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

LÉOPOLD KRONECKER

Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$

Journal de mathématiques pures et appliquées 1re série, tome 19 (1854), p. 177-192.
<http://www.numdam.org/item?id=JMPA_1854_1_19__177_0>

MÉMOIRE

SUR

LES FACTEURS IRRÉDUCTIBLES DE L'EXPRESSION $x^n - 1$;

PAR M. LÉOPOLD KRONECKER.

On sait que l'expression $x^n - 1$, n désignant un nombre entier quelconque, peut se décomposer en facteurs rationnels dont le nombre est égal à celui des diviseurs de n. En effet, en dénotant par $F_m(x) = 0$ l'équation qui ne contient que toutes les racines primitives de l'équation $x^m = 1$, on aura

$$x^n - 1 = F_d(x) \cdot F_{d'}(x) \cdot F_{d''}(x) \ldots,$$

où d, d', d'', etc., désignent tous les divers diviseurs du nombre n. On peut dire que cette manière de décomposer l'expression $x^n - 1$ correspond à la décomposition d'un nombre entier en facteurs premiers; car tous les facteurs $F_d(x)$, $F_{d'}(x)$, etc., sont irréductibles, et c'est cette propriété des fonctions $F_d(x)$, $F_{d'}(x)$, etc., bien importante pour la théorie des nombres, qui sera l'objet du présent Mémoire.

Décomposons le nombre n en ses facteurs premiers, et soit

$$n = p^a \cdot q^b \cdot r^c \ldots t^s,$$

p, q, r,..., t désignant des nombres premiers quelconques inégaux; on peut représenter de la manière suivante l'équation $F_n(x) = 0$, qui a pour racines les racines primitives de l'équation $x^n = 1$, savoir :

$$F_n(x) = \frac{(x^n - 1)\left(x^{\frac{n}{pq}} - 1\right)\left(x^{\frac{n}{pr}} - 1\right)\ldots}{\left(x^{\frac{n}{p}} - 1\right)\left(x^{\frac{n}{q}} - 1\right)\left(x^{\frac{n}{r}} - 1\right)\ldots} = 0.$$

Si l'on effectue la division, $F_n(x)$ se présentera comme fonction rationnelle et entière de x du degré

$$p^{a-1}.(p-1).q^{b-1}.(q-1)\ldots t^{g-1}.(t-1);$$

le coefficient du premier terme sera égal à 1, et tous les autres coefficients seront entiers.

En se proposant de prouver l'irréductibilité de l'équation $F_n(x)=0$, et en essayant de profiter des méthodes par lesquelles on a réussi dans le cas spécial où n est un nombre premier, on trouve que ces méthodes ne peuvent suffire, à moins que le nombre n ne soit une puissance d'un seul nombre premier (*voir* un article de M. Serret, tome XV de ce Recueil, page 296). Car si le nombre n contient des nombres premiers inégaux, la fonction $F_n(x)$ prend un caractère tout à fait différent, et il fallait des modifications essentielles pour adapter à ce cas les méthodes par lesquelles on a démontré l'irréductibilité de l'expression

$$F_p(x)=1+x+x^2+\ldots+x^{p-1},$$

p étant un nombre premier. On verra, en effet, que l'irréductibilité de $F_n(x)$ revient, au fond, à une propriété de $F_m(x)$, m désignant une des puissances p^a, q^b,..., t^g, propriété qu'on peut énoncer brièvement en disant que : *la fonction* $F_m(x)$ *est irréductible, même en admettant de certains nombres complexes.* C'est cette propriété de l'expression $F_m(x)$ qui fait voir distinctement la nature des difficultés qui s'offrent en passant du cas spécial où n ne contient qu'un seul nombre premier, au cas général où n est un nombre quelconque, et c'est cette même propriété qui sera l'objet d'un théorème auxiliaire que nous allons établir.

§ I.

THÉORÈME. — *En désignant par p un nombre premier et par a un nombre entier quelconque, je dis que l'expression*

$$1+x^{p^{a-1}}+x^{2p^{a-1}}+\ldots+x^{(p-1)p^{a-1}}$$

ne peut se décomposer en facteurs d'un moindre degré, dont les coefficients soient des fonctions rationnelles d'une racine primitive de l'unité, à moins que l'exposant de cette racine ne soit divisible par p.

Démonstration. — En désignant par $f(x)$ l'expression

$$1 + x^{p^{a-1}} + x^{2p^{a-1}} + \ldots + x^{(p-1)p^{a-1}}$$

et par ω une racine primitive quelconque de l'équation $x^{p^a} = 1$, on a, comme on sait,

$$f(x) = (x - \omega^k)(x - \omega^{k'})(x - \omega^{k''})\ldots,$$

où k, k', k'', etc., sont tous les nombres entiers positifs non divisibles par p au-dessous de p^a. Cela posé, si le théorème énoncé n'avait pas lieu, on aurait une équation

