n° **30**) nous fait voir qu'il suffit de comparer le nombre α à tous les termes de la suite (1) pour savoir s'il ne contient qu'un facteur premier du nombre p. Faisons d'abord voir que de tels nombres α existent effectivement.

Soit β un nombre quelconque de cette suite non premier avec p. Supposons qu'il existe un autre nombre γ non premier avec β suivant le module p et ne contenant pas tous les facteurs premiers de p appartenant à β.

Cela posé, on voit, d'après le numéro précédent, qu'il existe dans la suite (1) un nombre α tel que β contienne tous les facteurs de p appartenant à α; la norme $\mathrm{N}(\alpha)$ contiendra p comme facteur moins de fois que la norme $\mathrm{N}(\beta)$.

Si α contient plus d'un facteur premier du nombre p, on peut, par la même raison, trouver dans la suite (1) un nombre α' tel que α con-

tienne tous les facteurs de p appartenant à α', et p rentrera dans la norme $\mathrm{N}(\alpha')$ avec l'exposant moindre que dans la norme $\mathrm{N}(\alpha)$.

On voit que, en poursuivant la même marche, on trouvera un nombre qui ne contient qu'un seul facteur premier de p.

Ainsi, chaque nombre non premier avec p contient au moins un facteur premier de p appartenant au nombre compris dans la suite (1) et qui ne comprend point d'autres facteurs de p.

Soient

$$\beta_1, \beta_2, \ldots, \beta_k \tag{2}$$

tous les nombres de la suite (1), dont chacun ne contient qu'un seul facteur premier idéal du nombre p. Si les deux nombres de cette suite ne sont pas premiers entre eux suivant le module p, nous dirons qu'ils contiennent un même facteur idéal du nombre p. On peut choisir dans la suite (2) tous les nombres qui contiennent des facteurs distincts de p. Soient $\nu, \nu_1, \nu_2, \ldots, \nu_s$ ces nombres.

Nous dirons que le nombre complexe α contient le facteur de p appartenant m fois au nombre ν s'il contient tous les facteurs de p appartenant à ν^m et ne contient pas tous les facteurs de p appartenant à ν^{m+1}.

Il suit de cette définition que, dans ce cas, $\mathrm{H}\alpha = \nu^m\beta$, H étant un nombre ordinaire non divisible par p, et β un nombre complexe entier.

En prenant les normes, il vient

$$\mathrm{H}^n\mathrm{N}(\alpha) = [\mathrm{N}(\nu)]^m\mathrm{N}(\beta).$$

Il en résulte que, pour chaque nombre donné α, m ne surpasse pas une limite finie. En effet, soient p^λ et p^μ les plus hautes puissances de p qui divisent $\mathrm{N}(\alpha)$ et $\mathrm{N}(\nu)$; on aura

$$\lambda \geq m\mu.$$

34. THÉORÈME. — *Le produit $\beta\gamma$ de deux nombres complexes contient le facteur idéal de p appartenant à ν autant de fois que les deux nombres β et γ ensemble.*

Supposons que β contienne ce facteur m fois et r fois γ. Ainsi, on a

$$(1)\qquad \begin{cases} \mathrm{H}\,\beta = \nu^m \beta_1, \\ \mathrm{H}_1 \gamma = \nu^r \gamma_1, \end{cases}$$

H et H_1 étant des entiers ordinaires non divisibles par p, β_1 et γ_1 deux nombres complexes entiers.

Nous allons voir que chacun des nombres β_1 et γ_1 ne contient point de facteur idéal de p appartenant à ν.

Supposons que, par exemple, β_1 le contienne. Alors nous aurons

$$h\beta_1 = \nu\beta_2,$$

où h désigne un nombre ordinaire non divisible par p, et β_2 un nombre complexe entier. Donc

$$\mathrm{H}h\beta = \nu^{m+1}\beta_2,$$

de sorte que β contiendrait tous les facteurs de p appartenant à ν^{m+1}, ce qui est contraire à la supposition.

Les égalités (1) nous donnent la suivante,

$$\mathrm{HH}_1\beta\gamma = \nu^{m+r}\beta_1\gamma_1,$$

d'où l'on voit que le nombre $\beta\gamma$ contient tous les facteurs de p appartenant à ν^{m+r}. Maintenant, il nous reste à faire voir qu'il ne contient pas tous les facteurs de p appartenant à ν^{m+r+1}. Supposons, au contraire, que $h\beta\gamma = \nu^{m+r+1}\gamma_2$, h étant un nombre premier avec p et γ_2 un nombre complexe entier.

Il s'ensuit que

$$h\beta_1\gamma_1 = \mathrm{HH}_1\nu\gamma_2.$$

Donc $\beta_1\gamma_1$ contient le facteur de p appartenant à ν, ce qui ne peut être en vertu du théorème n° **31**.

En s'appuyant sur les théorèmes établis, on démontre facilement toutes les propositions connues sur la divisibilité des nombres complexes.