H. LAURENT

# Reconnaître si un polynôme à plusieurs variables peut être décomposé en facteurs entiers

*Nouvelles annales de mathématiques 3e série*, tome 12 (1893), p. 315-321

<http://www.numdam.org/item?id=NAM_1893_3_12__315_1>

# RECONNAITRE SI UN POLYNOME A PLUSIEURS VARIABLES PEUT ÊTRE DÉCOMPOSÉ EN FACTEURS ENTIERS;

PAR M. H. LAURENT.

Soient $f_1, f_2, \ldots, f_n$ des polynômes entiers en $x_1$, $x_2, \ldots, x_n$ de degré $m$. Soient

$$\begin{array}{cccc} x_{11}, & x_{21}, & \ldots, & x_{n1}, \\ x_{12}, & x_{22}, & \ldots, & x_{n2}, \\ \ldots, & \ldots, & \ldots, & \ldots, \\ x_{1\mu}, & x_{2\mu}, & \ldots, & x_{n\mu} \end{array}$$

les $\mu = m^n$ solutions supposées finies et distinctes des équations

$$(1) \qquad f_1 = 0, \qquad f_2 = 0, \qquad \ldots, \qquad f_n = 0.$$

On peut poser

$$f_i = f_i(x_{1j}, x_{2j}, \ldots) + f'_{i1}(x_1 - x_{1j}) + \ldots + f'_{in}(x_1 - x_{nj}),$$

$f_{i1}, f_{i2}, \ldots$ désignant des polynômes entiers de degré

$m - 1$ et cela d'une infinité de manières; posons alors

$$\xi_i = \begin{vmatrix} f_{11}^i & f_{12}^i & \cdots & f_{1n}^i \\ f_{21}^i & f_{22}^i & \cdots & f_{2n}^i \\ \cdots & \cdot\ \cdot & \cdots & \cdots \\ f_{n1}^i & f_{n2}^i & \cdots & f_{nn}^i \end{vmatrix} : \left[\frac{\partial(f_1, f_2, \ldots, f_n)}{\partial(x_1, x_2, \ldots, x_n)}\right]_{x_1 = x_{1i}}.$$

Les $\mu$ quantités $\xi_1, \xi_2, \ldots, \xi_\mu$ jouiront des propriétés suivantes (nous supposerons toujours que $\xi_i$ se change en $\xi_j$ quand $x_{1i}, x_{2i}, \ldots$ se changent en $x_{1j}, x_{2j}, \ldots$, ce qui est évidemment permis) :

1° Entre les $\xi$ il ne saurait exister de relations homogènes à coefficients constants. En effet, on peut remarquer que $\xi_i$ est nul en même temps que les $f$, excepté pour $x_1 = x_{1i}, x_2 = x_{2i}, \ldots$ et que pour ces valeurs des $x$ il se réduit à l'unité; si l'on pouvait avoir

$$a_1\xi_1 + a_2\xi_2 + \ldots + a_\mu\xi_\mu = 0,$$

en faisant $x_1 = x_1, x_2 = x_2, \ldots$, on aurait

$$a_1 = 0;$$

on verrait de même que

$$a_2 = 0, \qquad \ldots;$$

2° Si l'on a

$$a_1\xi_1 + a_2\xi_2 + \ldots = b_1\xi_1 + b_2\xi_2 + \ldots,$$

$a_1, a_2, \ldots, b_1, b_2, \ldots$ étant des constantes, on en conclura

$$a_1 = b_1, \qquad a_2 = b_2, \qquad \ldots;$$

3° Si l'on désigne par F un polynôme entier en $x$ qui prenne pour $x_{1i}, x_{2i}, \ldots$ la valeur $F_i$ quel que soit $i$, on aura

$$F = F_1\xi_1 + F_2\xi_2 + \ldots + F_\mu\xi_\mu.$$

le signe $\equiv$ désignant une égalité dans laquelle on néglige des multiples de $f_1, f_2, \ldots, f_n$; en effet, les deux membres de la formule précédente sont égaux quand les $f$ sont nuls.