$$f(x) = \varphi(x).\psi(x), \tag{1}$$

$\varphi(x)$ et $\psi(x)$ désignant des fonctions entières de x dont les coefficients seraient des fonctions rationnelles (entières ou fractionnaires) d'une racine primitive de l'équation $\rho^{\varpi} = 1$, ϖ étant un nombre entier quelconque non-divisible par p. La fonction $f(x)$ ayant pour coefficient de la plus haute puissance de x l'unité, on peut supposer que les fonctions $\varphi(x)$ et $\psi(x)$ jouissent de la même propriété. Cela posé, on aura, en vertu de l'équation (1), deux équations de la forme

$$\begin{cases} \varphi(x) = (x - \omega^h)(x - \omega^{h'})(x - \omega^{h''})\ldots, \\ \psi(x) = (x - \omega^i)(x - \omega^{i'})(x - \omega^{i''})\ldots, \end{cases} \tag{2}$$

où h, h', h'', etc., i, i', i'', etc., sont de certains nombres non divisibles par p. Ensuite, il est clair qu'en faisant $x = 1$ les fonctions $\varphi(x)$ et $\psi(x)$ se réduiront à des fonctions rationnelles de la racine ρ. On peut donc poser

$$\begin{cases} \varphi(1) = \dfrac{A + A_1\rho + A_2\rho^2 + \ldots + A_{r-1}\rho^{r-1}}{M}, \\ \psi(1) = \dfrac{B + B_1\rho + B_2\rho^2 + \ldots + B_{r-1}\rho^{r-1}}{N}, \end{cases} \tag{3}$$

où r désigne le degré de l'équation rationnelle *irréductible*, à laquelle satisfait la racine ρ, et où M, N, A, A_1, A_2,..., A_{r-1}, B, B_1, B_2,..., B_{r-1} désignent des nombres entiers, tels que M n'ait aucun diviseur commun avec *tous* les nombres A, A_1, A_2,..., A_{r-1} et que N n'ait aucun diviseur commun avec *tous* les nombres B, B_1, B_2,..., B_{r-1}.

En observant que $f(1) = p$, on obtient, par l'équation (1),

$$\varphi(1).\psi(1) = p.$$

Donc, en remplaçant $\varphi(1)$ et $\psi(1)$ par leurs valeurs tirées de l'équation (3) et en posant, pour abréger,

$$A + A_1\rho + A_2\rho^2 + \ldots + A_{r-1}\rho^{r-1} = A(\rho),$$
$$B + B_1\rho + B_2\rho_2 + \ldots + B_{r-1}\rho^{r-1} = B(\rho),$$

on aura

$$A(\rho).B(\rho) = p.M.N. \tag{4}$$

Or, en faisant $x = 1$ dans l'une des équations (2), on obtient

$$\varphi(1) = (1-\omega^h)(1-\omega^{h'})(1-\omega^{h''})\ldots;$$

cette égalité, élevée à la puissance p^a, peut s'écrire

$$\varphi(1)^{p^a} = p.X(\omega),$$

$X(\omega)$ désignant une fonction entière de ω à coefficients entiers. En effet, en ne développant que le premier facteur $(1-\omega^h)^{p^a}$ suivant les puissances de ω^h, on voit aisément que le premier et le dernier terme se détruisent, si p est impair, et que la somme de ces deux termes est égale à 2, si p est lui-même égal à 2; tandis que les coefficients de tous les autres termes sont toujours divisibles par p. Donc, en faisant, pour abréger, $p^a = m$, l'équation

$$[Z - p.X(\omega)][Z - p.X(\omega^2)][Z - p.X(\omega^3)\ldots[Z - p.X(\omega^m)] = 0 \tag{5}$$

sera évidemment satisfaite en posant $Z = \varphi(1)^m$. En développant le le premier membre de cette équation suivant les puissances de Z, le coefficient du premier terme sera égal à 1, tandis que les coefficients des autres termes contiendront des fonctions symétriques et entières des quantités ω, ω^2, ω^3,..., ω^m, c'est-à-dire de toutes les racines de l'équation $x^m = 1$, multipliées par les diverses puissances du nombre p. Donc, comme les dites fonctions symétriques se réduisent à de simples nombres entiers, l'équation (5) prendra la forme

$$Z^m + p.u_1 Z^{m-1} + p^2.u_2 Z^{m-2} + \ldots + p^m.u_m = 0,$$

$u_1, u_2, \ldots, u_m$ désignant des nombres entiers. En substituant dans cette équation la valeur

$$Z = \varphi(1)^m = \frac{A(\rho)^m}{M^m},$$

par laquelle elle est satisfaite, on obtient une égalité de la forme suivante

$$A(\rho)^{m^2} = p.C(\rho),$$

où $C(\rho)$ désigne une fonction entière de ρ à coefficients entiers; et il est évident qu'une équation de la même forme aura lieu pour toute puissance de $A(\rho)$ dont l'exposant est plus grand que m^2. Soit donc k un nombre tel, que l'on ait $p^k > m^2$ et $p^k \equiv 1 \pmod{\varpi}$, ce qui est évidemment possible, ϖ étant premier à p; alors on aura une équation de la forme

