BULLETIN DES SCIENCES

MATHÉMATIQUES ET ASTRONOMIQUES

A.-E. PELLET

Sur une classe d'équations dont toutes les racines peuvent s'exprimer linéairement en fonction de l'une d'elles

Bulletin des sciences mathématiques et astronomiques 2e série, tome 4, nº 1 (1880), p. 262-265

<http://www.numdam.org/item?id=BSMA_1880_2_4_1_262_0>

MÉLANGES.

SUR UNE CLASSE D'ÉQUATIONS DONT TOUTES LES RACINES PEUVENT S'EXPRIMER LINÉAIREMENT EN FONCTION DE L'UNE D'ELLES;

PAR M. A.-E. PELLET.

1. Dans un Mémoire présenté à l'Académie des Sciences le 10 mai 1880, j'ai montré que, si les racines d'une équation de degré m peuvent être représentées par x, $\theta(x), \ldots, \theta^{m-1}(x)$, x étant l'une quelconque d'entre elles et $\theta(x)$ représentant une fonction linéaire $\frac{ax+b}{a'x+b'}$ telle que $\theta^m(x) = x$ identiquement, cette équation peut se mettre sous la forme

$$A(x+\lambda)^m + B(x+\lambda')^m = 0.$$

En développant et ordonnant le premier membre par rapport à x, il devient

$$\begin{aligned} f(x) = a_0 x^m + m a_1 x^{m-1} + \ldots \\ + \frac{m(m-1)\ldots(m-i+1)}{1.2\ldots i} a_i x^{m-i} + \ldots + a_m, \end{aligned}$$

trois termes consécutifs de la suite $a_0, a_1, \ldots, a_m$ étant reliés par une relation linéaire homogène $\alpha_0 a_i + \alpha_1 a_{i+1} + \alpha_2 a_{i+2} = 0$, de sorte que cette suite est formée de m termes consécutifs d'une série récurrente provenant d'une fraction dont le dénominateur est du second degré.

Réciproquement, $f(x)$ étant une fonction satisfaisant aux conditions précédentes, on a identiquement

$$(\lambda' - \lambda) f(x) = (a_0\lambda' - a_1)(x+\lambda)^m - (a_0\lambda - a_1)(x+\lambda')^m,$$

λ et λ' représentant les deux racines de l'équation

$$\alpha_0 + \alpha_1 a_1 \lambda + \alpha_2 \lambda^2 = 0,$$

supposées distinctes. Si les deux racines de cette équation sont égales, on a, λ désignant cette racine double,

$$f(x) = (x+\lambda)^{m-1}[a_0(x+\lambda) - m(a_0\lambda - a_1)].$$

L'équation $f(x) = 0$ a alors $m-1$ racines égales à $-\lambda$ et une racine simple, pourvu que λ ne soit pas égal à $\frac{a_1}{a_0}$. Dans le premier cas, les racines de l'équation $f(x) = 0$ sont égales à $\frac{\lambda' y - \lambda}{1-y}$, y prenant les m valeurs racines de l'équation

$$(a_0\lambda' - a_1)y^m - (a_0\lambda - a_1) = 0.$$

Les m racines de l'équation $f(x) = 0$ sont distinctes.

Supposons les coefficients de $f(x)$ réels. Si les racines de l'équation en λ sont imaginaires, la quantité $\frac{a_0\lambda - a_1}{a_0\lambda' - a_1}$ est imaginaire et a un module égal à 1; les m racines de $f(x) = 0$ sont réelles, car, si on change $\sqrt{-1}$ en $-\sqrt{-1}$ dans $\frac{\lambda' y - \lambda}{1-y}$, on a

$$\frac{\lambda\frac{1}{y} - \lambda'}{1 - \frac{1}{y}} = \frac{\lambda' y - \lambda}{1-y}.$$

Si les racines de l'équation en λ sont réelles, les seules racines réelles de l'équation $f(x) = 0$ sont celles qui correspondent aux racines réelles de l'équation en y.

Les équations que nous venons d'étudier comprennent comme cas particulier l'équation générale du troisième degré.

