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

V.-A. LEBESGUE

Démonstration de l'irréductibilité de l'équation aux racines primitives de l'unité

Journal de mathématiques pures et appliquées 2^e série, tome 4 (1859), p. 105-110.
<http://www.numdam.org/item?id=JMPA_1859_2_4__105_0>

DÉMONSTRATION

DE

L'IRRÉDUCTIBILITÉ DE L'ÉQUATION AUX RACINES PRIMITIVES DE L'UNITÉ;

PAR M. V.-A. LEBESGUE.

Une racine de l'équation

$$x^n = 1$$

est dite primitive quand toutes ses puissances ρ, ρ^2, ρ^3, ..., ρ^{n-1}, $\rho^n = 1$ sont différentes et composent la suite complète des racines de l'équation

$$x^n = 1.$$

Cela arrive par exemple quand on prend

$$\rho = \cos\frac{2\pi}{n} + \sin\frac{2\pi}{n}\sqrt{-1}.$$

La puissance ρ^α est encore racine primitive si α est premier à n, mais cela n'arrive pas dans le cas contraire, car si δ diviseur de n divisait aussi α, on aurait alors

$$(\rho^\alpha)^{\frac{n}{\delta}} = 1.$$

Si l'on pose

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

les nombres p, q, r, etc., étant premiers et différents, et

$$\varphi(n) = p^{a-1}(p-1)\,q^{b-1}(q-1)\ldots,$$

les racines primitives seront en nombre $\varphi(n)$, et l'équation aux racines primitives sera

$$F(x) = 0.$$

La règle pour former le polynôme $F(x)$ à coefficients entiers est

bien connue : on peut la voir dans les *Exercices* de M. Cauchy, année 1829.

L'irréductibilité de l'équation

$$F(x) = 0$$

assez facile à établir pour

$$n = p \quad \text{et} \quad n = p^a,$$

le nombre p étant supposé premier, paraissait l'être beaucoup moins pour le cas général. En 1854 M. Kronecker a donné la démonstration complète dans le t. XIX du *Journal de Mathématiques*, en employant, pour obtenir des théorèmes plus généraux, la théorie des nombres complexes formés avec les racines de l'unité. Depuis, M. Arndt (Journal de Crelle, t. LVI, p. 178) a donné une démonstration plus courte. En cherchant à éclaircir sa Note, dont la seconde partie est rendue obscure par une faute d'impression qui ne se découvre pas immédiatement, j'ai complété une démonstration commencée depuis longtemps et que le Mémoire de M. Kronecker m'avait semblé rendre inutile.

La voici cependant; elle est assez facile à suivre. Ce n'est qu'une modification de la démonstration de M. Arndt.

PROPOSITION I. — *Soit*

$$F(x) = 0$$

l'équation aux racines primitives de l'équation

$$x^n = 1,$$

de plus

$$n = p^a q^b r^c \ldots, \quad \varphi(n) = p^{a-1}(p-1)\, q^{b-1}(q-1)\ldots,$$

comme il a été dit plus haut, et

$$n = p^a n' :$$

on aura, en posant $x'^{n'} = 1$,

$$p = F(x').G(x'),$$

et, pour $n' = 1$,

$$p = F(1),$$

la caractéristique G *indiquant une fonction de* x *à coefficients entiers comme* F, *et qui se réduit à l'unité pour* $n' = 1$.

Quand n *renferme plusieurs nombres premiers différents, on a toujours*

$$F(1) = 1.$$

N. B. Cette dernière partie n'étant pas nécessaire pour la démonstration de l'irréductibilité, sa démonstration est omise.

PROPOSITION II. — *Si l'équation*

$$F(x) = 0$$

est réductible, on aura

$$F(x) = f_1(x) f_2(x) \dots f_r(x),$$

les polynômes irréductibles $f_i(x)$ *à coefficients entiers étant tous de même degré.*

PROPOSITION III. — *La proposition I montre que la décomposition supposée dans la proposition II est impossible ; de là résulte l'irréductibilité de l'équation* $F(x) = 0$, *quel que soit l'exposant* n.

Voici la démonstration de la proposition I :

On a

$$(a) \quad \frac{x^n - 1}{x^{\frac{n}{p}} - 1} = \left(x^{\frac{n}{p}}\right)^{p-1} + \left(x^{\frac{n}{p}}\right)^{p-2} + \dots + x^{\frac{n}{p}} + 1 = F(x) \cdot G(x).$$

Pour $n = p^a$, on voit, par ce qui précède, que

$$G(x) = 1.$$

Ainsi, pour $x = 1$ on a, dans ce cas,

$$p = F(1).$$

En général, si

$$x'^{n'} = 1 \quad \text{ou} \quad x'^{\frac{n}{p^a}} = 1,$$

il en résulte

$$x'^{\frac{n}{p}} = 1,$$

et, par conséquent, l'identité (a) donne

$$p = F(x') \cdot G(x').$$

La démonstration des propositions II et III dépend de théorèmes bien connus. Si de l'équation à coefficients entiers

$$f(x) = x^m + Ax^{m-1} + Bx^{m-2} + \ldots + M = 0,$$

où les racines sont $\alpha, \beta, \gamma, \ldots$, on passe à l'équation de même degré

$$\mathcal{F}(x') = x'^m + A_1 x'^{m-1} + B_1 x'^{m-2} + \ldots + M_1 = 0,$$

où les racines sont $\alpha^k, \beta^k, \gamma^k, \ldots$, k étant un entier positif, les coefficients $A_1, B_1, C_1, \ldots, M_1$ sont entiers. Cela suffit pour établir la proposition II; mais pour la proposition III, il faut ajouter que si $k = p^a$, le nombre p étant premier, les coefficients $A_1, B_1, C_1, \ldots$ se changent, en supposant $A', B', C', \ldots$ entiers, en

$$A + pA', \quad B + pB', \quad C + pC' \ldots;$$

de là, en posant $x^{p^a} = x'$, on a l'identité

$$(b) \qquad f(x') + p\psi(x') = \mathcal{F}(x')$$

où, ce qu'il faut remarquer, $\psi(x')$ est aussi bien que $f(x')$ une fonction entière à coefficients entiers.