$$A(\rho)^{p^k} = p.D(\rho).$$

Or, en développant l'expression du premier membre de cette équation, on obtient

$$A(\rho)^{p^k} = A^{p^k} + A_1^{p^k}.\rho^{p^k} + A_2^{p^k}.\rho^{2p^k} + \ldots + A_{r-1}^{p^k}.\rho^{(r-1)p^k} + p.E(\rho),$$

où $D(\rho)$ et $E(\rho)$ désignent des fonctions entières de ρ à coefficients entiers. Donc, en observant que $p^k \equiv 1 \pmod{\varpi}$, et que, par conséquent, $\rho^{p^k} = \rho$, on aura enfin

$$(6) \qquad \begin{cases} A^{p^k} + A_1^{p^k}.\rho + A_2^{p^k}.\rho^2 + \ldots + A_{r-1}^{p^k}.\rho^{r-1} \\ \quad = p.D(\rho) - p.E(\rho) = p.G(\rho), \end{cases}$$

$G(\rho)$ désignant une fonction entière de ρ à coefficients entiers *d'un degré quelconque*. Mais l'équation irréductible du degré r à laquelle satisfait la racine ρ doit être un facteur de l'équation $x^{\varpi} - 1 = 0$; donc, en vertu d'un théorème connu (*voir* GAUSS, *Disquisitiones arithmeticæ*, sect. II, art. 42), le coefficient du premier terme x^r étant égal à 1, tous les autres coefficients sont des nombres entiers. C'est pourquoi toute fonction rationnelle entière de ρ à coefficients entiers peut se réduire à une fonction dont le degré est inférieur à r et dont

les coefficients sont encore des nombres entiers. D'où il suit qu'on peut poser

$$G(\rho) = G + G_1 \rho + G_2 \rho^2 + \ldots + G_{r-1} \rho^{r-1},$$

$G, G_1, G_2, \ldots, G_{r-1}$ désignant des nombres entiers. On a donc par l'équation (6), en observant que la racine ρ ne peut satisfaire à une équation rationnelle d'un degré inférieur à r, les égalités suivantes :

$$A^{p^k} = p.G, \quad A_1^{p^k} = p.G_1, \quad A_2^{p^k} = p.G_2, \ldots, \quad A_{r-1}^{p^k} = p.G_{r-1}.$$

Il faut donc que les nombres $A, A_1, A_2, \ldots, A_{r-1}$ aient le nombre p comme diviseur commun, et, par suite, que le quotient $\frac{A(\rho)}{p}$ soit une fonction entière de ρ à coefficients entiers.

Par le même procédé, en partant de la seconde des équations (3), on obtiendra un résultat analogue; ainsi l'on trouvera que les nombres $B, B_1, B_2, \ldots, B_{r-1}$ ont le diviseur commun p, et que le quotient $\frac{B(\rho)}{p}$ est, par suite, une fonction entière de ρ à coefficients entiers. Le produit $\frac{A(\rho)}{p} \cdot \frac{B(\rho)}{p}$ sera donc lui-même une fonction entière de ρ à coefficients entiers, et en désignant cette fonction par $H(\rho)$, l'équation (4) pourra s'écrire

$$p.H(\rho) = M.N.$$

Or, en vertu de ce que nous avons exposé plus haut, la fonction $H(\rho)$ peut se réduire à un degré inférieur à r, sans que les coefficients cessent d'être des nombres entiers. On aura donc, en posant

$$H(\rho) = H + H_1 \rho + H_2 \rho^2 + \ldots + H_{r-1} \rho^{r-1},$$

où $H, H_1, H_2, \ldots, H_{r-1}$ sont des nombres entiers,

$$p.(H + H_1 \rho + H_2 \rho^2 + \ldots + H_{r-1} \rho^{r-1}) = MN,$$

d'où l'on peut conclure, comme plus haut,

$$H_1 = H_2 = \ldots = H_{r-1} = 0$$

et

$$M.N = p.H.$$

Il faut donc qu'un des nombres M ou N soit divisible par p; mais tous les nombres $A, A_1, \ldots, A_{r-1}, B, B_1, \ldots, B_{r-1}$ sont eux-mêmes divisibles par p: un des nombres M ou N aurait donc le facteur p commun avec les nombres $A, A_1, \ldots, A_{r-1}, B, B_1, \ldots, B_{r-1}$, ce qui est contre l'hypothèse; car nous avons supposé chacune des fractions (3) tellement réduite, que le dénominateur et les nombres entiers contenus comme coefficients dans le numérateur soient dégagés de tout diviseur commun.

§ II.