$D_i \xi_i$ est de degré $n(m-1)$ en $x_{1i}, x_{2i}, \ldots$. $D_i$ désignant la valeur de

$$D = \frac{\partial(f_1 \ldots f_n)}{\partial(x_1 \ldots x_n)}$$

pour $x_1 = x_{1i}$, $x_2 = x_{2i}$, ..., les termes de $D_i \xi_i$ qui contiennent $x_1, x_2, \ldots$ ou $x_n$ sont de degré inférieur : donc, d'après un théorème connu de Jacobi, dans la somme $\Sigma \xi_i$ tous les termes contenant les variables $x_1$, $x_2$, ... seront nuls; ainsi $\Sigma \xi_i$ ne dépend pas des $x$; or pour des valeurs des $x$ annulant les $f$, $\Sigma \xi_i$ est égal à un, donc;

4° On a la relation

$$\xi_1 + \xi_2 + \ldots + \xi_\mu = 1; \tag{2}$$

5° De (2) on tire

$$\left\{\begin{array}{l} \xi_1^2 + \xi_1 \xi_2 + \ldots + \xi_1 \xi_\mu = \xi_1, \\ \xi_1 \xi_2 + \xi_2^2 + \ldots + \xi_2 \xi_\mu = \xi_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \end{array}\right. \tag{3}$$

6° $\xi_i \xi_j$ est nul en même temps que les $f$, $\xi_i^2$ aussi, excepté pour $x_1 = x_{i1}$, $x_2 = x_{2i}$, ... et alors il est égal à un; on a donc

$$\xi_i \xi_j \equiv 0, \qquad \xi_i^2 \equiv \xi_i.$$

Cela posé, considérons un polynôme F de degré $m-1$ au plus; on peut poser

$$F = F(x_{1i}, x_{2i}, \ldots)(x_1 - x_{1i}) F_1^i + \ldots + (x_n - x_{ni}) F_n^i,$$

$F_1^i$, $F_2^i$, ... désignant des polynômes de degré inférieur à $m-1$ et l'on aura, en posant

$$F_i = F(x_{1i}, x_{2i}, \ldots),$$

$$\begin{vmatrix} F - F_1 & F_1^i & F_2^i & \ldots & F_n^i \\ f_1 & f_{11}^i & \ldots & \ldots & f_{1n}^i \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ f_n & f_{n1}^i & \ldots & \ldots & f_{nn}^i \end{vmatrix} = 0,$$

ce que l'on peut écrire

$$(F - F_i)\xi_i D_i = \lambda_1 f_1 + \lambda_2 f_2 + \ldots + \lambda_n f_n,$$

$\lambda_1, \lambda_2, \ldots$ désignant des polynômes de degré inférieur à $n(m-1)$; on en tire

$$(F - F_i)\xi_i = \frac{\lambda_1}{D_i} f_1 + \ldots + \lambda_n \frac{f_n}{D_i}.$$

Si dans cette formule on fait $i = 1, 2, \ldots$ et si l'on ajoute les résultats obtenus, on aura, en vertu du théorème de Jacobi déjà invoqué,

$$\Sigma(F - F_i)\xi_i = 0$$

et, en vertu de (2),

$$F = F_1\xi_1 + F_2\xi_2 + \ldots + F_\mu \xi \quad . \tag{4}$$

Le signe $=$ devrait être remplacé par $\equiv$ si le degré de F surpassait $m-1$.

Supposons que le polynôme F de $m-1$ soit le produit de deux facteurs $\varphi$, $\psi$ des degrés $n$, $p$, $n + p < m$, on aura

$$\varphi = \varphi_1\xi_1 + \varphi_2\xi_2 + \ldots + \varphi_\mu\xi_\mu,$$
$$\psi = \psi_1\xi_1 + \psi_2\xi_2 + \ldots + \psi_\mu\xi_\mu,$$

$\varphi_i$, $\psi_i$ désignant $\varphi(x_{1i}, x_{2i}, \ldots)$ et $\psi(x_{1i}, x_{2i}, \ldots)$ et par suite

$$\varphi\psi = F = \Sigma\varphi_i\psi_i\xi_i^2 + \Sigma\varphi_i\psi_j\xi_i\xi_j:$$

remplaçons dans cette formule $\xi_i^2$ par sa valeur tirée de (3), nous aurons

$$\varphi\psi = F = \Sigma\varphi_i\psi_i\xi + \Sigma\xi_i\xi_j(\varphi_i\psi_j + \psi_i\varphi_j - \varphi_i\psi_i - \psi_i\psi_j),$$

et, en vertu de (4),

$$\Sigma\xi_i\xi_j(\varphi_i\psi_j + \psi_i\varphi_j - \varphi_i\psi_j - \varphi_j\psi_j) = 0;$$

c'est une relation entre les $\xi_i$, $\xi_j$ : il existera ainsi entre ces quantités une infinité de relations, mais il est clair qu'elles ne seront pas toutes distinctes.