Démonstration de la proposition II.

Admettons que l'on ait

$$F(x) = f_1(x) f_2(x) \ldots f_\nu(x),$$

les différents facteurs $f_i(x)$ étant irréductibles et à coefficients entiers. Soit

$$f_i(x) = (x - \rho^\alpha)(x - \rho^\beta) \ldots$$

et

$$f_k(x) = (x - \rho^{\alpha'})(x - \rho^{\beta'}) \ldots;$$

ρ étant une racine primitive, et $\alpha, \beta, \ldots, \alpha', \beta', \ldots$ des nombres premiers à n. Si le degré de $f_i(x)$ surpasse celui de $f_k(x)$, en posant

$$\alpha j = hn + \alpha',$$

et passant de l'équation $f_i(x) = 0$ à l'équation $f_i(x^j) = 0$, on changerait le polynôme $f_i(x)$ en un autre de même degré ayant le facteur $x - \rho^{\alpha'}$, et il s'ensuivrait que $f_i(x)$ pourrait se décomposer, ce qui est contre l'hypothèse. Il se trouve donc prouvé que les facteurs $f_i(x)$ sont nécessairement de même degré.

Démonstration de la proposition III.

Si d'abord on suppose

$$n = p^a,$$

et que l'on ait

$$F(x) = f_1(x) f_2(x) \dots f_\nu(x),$$

on trouvera

$$f_1(x') + p\psi_1(x') = \mathcal{F}_1(x'),$$

d'après l'équation (b); or ici

$$x^{p^a} = 1,$$

$\mathcal{F}_i(x')$ devient une puissance de $x' - 1$ et s'annule pour $x' = 1$: ainsi

$$f_1(1) = -p\psi_1(1);$$

en multipliant membre à membre toutes les équations semblables, on aura, en posant $(-1)^\nu \psi_1(1)\psi_2(1)\dots\psi_\nu(1) = \Psi(1)$, l'équation

$$F(1) = p^\nu . \Psi(1)$$

et, par suite,

$$1 = p^{\nu-1} . \Psi(1);$$

ce qui est impossible, $\Psi(1)$ étant entier.

Quand on a

$$n = p^a q^b,$$

l'équation transformée

$$\mathcal{F}_i(x') = 0$$

n'a plus toutes ses racines égales à l'unité; mais comme pour avoir

$$(x^{p^a})^m = 1$$

il faut prendre m multiple de n' $(n = p^a . n')$, l'équation

$$\mathcal{F}_i(x') = (x' - \rho^{\alpha p^a}) \dots = 0$$

a pour racines seulement des racines primitives de

$$x'^{m'} = 1 \quad \text{ou} \quad x'^{q^b} = 1.$$

Or l'équation qui donne les racines primitives de l'équation $x'^{q^b} = 1$ est irréductible; il faut donc que l'équation

$$\mathcal{F}_i(x') = 0$$

les contienne toutes; ainsi, en représentant l'une d'elles par x', on aura nécessairement, en vertu de l'équation

$$f_i(x') + p\psi_i(x') = \mathcal{F}_i(x')$$

l'équation

$$f_i(x') = -p\psi_i(x').$$

La multiplication des ν équations analogues donnera

$$\mathrm{F}(x') = p^\nu \Psi(x');$$

mais

$$p = \mathrm{F}(x').\mathrm{G}(x'),$$

de là

$$p = p^\nu \Psi(x').\mathrm{G}(x') = p^\nu \xi(x')$$

ou

$$(c) \qquad 1 = p^{\nu-1}\xi(x').$$

Or l'équation en x' est irréductible et de degré

$$\varphi(q^b) = \lambda,$$

donc $\xi(x')$ se ramène à la forme

$$\mathrm{A}_0 + \mathrm{A}_1 x' + \ldots + \mathrm{A}_{\lambda-1} x'^{\lambda-1},$$

de sorte que l'équation (c) devenant

$$-1 + p^{\nu-1}\left(\mathrm{A}_0 + \mathrm{A}_1 x' + \ldots + \mathrm{A}_{\lambda-1} x'^{\lambda-1}\right) = 0,$$

le premier membre devrait être identiquement nul, ce qui est impossible, $-1 + p^{\nu-1}\mathrm{A}_0$ ne pouvant l'être.

Ainsi, l'équation $\mathrm{F}(x) = 0$ est irréductible pour $n = p^a q^b$.

Si l'on fait maintenant $n = p^a q^b r^c = p^a n'$, $n' = q^b r^c$, la démonstration se donnera précisément dans les mêmes termes, parce que l'irréductibilité est prouvée pour $n' = q^b r^c$. La démonstration s'établit donc de proche en proche.

Le lecteur verra facilement, en consultant la Note de M. Arndt, ce que j'y ai pris, et quelle est la part qui me revient dans la démonstration précédente.