Maintenant, pour démontrer l'irréductibilité de l'équation qui ne contient que les racines primitives de l'équation $x^n = 1$, n étant un nombre entier quelconque, conservons les notations employées plus plus haut, et soit

$$n = p^a . q^b . r^c \ldots t^g.$$

Puis, en désignant par ϖ le nombre $q^b . r^c \ldots t^g$, supposons que l'irréductibilité de l'équation qui ne contient que les racines primitives de l'équation $x^\varpi = 1$ soit démontrée. Enfin, désignons par $\omega, \omega_1, \omega_2, \ldots, \omega_{\mu-1}$ toutes les racines primitives de l'équation $x^{p^a} = 1$, et par $\rho, \rho_1, \rho_2, \ldots, \rho_{r-1}$ celles de l'équation $x^\varpi = 1$. Cela posé, l'équation dont nous allons démontrer l'irréductibilité peut s'écrire de la manière suivante

$$(1)\quad \Pi(x - \rho.\omega_k).\Pi(x - \rho_1.\omega_k).\Pi(x - \rho_2.\omega_k)\ldots\Pi(x - \rho.\omega_k) = 0,$$

où chacun des signes Π s'étend à tous les indices de $k = 0$ jusqu'à $k = \mu - 1$. En observant que le produit $\Pi(x - \omega_k)$ est égal à

$$1 + x^{p^{a-1}} + x^{2p^{a-1}} + \ldots + x^{(p-1)p^{a-1}},$$

et, en désignant comme plus haut cette expression par $f(x)$, l'équation (1) prendra la forme

$$f\left(\frac{x}{\rho}\right) \cdot f\left(\frac{x}{\rho_1}\right) \cdot f\left(\frac{x}{\rho_2}\right) \cdots f\left(\frac{x}{\rho_{r-1}}\right) = 0.$$

Le degré de cette équation est égal à $\mu . r$, et pour en démontrer l'ir-

réductibilité il suffit de prouver que tout facteur rationnel de cette équation devrait être du même degré. Soit donc $\varphi(x)$ un facteur rationnel quelconque de l'équation précédente; on peut évidemment supposer que ce facteur s'annule pour $x = \rho\omega$; alors les équations

$$\varphi(x) = 0 \quad \text{et} \quad f\left(\frac{x}{\rho}\right) = 0$$

auront la racine commune $x = \rho\omega$; donc, en cherchant le plus grand commun diviseur des fonctions $\varphi(x)$ et $f\left(\frac{x}{\rho}\right)$, on trouvera une fonction d'un degré ≥ 1 dont les coefficients ne sauraient contenir que l'irrationnelle ρ. Si l'on désigne cette fonction par $\varphi(\rho, x)$, on aura une équation de la forme suivante :

$$f\left(\frac{x}{\rho}\right) = \varphi(\rho, x).\psi(\rho, x);$$

ou, en faisant $x = \rho Z$,

$$f(Z) = \varphi(\rho, \rho Z).\psi(\rho, \rho Z).$$

Mais, en vertu du paragraphe précédent, cette équation ne peut subsister, à moins que le degré de $\varphi(\rho, \rho Z)$ par rapport à Z ne soit égal à celui de $f(Z)$; donc le plus grand commun diviseur des fonctions $\varphi(x)$ et $f\left(\frac{x}{\rho}\right)$ doit être la fonction $f\left(\frac{x}{\rho}\right)$ elle-même, et l'on aura, par suite, une équation telle que

$$\varphi(x) = f\left(\frac{x}{\rho}\right) \cdot \psi(\rho, x), \tag{2}$$

où $\psi(\rho, x)$ désigne une fonction entière de x, dont les coefficients sont des fonctions rationnelles de ρ. Comme nous avons supposé l'irréductibilité de l'équation dont les racines sont ρ, ρ_1, $\rho_2, \ldots, \rho_{r-1}$, on peut évidemment changer dans l'équation (2) successivement ρ en ρ_1, $\rho_2, \ldots, \rho_{r-1}$; en d'autres termes, la fonction $\varphi(x)$ n'est pas seulement divisible par $f\left(\frac{x}{\rho}\right)$, mais aussi par $f\left(\frac{x}{\rho_1}\right), f\left(\frac{x}{\rho_2}\right), \ldots, f\left(\frac{x}{\rho_{r-1}}\right)$. Il n'y a pas de facteur commun à deux de ces fonctions, car le produit de toutes ces fonctions étant diviseur de l'expression $x^n - 1$,

l'équation $x^n = 1$ aurait des racines égales, ce qui n'a pas lieu. Par conséquent, la fonction $\varphi(x)$ doit être divisible par le produit

$$f\left(\frac{x}{\rho}\right) \cdot f\left(\frac{x}{\rho_1}\right) \cdot f\left(\frac{x}{\rho_2}\right) \cdots f\left(\frac{x}{\rho_{r-1}}\right)$$

qui est du degré $\mu . r$; elle ne saurait donc être d'un degré inférieur à $\mu . r$; ce qu'il fallait démontrer.

La démonstration qui précède repose sur l'hypothèse de l'irréductibilité de l'équation qui contient les racines primitives de l'équation $x^{\varpi} = 1$; donc, en conservant les notations employées plus haut, l'irréductibilité de $F_u(x)$ dépend de celle de $F_{\varpi}(x)$. Par le même procédé, on voit que l'irréductibilité de $F_{\varpi}(x)$ dépend de celle de $F_{\varpi'}(x)$, où $\varpi' = r^c . s^d \ldots t^g$; et en continuant ainsi, l'on voit que, pour compléter la démonstration qui est l'objet de ce paragraphe, il ne s'agit que de prouver l'irréductibilité de $F_{\tau}(x)$ où $\tau = t^g$. Or c'est ce qui a été fait dans le paragraphe précédent, comme on peut s'en assurer en y supposant $p^a = t^g$, $\varpi = 1$, et, par suite, $\rho = 1$.

