BULLETIN DE LA S. M. F.

A. E. PELLET

Sur la réduction des fonctions entières algébriques

Bulletin de la S. M. F., tome 19 (1891), p. 48-52

<http://www.numdam.org/item?id=BSMF_1891__19__48_1>

Sur la réduction des fonctions entières algébriques;

par M. A.-E. PELLET.

1. Soit $f(x) = 0$ une équation algébrique à coefficients entiers. Si elle est irréductible suivant un module premier p, elle est irréductible *a fortiori* algébriquement; si, suivant le module premier p, elle se décompose en deux facteurs irréductibles de degrés μ et ν par exemple, elle est irréductible algébriquement ou se décompose en deux facteurs de degrés μ et ν, irréductibles. Ces propositions permettent souvent de reconnaître si une équation est irréductible, et, dans le cas contraire, donnent des indications précieuses sur la manière dont elle peut se décomposer.

Supposons que $f(x) = 0$ soit irréductible et que toutes ses racines puissent s'exprimer rationnellement en fonction de l'une d'elles; m étant le degré de $f(x)$ et x une racine de $f(x) = 0$, les autres seront $\theta_1(x)$, $\theta_2(x)$, $\ldots$, $\theta_{m-1}(x)$, ces fonctions θ étant entières en x et ayant pour coefficients des nombres commensurables, entiers ou fractionnaires. Si toutes ces fonctions θ sont distinctes suivant un module premier p, $f(x)$ se décompose suivant ce module en facteurs irréductibles d'égal degré. Mais il n'en est plus ainsi si quelques-unes des fonctions θ deviennent égales entre

elles (mod p), ou si p divise le dénominateur de quelques-uns des coefficients entrant dans les fonctions θ.

Soit, dans tous les cas,

$$f(x) \equiv f_1^{n_1}(x) f_2^{n_2}(x) \dots f_k^{n_k}(x) \pmod{p},$$

$f_1(x), f_2(x), \dots, f_k(x)$ étant des fonctions irréductibles mod p et entrant respectivement $n_1, n_2, \dots, n_k$ fois comme facteurs dans $f(x)$, suivant le mod p; le degré de $f(x)$ est un multiple des degrés de $f_1(x), f_2(x), \dots, f_k(x)$. En effet, les racines de la congruence $f_1(x) \equiv 0 \pmod{p}$ peuvent être représentées par $x, \psi(x), \psi^2(x), \dots, \psi^{\mu-1}(x)$, μ étant le degré de $f_1(x)$, $\psi(x)$ une fonction entière, $\psi^2(x)$ représentant $\psi[\psi(x)]$, et en général

$$\psi[\psi^j(x)] = \psi^{j+1}(x).$$

La fonction $\psi(x)$ est congrue suivant le module p, et la fonction modulaire $f_1(x)$ à l'une des fonctions θ, soit θ_1. Le plus petit nombre ν, tel que $\theta_1^\nu(x) - x$ soit divisible par $f(x)$ algébriquement, est un diviseur de m, degré de l'équation $f(x)$, et aussi un multiple de μ; donc μ est un diviseur de m.

Revenant au cas où $f(x) = 0$ est une équation quelconque à coefficients entiers, soit $F(\rho) = 0$ son équation résolvante. Les racines de $f(x) = 0$ s'expriment rationnellement en fonction d'une quelconque des racines de l'équation $F(\rho) = 0$. Suivant un module quelconque premier p, $F(\rho)$ se décompose en facteurs irréductibles dont les degrés divisent le degré de $F(\rho)$. La fonction résolvante ρ étant convenablement choisie, chacune des racines de la congruence $f(x) \equiv 0 \pmod{p}$ peut s'exprimer en fonction entière des racines de la congruence $F(\rho) \equiv 0 \pmod{p}$; les degrés des facteurs de $f(x)$ sont donc diviseurs du plus petit commun multiple des degrés des facteurs de $F(\rho)$, suivant le module p. Ainsi :

Le degré de l'équation résolvante d'une équation à coefficients entiers est un multiple des degrés des divers facteurs irréductibles en lesquels se décompose le premier membre de l'équation suivant un module premier quelconque.

Par exemple, $x^4 - x + 1$ est irréductible suivant le module 2; elle admet, suivant le module 3, un facteur du premier degré

$x+1$, et un autre du troisième degré x^3-x^2+x+1; la résolvante de l'équation du quatrième degré $x^4-x+1=0$, ou de l'équation plus générale $A(x^4-x+1)+6f(x)=0$, A étant un nombre premier avec 6, et $f(x)$ un polynôme du quatrième degré à coefficients entiers, est donc d'un degré égal à 12 ou 24, et la résolution de cette équation exige l'extraction d'une racine cubique.

D'après un théorème de Galois, le degré de l'équation résolvante d'une équation de degré premier, irréductible, mais soluble par radicaux, est diviseur du produit $p(p-1)$, p étant le degré de l'équation. Il en résulte qu'une équation de degré premier p, à coefficients entiers, et irréductible, n'est pas soluble par radicaux si son premier membre se décompose, suivant certains modules premiers, en facteurs dont le degré ne divise pas $p-1$. Ainsi, x^5-x+1 est irréductible, module 5; suivant le module 2, cette fonction se décompose en un produit de deux facteurs irréductibles, de degrés 2 et 3,

$$x^5-x+1\equiv(x^2+x+1)(x^3+x^2+1) \qquad (\mathrm{mod}\,2);$$

3 ne divisant pas 4, nombre auquel se réduit ici $p-1$, l'équation $x^5-x+1=0$, ou l'équation plus générale

$$A(x^5-x+1)+10f(x),$$

A étant un entier premier avec 10, $f(x)$ un polynôme entier du cinquième degré à coefficients entiers, n'est pas soluble par radicaux.