Dans la pratique, il conviendra de prendre

$$\begin{aligned} f_1 &= (x_1 - a_1)(x_1 - a_2)\ldots(x_1 - a_m), \\ f_2 &= (x_2 - b_1)(x_2 - b_2)\ldots(x_2 - b_m), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \end{aligned}$$

alors les $\xi_i$ seront de la forme

$$\frac{f_1 f_2 \ldots f_n}{f_1'(a_i) f_2'(b_j)\ldots} = \frac{1}{x_1 - a_1}\,\frac{1}{x_2 - b_j}\cdots.$$

Pour former les relations identiques du second degré entre les $\xi_i$ nous calculerons les $\xi_i$, $\xi_j$ en observant qu'ils sont égaux à des sommes de fractions simples, abstraction faite du facteur $f_1^2 f_2^2 \ldots$ et qu'ils sont par suite exprimables linéairement en fonction de quantités de la forme $f_1 f_2 f_n \ldots \xi$ pourvu qu'ils ne contiennent pas en dénominateur de facteur carré.

Considérons d'abord les produits $\xi_i\xi_j$, dans lesquels les lettres $a$, $b$, $c$, ... n'entrent qu'avec les indices 1, 2; l'un d'eux contiendra en dénominateur

$$\frac{1}{(x_1 - a_1)(x_1 - a_2)(x_2 - b_1)(x_2 - b_2)\ldots};$$

ce produit que l'on peut obtenir en prenant les facteurs $\xi$ de plusienrs manières est le seul que l'on pourra utiliser : il en résulte l'égalité de plusieurs produits de la forme $\xi_i\xi_j$: ces produits sont au nombre de $\frac{2^n}{2} = 2^{n-1}$, et fournissent $2^{n-1}-1$ relations entre les $\xi_i$, $\xi_j$; mais, au lieu de combiner les lettres portant les indices 1, 2, on peut choisir deux indices quelconques : le nombre total des résultats obtenus sera $2^{n-1}-1$ multiplié par le nombre de combinaisons de $mn$ lettres où il y aura deux $a$, deux $b$, etc., c'est-à-dire $\frac{C_{mn}^{2n}}{2^n}$. Ce n'est pas tout : nous avons dit que les produits $\xi_i\xi_j$ s'exprimaient linéairement au moyen des $f_1, f_2, \ldots, f_n$, $\xi_i$ entre les relations qui expriment les $\xi_i\xi_j$; on pourra en général éliminer les $f_1, f_2, \ldots, f_n$, $\xi_i$, ce qui fournira de nouvelles identités entre les $\xi_i\xi_j$.

Quels que soient les polynômes $f$ dont on fera usage, les identités entre les $\xi_i\xi_j$ ne renfermeront pas les $\xi_i^2$, car devant avoir lieu pour $x_1 = x_{11}$, $x_2 = x_{21}$, ... leurs coefficients seront nuls, etc.

Lorsque l'on aura formé les identités entre les $\xi_i\xi_j$, il sera facile de résoudre la question suivante :

*Étant donné un polynôme* F *de degré* $m-1$, *reconnaître s'il est réductible et dans ce cas le décomposer en facteurs entiers.*

Pour cela on ajoutera à l'identité

$$F = \Sigma F_i \xi_i \Sigma \xi_i = \Sigma \xi_i \xi_j (F_i + F_j),$$

toutes les identités qui ont lieu entre les $\xi_i$, $\xi_i$ respectivement multipliées par des facteurs $\lambda_1, \lambda_2, \ldots$. F prendra la forme

$$F = \Sigma a_{ij} \xi_i \xi_j,$$

où les $a_{ij}$ contiennent les $\lambda$ linéairement. S'il existe alors des valeurs non nulles des $\lambda$ pour lesquelles $\Sigma a_{ij}$, $\xi_i\xi_j$ se réduise à une somme de deux carrés, F ne sera pas irréductible, et réciproquement si F est le produit de deux facteurs entiers $\Sigma a_{ij}$, $\xi_i\xi_j$ pour des valeurs convenables des $\lambda$, se réduira à une somme de carrés : il y aura autant de systèmes de valeurs de $\lambda$ satisfaisant à cette condition que de manières de décomposer F en facteurs entiers.

Pour exprimer que F est une somme de deux carrés, il faut écrire qu'une certaine équation bien connue

$$\Sigma \pm (a_{11} - s) \ldots (a_{\mu\mu} - s) = 0$$

a $\mu - 2$ racines nulles, ee qui fait $\mu - 2$ conditions à écrire et, comme F n'est généralement pas un produit, le nombre des $\lambda$ est inférieur à $\mu - 2$ : le nombre des identités entre les $\xi_i \xi_j$ est donc inférieur à $\mu - 2$.