§ III.

La méthode que je viens d'exposer suffit pour démontrer le théorème plus général que voici :

THÉORÈME. — *En désignant par n un nombre entier quelconque et par α une racine d'une équation irréductible à coefficients entiers dont le premier soit égal à 1; en supposant, enfin, que le déterminant de cette équation soit premier à n; je dis que l'équation qui ne contient que les racines primitives de l'équation* $x^n - 1$ *reste irréductible, même en adjoignant la quantité α; c'est-à-dire, elle ne peut se décomposer en facteurs dont le degré soit inférieur à celui de l'équation et dont les coefficients soient des fonctions rationnelles de la quantité α.*

En effet, en conservant toujours les notations employées précédemment et en supposant que l'équation qui ne contient que les racines primitives de l'équation $p^{\varpi} = 1$ reste irréductible en adjoignant la

quantité α, on peut se servir de la méthode exposée pour démontrer le théorème énoncé, si l'on veut prouver que :

L'expression $1 + x^{p^{a-1}} + x^{2p^{a-1}} + \ldots + x^{(t-1)p^{a-1}}$ *n'est pas décomposable en facteurs d'un moindre degré dont les coefficients soient des fonctions rationnelles des deux quantités* ρ *et* α.

C'est donc à l'aide de ce second théorème qu'on pourra employer les conclusions du paragraphe précédent pour ramener finalement le théorème énoncé plus haut à un cas spécial du même théorème, savoir à celui où n est une puissance d'un nombre premier. Or il est visible que pour une telle valeur de n le premier théorème est en même temps un cas spécial du second théorème, savoir en y faisant $\varpi = 1$, et, par suite, $\rho = 1$. Il ne s'agit donc que de prouver généralement ce second théorème, en supposant que l'équation $F_\varpi(x) = 0$ reste irréductible en adjoignant la quantité α. Ce qu'on peut faire comme il suit.

Supposons que le théorème en question n'ait pas lieu et conservons les notations employées dans le § I. Alors on aura, comme plus haut, les équations

$$f(x) = \varphi(x).\psi(x), \tag{1}$$

$$\begin{cases} \varphi(x) = (x - \omega^h)(x - \omega^{h'})(x - \omega^{h''})\ldots, \\ \psi(x) = (x - \omega^i)(x - \omega^{i'})(x - \omega^{i''})\ldots, \end{cases} \tag{2}$$

où $\varphi(x)$ et $\psi(x)$ désignent des fonctions entières de x dont les coefficients sont des fonctions rationnelles des deux quantités α et ρ. Donc, en faisant $x = 1$, les fonctions $\varphi(x)$ et $\psi(x)$ sont réductibles à la forme suivante

$$\begin{cases} \varphi(1) = \dfrac{A(\alpha) + A_1(\alpha).\rho + A_2(\alpha).\rho^2 + \ldots + A_{r-1}(\alpha).\rho^{r-1}}{M}, \\ \psi(1) = \dfrac{B(\alpha) + B_1(\alpha)\,\rho + B_2(\alpha).\rho^2 + \ldots + B_{r-1}(\alpha).\rho^{r-1}}{N}, \end{cases} \tag{3}$$

où M et N désignent des nombres entiers, tandis que $A(\alpha)$, $A_1(\alpha)$, $A_2(\alpha), \ldots, A_{r-1}$, $B(\alpha)$, $B_1(\alpha)$, $B_2(\alpha), \ldots, B_{r-1}(\alpha)$ désignent des fonctions entières de α à coefficients entiers d'un degré inférieur à celui de l'équation irréductible, à laquelle satisfait la racine α. La lettre r dé-

signe le degré de l'équation irréductible $F_\varpi(x) = 0$. En outre, on peut supposer que chacune des deux fractions (3) soit tellement réduite, que le dénominateur n'ait aucun diviseur qui soit en même temps un facteur commun de tous les nombres entiers contenus comme coefficients dans le numérateur.

Or, en dénotant, pour abréger, par $A(\alpha, \rho)$ et $B(\alpha, \rho)$ respectivement les numérateurs des deux fractions (3), on aura, comme plus haut,

$$A(\alpha, \rho) \cdot B(\alpha, \rho) = p \cdot M \cdot N, \tag{4}$$

et, en suivant tout à fait la marche expliquée dans le § 1, on arrive à l'équation correspondante à celle du § 1, (6),

$$\begin{aligned} &A(\alpha)^{p^k} + A_1(\alpha)^{p^k} \cdot \rho + A_2(\alpha)^{p^k} \cdot \rho^2 + \dots \\ &\qquad + A_{r-1}(\alpha)^{p^k} \cdot \rho^{r-1} = p \cdot G(\alpha, \rho), \end{aligned} \tag{5}$$

$G(\alpha, \rho)$ désignant une fonction rationnelle entière de α et ρ à coefficients entiers.

