NOUVELLES ANNALES DE MATHÉMATIQUES

Nouvelle démonstration de l'irréductibilité de l'équation $1 + x + x^2 + \ldots + x^{p-1} = 0$; p étant un nombre premier. D'après M. L. Kronecker, étudiant à Berlin

Nouvelles annales de mathématiques 1re série, tome 8 (1849), p. 419-421

<http://www.numdam.org/item?id=NAM_1849_1_8__419_1>

NOUVELLE DÉMONSTRATION

De l'irréductibilité de l'équation $1 + x + x^2 + \ldots + x^{p-1} = 0$; p étant un nombre premier;

D'APRÈS M. L. KRONECKER,
Etudiant a Berlin.

(Journal de M. Crelle, tome XXIX, page 280; 1845.)

1. *Lemme.* p étant un nombre premier, soit α une racine imaginaire de l'équation $x^p - 1 = 0$; $a, a_1 \ldots a_{p-1}$ sont p nombres entiers donnés; faisant

$$a + a_1 x + a_2 x^2 + \ldots + a_{p-1} x^{p-1} = f(x),$$

et

$$a + a_1 + a_2 + \ldots + a_{p-1} = f(1) = \mathrm{A}, \quad f(\alpha) f(\alpha^2) \ldots f(\alpha^{p-1}) = \mathrm{B}.$$

On sait que B est un nombre rationnel entier; on aura

$$\mathrm{B} - \mathrm{A}^{p-1} = \dot{p} \ (*).$$

Démonstration. Posant

$$a + a_1 x + a_2 x^2 + \ldots + a_n x^{p-1} = f(x),$$

(*) Je designe par le point leibnitzien place au-dessus d'un nombre le multiple de ce nombre.

on aura

$$f(x)f(x^2)\dots f(x^{p-1}) = M_0 + M_1 x + M_2 x^2 + \dots + M_n x^n + \dots.$$

Faisant successivement x égal à 1, α, $\alpha^2 \dots \alpha^{p-1}$, le membre à gauche devient d'abord A^{p-1}, et pour les autres racines le produit reste toujours égal à B; il n'y a de changement que dans l'ordre des facteurs. Donc la somme de ces membres à gauche est $A^{p-1} + (p-1)B$. Prenons dans le membre à droite le terme général $M_n x^n$, la somme sera

$$M_n[1 + \alpha^n + \alpha^{2n} + \dots + \alpha^{(p-1)n}].$$

On sait que lorsque n n'est pas un multiple de p, ce qui multiplie M_n est nul; et lorsque n est un multiple de p, ce coefficient est égal à p; donc

$$A^{p-1} + (p-1)B = p(M_0 + M_p + M_{2p} + \dots);$$

de là

$$B - A^{p-1} = p. \qquad C.\ Q.\ F.\ D.$$

Théorème II. *La fonction* $X = 1 + x + x^2 + \dots + x^{p-1}$, *où p est un nombre premier, ne peut être le produit de deux fonctions rationnelles à coefficients entiers.*

Démonstration. Soit

$$X = \varphi(x)\ \psi(x),$$

φ et ψ sont des fonctions rationnelles à coefficients entiers; ils ne peuvent avoir des coefficients fractionnaires (t. III, p. 47); faisant $x = 1$, on obtient

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

il faut que l'une de ces deux valeurs $\varphi(1)$ et $\psi(1)$ soit égale à l'unité et l'autre à p. Supposons donc $\varphi(1) = 1$; α étant une racine imaginaire quelconque de $X = 0$, on a, d'après le lemme,

$$\varphi(\alpha)\ \varphi(\alpha^2) \dots \varphi(\alpha^{p-1}) - 1 = p;$$

car

$$A = \varphi(1) = 1.$$

En prenant pour α une racine commune à $X = 0$ et $\varphi(x) = 0$, on aurait donc $-1 = \dot{p}$, résultat absurde; donc, etc.

Remarque. Ce théorème fondamental est dans les *Disquisitiones arithmeticæ*, p. 599, § CCCXLI; et l'on en trouve aussi une démonstration dans Legendre. Celle de M. Kronecker semble la plus simple.