2. Supposons que les coefficients a dans le polynôme $f(x)$ défini plus haut soient entiers; la congruence $f(x) \equiv 0 \pmod{p}$, p étant premier, se ramène à la congruence binôme

$$(x+\lambda)^m - u(x+\lambda')^m \equiv 0 \pmod{p},$$

si les racines de la congruence

$$\alpha_0 + \alpha_1\lambda + \alpha_2\lambda^2 \equiv 0$$

sont distinctes; $u = \dfrac{a_0\lambda - a_1}{a_0\lambda' - a_1}$ est racine de la congruence

$$u^2 - \frac{(a_0\lambda - a_1)^2 + (a_0\lambda' - a_1)^2}{(a_0\lambda - a_1)(a_0\lambda' - a_1)} u + 1 \equiv 0 \pmod{p}.$$

Les racines de la congruence en u sont imaginaires en même temps que celles de la congruence en λ ou égales à -1, et l'on a

$$u^{p+1} \equiv 1;$$

si les racines de la congruence en λ sont réelles, u est aussi réel.

Cherchons dans quels cas $f(x)$ est irréductible (mod. p). Soit k le plus petit nombre tel que $u^k \equiv 1$ (mod. p.) : 1° u est réel. La fonction binôme $y^m - u$ est irréductible (mod. p), si m ne contient que les facteurs premiers de k et est premier avec $\dfrac{p-1}{k}$, dans le cas où p est de la forme $4q+1$; si p est de la forme $4q-1$, m doit en outre être impair ou double d'un impair (Serret, *Algèbre supérieure,* n° 358). D'ailleurs la fonction $f(x)$ est irréductible ou se décompose de la même manière que $y^m - u$. 2° u est imaginaire. Alors k divise $p+1$. Par un raisonnement analogue à celui de M. Serret dans le cas où u est un nombre réel, on voit que, pour que $y^m - u$ soit irréductible suivant le module p et la fonction modulaire $\alpha_0 + \alpha_1\lambda + \alpha_2\lambda^2$, il faut et il suffit que m ne contienne que les facteurs premiers de k autres que 2 et soit premier avec $\dfrac{p+1}{k}$. La fonction $f(x)$ est *a fortiori* irréductible (mod. p) si m satisfait à ces conditions. Réciproquement, soient k un diviseur de $p+1$, u une racine primitive de la congruence $u^k - 1 \equiv 0$ (mod. p); la fonction

$$\frac{(x + au + b)^m - u(x + au^{-1} + b)^m}{1 - u}$$

est irréductible suivant le module p si m ne contient que les facteurs premiers de k autres que 2 et est premier avec $\dfrac{p+1}{k}$; d'ailleurs elle a ses coefficients réels, car, si l'on change u en $\dfrac{1}{u}$, elle ne change pas, de sorte qu'ils sont des fonctions symétriques des racines de la congruence du second degré dont dépend u ; a et b sont supposés entiers, et a non congru à o (mod. p). On a ainsi une méthode pour former suivant le module p des fonctions irréductibles dont le degré ne contient que les facteurs premiers de $p+1$ autres que 2. J'en ai donné une autre dans un Mémoire présenté à l'Académie des Sciences (*Comptes rendus* du 7 juin).

Exemple. — Prenons pour u une racine de la congruence

$$u^2+u+1\equiv 0 \quad (\text{mod. } p).$$

Alors $k=3$. L'un des nombres $p-1$, $p+1$ est divisible par 3, et de ce qui précède on déduit que la fonction

$$\frac{(x+au+b)^{3^n}-u(x+au^{-1}+b)^{3^n}}{1-u}$$

est irréductible (mod. p), pourvu que $\frac{p^2-1}{3}$ ne soit pas divisible par 3. Si l'on fait $a=b=-1$ et $n=1$, la fonction précédente devient x^3-3x+1, et l'on a une proposition qui a fait l'objet de Communications à l'Académie des Sciences de MM. Sylvester, Pépin et Lucas (*Comptes rendus,* février à juin 1880).