En vertu de ce que nous avons dit plus haut on sait que l'équation irréductible $F_\varpi(x) = 0$, à laquelle satisfait la racine ρ, jouit de la propriété d'avoir pour coefficients des nombres entiers et celui du premier terme égal à 1. Donc le degré de $F_\varpi(x)$ étant égal à r, la fonction $G(\alpha, \rho)$, quel que soit son degré par rapport à ρ, peut se réduire à la forme

$$G(\alpha, \rho) = G(\alpha) + G_1(\alpha) \cdot \rho + G_2(\alpha) \cdot \rho^2 + \dots + G_{r-1}(\alpha) \cdot \rho^{r-1},$$

$G(\alpha), G_1(\alpha), G_2(\alpha), \dots, G_{r-1}(\alpha)$ désignant des fonctions entières de α à coefficients entiers. Donc l'équation (5) peut s'écrire

$$\begin{aligned} &A(\alpha)^{p^k} + A_1(\alpha)^{p^k} \cdot \rho + A_2(\alpha)^{p^k} \cdot \rho^2 + \dots + A_{r-1}(\alpha)^{p^k} \cdot \rho^{r-1} \\ &+ p \cdot G(\alpha) + p \cdot G_1(\alpha) \cdot \rho + p \cdot G_2(\alpha) \cdot \rho^2 + \dots + p \cdot G_{r-1}(\alpha) \cdot \rho^{r-1}, \end{aligned}$$

ce qui entraîne les équations

$$\begin{cases} A(\alpha)^{p^k} = p \cdot G(\alpha), \\ A_1(\alpha)^{p^k} = p \cdot G_1(\alpha), \\ A_2(\alpha)^{p^k} = p \cdot G_2(\alpha), \dots, \\ A_{r-1}(\alpha)^{p^k} = p \cdot G_{r-1}(\alpha). \end{cases} \tag{6}$$

Car nous avons supposé que l'équation $F_\varpi(x) = 0$, à laquelle satisfait la racine ρ, reste irréductible en adjoignant la quantité α; la racine ρ ne peut donc satisfaire à une équation d'un degré inférieur à celui de $F_\varpi(x)$ dont les coefficients soient des fonctions rationnelles de α.

Désignons maintenant par $\varphi(x) = 0$ l'équation irréductible à laquelle satisfait la racine α, et par $\beta, \gamma, \ldots, \theta$ ses autres racines. Puis considérons une quelconque des égalités (6), par exemple la première, et posons, en dénotant par λ le degré de $\varphi(x)$,

$$A(\alpha) = a + b\alpha + c\alpha^2 + \ldots + l\alpha^{\lambda-1},$$

$a, b, c, \ldots, l$ désignant des nombres entiers. Alors on a, par une formule connue,

$$(7) \qquad A(Z) = \frac{A(\alpha)}{\varphi'(\alpha)} \cdot \frac{\varphi(Z)}{Z-\alpha} + \frac{A(\beta)}{\varphi'(\beta)} \cdot \frac{\varphi(Z)}{Z-\beta} + \ldots + \frac{A(\theta)}{\varphi'(\theta)} \cdot \frac{\varphi(Z)}{Z-\theta},$$

où $\varphi'(Z)$ est la fonction dérivée de $\varphi(Z)$. Désignons par Δ le déterminant de l'équation $\varphi(Z) = 0$, ainsi qu'on a

$$\Delta = \varphi'(\alpha) \cdot \varphi'(\beta) \cdot \varphi'(\gamma) \ldots \varphi'(\theta),$$

et faisons

$$\frac{\Delta}{\varphi'(\alpha)} \cdot \frac{\varphi'(Z)}{Z-\alpha} = \psi(\alpha, Z),$$

où $\psi(\alpha, Z)$ est évidemment une fonction rationnelle entière de α et Z à coefficients entiers. Cela posé, l'équation (7) peut s'écrire

$$\Delta \cdot a + \Delta \cdot bZ + \Delta \cdot cZ^2 + \ldots + \Delta \cdot lZ^{\lambda-1} = A(\alpha) \cdot \psi(\alpha, Z) + A(\beta) \cdot \psi(\beta, Z) + \ldots + A(\theta) \cdot \psi(\theta, Z).$$

En comparant les coefficients des diverses puissances de la variable Z, on obtient, pour chacun des coefficients $a, b, c, \ldots, l$, par exemple pour le coefficient h, une équation de la forme

$$\Delta \cdot h = A(\alpha) \cdot V(\alpha) + A(\beta) \cdot V(\beta) + \ldots + A(\theta) \cdot V(\theta),$$