2. Le théorème suivant peut être utile dans la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier.

Le produit Δ des carrés des différences des racines d'une équation, irréductible et abélienne, $f(x)=0$, est un carré parfait si le degré de l'équation est impair; dans le cas où le degré de $f(x)$ est pair, $\sqrt{\Delta}$ est une quantité irrationnelle.

Nous appelons *abéliennes,* suivant M. Kronecker, les équations irréductibles dont toutes les racines peuvent s'exprimer par x, $\theta(x)$, $\theta^2(x)$, ..., $\theta^{m-1}(x)$, x étant l'une d'elles, θ une fonction rationnelle, m le degré de l'équation.

Considérons le produit

$$(1) \qquad P_{l=1}^{l=m-1} P_{k=0}^{k=l-1} [\theta^k(x) - \theta^l(x)],$$

x étant l'une des racines de $f(x) = 0$. Il acquiert deux valeurs égales et de signes contraires, si m est pair, lorsqu'on substitue $\theta(x)$ à x; au contraire, si m est impair, il ne change pas par la substitution de $\theta(x)$ à x. Donc, dans le premier cas, l'équation $y^2 - \Delta = 0$, qui admet pour racine le produit (1), est irréductible; dans le second cas, lorsque m est impair, $y^2 - \Delta$ se décompose en un produit de deux facteurs rationnels.

Une congruence irréductible suivant un module premier est analogue à une équation abélienne; son Δ sera résidu quadratique si le degré de la congruence est impair, et non-résidu quadratique si son degré est pair. Plus généralement, soit $f(x) \equiv 0 \pmod{p}$ une congruence n'ayant pas de racines égales, on a

$$\Delta \equiv a^2 \delta_1 \delta_2 \delta_3 \ldots \delta_k \pmod{p},$$

a étant un nombre entier, $\delta_1, \delta_2, \ldots, \delta_k$ les valeurs de Δ correspondant aux divers facteurs irréductibles de $f(x)$. Il en résulte que Δ est non-résidu quadratique $(\mathrm{mod}\, p)$, si $f(x)$ admet un nombre impair de facteurs irréductibles de degré pair; Δ est au contraire résidu quadratique $(\mathrm{mod}\, p)$, si $f(x)$ n'admet pas de facteur irréductible de degré pair ou en admet un nombre pair.

Ainsi, une congruence du quatrième degré, n'ayant pas de racine réelle, $(\mathrm{mod}\, p)$, sera irréductible si son Δ est non-résidu quadratique; et une congruence du cinquième degré, n'ayant pas de racine réelle, sera irréductible si son Δ est résidu quadratique.

Exemple. — Soit la fonction

$$f(x) = x^6 - 12x^5 + 60x^4 + 123x^2 + 4567x - 89012$$

considérée par Fourier et Serret.

On a

$$f(x) \equiv x(x-1)(x^4 + 3x^3 - 3) \pmod{7}.$$

Le Δ de la congruence $x^4 + 3x^3 - 3 \equiv 0 \pmod{7}$, laquelle n'a pas de racine réelle, est congru à -2, à un facteur quadratique près; -2 étant non-résidu quadratique $(\mathrm{mod}\, 7)$, $x^4 + 3x - 3$ est irréductible suivant ce module 7.

$f(x)$, réduit à l'aide de $x^4 - 1 \equiv 0 \pmod{5}$, devient $-x^2 - 2$,

et la congruence $x^2+2\equiv 0 \pmod 5$ n'a pas de racine réelle; $f(x)=0$ n'admet donc pas de racine commensurable, et ne peut algébriquement se ramener qu'à deux équations, l'une du quatrième degré, l'autre du deuxième, si elle n'est pas irréductible. Nous allons voir que $f(x)$ n'admet pas de facteur du deuxième degré $(\mathrm{mod}\,5)$; il en résultera que $f(x)$ est irréductible algébriquement. En effet, $x^2+x+1\equiv 0 \pmod 5$ est irréductible. Soit i une de ses racines; on a

$$f(ai+b)\equiv 2a(a-2b+2)i+3a^2-b^2-ab+2a-2 \pmod 5,$$

en remarquant que $(ai+b)^5\equiv -ai+b-a \pmod 5$; a et b sont des nombres réels. Pour que $f(ai+b)\equiv 0 \pmod 5$, il faut qu'on ait simultanément

$$a-2b+2\equiv 0, \qquad 3a^2-b^2-ab+2a-2\equiv 0 \pmod 5;$$

d'où, par l'élimination de a,

$$b^2-2b-1=0 \pmod 5;$$

or cette congruence n'a pas de racine réelle.

Suivant le module 11, $f(x)$ est congrue à $x(x^5-x^4+5x^3+2)$. La fonction $x^5-x^4+5x^3+2$ n'a pas de racine réelle, et son Δ est résidu quadratique $(\mathrm{mod}\,11)$; elle est donc irréductible suivant ce module. L'équation $f(x)=0$ est donc irréductible, et le degré de son équation résolvante est divisible par 4, 5 et 3, c'est-à-dire par 60.