$V(\alpha)$ désignant une fonction entière de α à coefficients entiers. En élevant cette égalité à la puissance p^k et en réunissant ceux des termes du second membre, dont les coefficients sont divisibles par p, il ré-

sulte une équation de la forme suivante

$$(8)\qquad \begin{cases} \Delta^{p^k}.h^{p^k} = \mathrm{A}(\alpha)^{p^k}.\mathrm{V}(\alpha)^{p^k} + \mathrm{A}(\beta)^{p^k}.\mathrm{V}(\beta)^{p^k} + \dots \\ \qquad\qquad + \mathrm{A}(\theta)^{p^k}.\mathrm{V}(\theta)^{p^k} + p.\mathrm{W}(\alpha,\beta,\dots,\theta), \end{cases}$$

où $\mathrm{W}(\alpha,\beta,\dots,\theta)$ désigne une fonction rationnelle entière des racines $\alpha,\beta,\dots,\theta$ à coefficients entiers. Or il est visible que cette fonction est symétrique; elle se réduit donc à un simple nombre entier. Désignons ce nombre par P et observons que $\varphi(x)=0$ étant irréductible, l'équation (6)

$$\mathrm{A}(\alpha)^{p^k} = p.\mathrm{G}(\alpha)$$

entraîne les équations

$$\mathrm{A}(\beta)^{p^k} = p.\mathrm{G}(\beta),\quad \mathrm{A}(\gamma)^{p^k} = p.\mathrm{G}(\gamma),\dots,\quad \mathrm{A}(\theta)^{p^k} = p.\mathrm{G}(\theta).$$

Donc, en faisant usage de ces égalités, l'équation (8) se change en celle-ci :

$$(9)\qquad \Delta^{p^k}.h^{p^k} = p.\left[\begin{matrix}\mathrm{G}(\alpha).\mathrm{V}(\alpha)^{p^k} + \mathrm{G}(\beta).\mathrm{V}(\beta)^{p^k} + \dots \\ \qquad\qquad + \mathrm{G}(\theta).\mathrm{V}(\theta)^{p^k}\end{matrix}\right] + p.\mathrm{P}.$$

L'expression contenue entre les parenthèses est une fonction entière symétrique des racines $\alpha,\beta,\dots,\theta$ et à coefficients entiers; elle se réduit donc à un simple nombre entier; car dans l'équation $\varphi(x)=0$ (qui a pour racines $\alpha,\beta,\dots,\theta$), tous les coefficients sont supposés être des nombres entiers et celui du premier terme égal à 1. Par suite, l'équation (9) entraîne la congruence

$$\Delta^{p^k}.h^{p^k} \equiv 0 \pmod{p},$$

et, enfin, Δ étant supposé premier au nombre n qui est divisible par p,

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

c'est-à-dire : *Il faut que tous les coefficients de* $\mathrm{A}(\alpha)$ *soient divisibles par* p".

On peut conclure de la même manière que tous les coefficients contenus dans $\mathrm{A}_1(\alpha), \mathrm{A}_2(\alpha),\dots, \mathrm{A}_{r-1}(\alpha)$, de même que les coefficients contenus dans $\mathrm{B}(\alpha), \mathrm{B}_1(\alpha), \mathrm{B}_2(\alpha),\dots, \mathrm{B}_{r-1}(\alpha)$ doivent être divisibles par p. Les quotients $\frac{\mathrm{A}(\alpha,p)}{p}$ et $\frac{\mathrm{B}(\alpha,p)}{p}$ seront, par suite, des fonctions

entières de α et ρ à coefficients entiers. Donc, en posant

$$\frac{A(\alpha,\rho)}{p}\cdot\frac{B(\alpha,\rho)}{p}=H(\alpha,\rho),$$

l'expression $H(\alpha,\rho)$ sera elle-même une fonction entière de α et ρ à coefficients entiers; et, à l'aide de cette égalité, l'équation (4) peut s'écrire

$$p.H(\alpha,\rho)=M.N.$$

Or, en vertu de ce que nous avons dit plus haut, la fonction $H(\alpha,\rho)$ est réductible à la forme

$$H(\alpha,\rho)=H(\alpha)+H_1(\alpha).\rho+H_2(\alpha).\rho^2+\ldots+H_{r-1}(\alpha).\rho^{r-1},$$

$H(\alpha)$, $H_1(\alpha)$, $H_2(\alpha)$,..., $H_{r-1}(\alpha)$ désignant des fonctions entières de α et ρ à coefficients entiers. On a donc

$$p.H(\alpha)+p.H_1(\alpha).\rho+p.H_2(\alpha).\rho^2+\ldots+p.H_{r-1}(\alpha).\rho^{r-1}=M.N;$$

d'où il suit, en ayant égard à ce que nous avons supposé, que l'équation irréductible du degré r, dont ρ est une racine, reste irréductible en adjoignant la quantité α,

$$p.H(\alpha)=M.N. \tag{10}$$

Rappelons encore que, dans l'équation irréductible à laquelle satisfait la racine α, tous les coefficients sont supposés être des nombres entiers et celui du premier terme égal à 1. Donc, en dénotant comme plus haut par λ le degré de cette équation, l'expression $H(\alpha)$ est réductible à la forme

$$H(\alpha)=h+h_1\alpha+h_2\alpha^2+\ldots+h_{\lambda-1}\alpha^{\lambda-1},$$

h, h_1, h_2,..., $h_{\lambda-1}$ désignant des nombres entiers, en substituant cette valeur de $H(\alpha)$ dans l'équation (10) et en observant que la racine α ne peut satisfaire à une équation rationnelle d'un degré inférieur à λ, on arrive à l'égalité suivante

$$p.h=M.N.$$

Il faut donc qu'un des nombres M ou N soit divisible par p; mais

nous avons prouvé que tous les nombres contenus comme coefficients dans $A(\alpha, \rho)$ et $B(\alpha, \rho)$ sont divisibles par p; un des nombres M ou N aurait donc le facteur p commun avec tous les coefficients de $A(\alpha, \rho)$ et $B(\alpha, \rho)$, ce qui est contre l'hypothèse: car nous avons supposé chacune des fractions (3) tellement réduite, que le dénominateur et les nombres entiers contenus comme coefficients dans le numérateur soient débarrassés de tout diviseur commun.

§ IV.

Nous avons assujetti dans le paragraphe précédent la quantité α à la condition d'être la racine d'une équation irréductible dont le déterminant soit premier au nombre n. Cependant on peut encore simplifier cette condition en supprimant le mot *irréductible*. Car nous allons voir que l'équation *irréductible* $\varphi(x) = 0$, dont α est une racine, remplit la condition proposée, si le déterminant d'une équation *quelconque* $F(x) = 0$ à laquelle satisfait la racine α est premier à n.

En effet, soit

$$F(x) = \varphi(x) . \psi(x),$$

$\psi(x)$ désignant [de même que $F(x)$ et $\varphi(x)$] une fonction entière de x à coefficients entiers, dont le premier soit égal à 1. Puis dénotons, comme plus haut, par $\alpha, \beta, \gamma, \ldots, \vartheta$ toutes les racines de l'équation $\varphi(x) = 0$, et par $a, b, c, \ldots, k$ celles de l'équation $\psi(x) = 0$. Alors, en désignant par D, Δ, Δ_1 respectivement les déterminants des équations $F(x) = 0$, $\varphi(x) = 0$, $\psi(x) = 0$, et, en employant les notations ordinaires des dérivées de $F(x)$, $\varphi(x)$ et $\psi(x)$, on aura l'égalité

$$(1) \qquad D = F'(\alpha) . F'(\beta) \ldots F'(\vartheta) . F'(a) . F'(b) \ldots F'(k).$$

Remplaçons les facteurs du second membre par les valeurs tirées de l'équation

$$F'(x) = \varphi'(x) . \psi(x) + \psi'(x) . \varphi(x),$$

et observons que

$$\varphi(\alpha) = \varphi(\beta) = \ldots = \varphi(\vartheta) = 0,$$

de même que

$$\psi(a) = \psi(b) = \ldots = \psi(k) = 0.$$

Alors l'égalité (1) se change en celle-ci :

$$D = \varphi'(\alpha).\psi(\alpha).\varphi'(\beta).\psi(\beta)\ldots \times \varphi'(\theta).\psi(\theta).\psi'(a).\varphi(a).\psi'(b).\varphi(b)\ldots\psi'(k).\varphi(k),$$

équation qui peut s'écrire comme il suit :

$$D = \Delta.\Delta_1.\psi(\alpha).\psi(\beta)\ldots\psi(\theta).\varphi(a).\varphi(b)\ldots\varphi(k).$$

Les produits dans le second membre de cette équation se réduisent évidemment à de simples nombres entiers, d'où il suit que

$$D \text{ divisible par } \Delta.\Delta_1.$$

Donc si D est premier à un nombre quelconque n, le déterminant Δ jouit de la même propriété; ce qu'il fallait démontrer.

D'après ce que nous venons d'exposer, on peut énoncer le théorème général du paragraphe précédent de la manière suivante :

Tous les facteurs irréductibles de l'expression $x^n - 1$ *restent irréductibles même si l'on adjoint une quantité* α *qui satisfait à une équation à coefficients entiers dont le premier est l'unité, pourvu que le déterminant de cette équation soit un nombre premier à* n.

Pour donner une seule application de ce théorème, supposons que α soit une racine primitive de l'équation $x^m = 1$. Donc, le déterminant de cette équation étant égal à m^m, les conditions du théorème seront remplies si l'on suppose que m soit premier à n. D'où l'on voit que *tous les facteurs irréductibles de l'expression* $x^n - 1$ *restent irréductibles en adjoignant une racine primitive de l'unité dont l'exposant est premier à* n. Or il est visible que celui des facteurs de la fonction $x^n - 1$, que nous avons désigné par $F_n(x)$, cesse d'être irréductible si l'on adjoint une racine primitive de l'unité telle, que son exposant ait un diviseur commun avec le nombre n. On a donc, enfin, ce résultat qui comprend comme cas spécial le théorème énoncé dans le § I :

Afin que l'équation qui ne contient que toutes les racines primitives de l'équation $x^n - 1$ *devienne réductible en adjoignant une racine primitive de l'unité, il faut et il suffit que l'exposant de cette racine ait un diviseur commun avec le nombre* n.