H. LAURENT

Mémoire sur les équivalences algébriques et l'élimination

Nouvelles annales de mathématiques 3e série, tome 5 (1886), p. 456-460

<http://www.numdam.org/item?id=NAM_1886_3_5__456_1>

MÉMOIRE SUR LES ÉQUIVALENCES ALGÉBRIQUES ET L'ÉLIMINATION [1];

PAR M. H. LAURENT.

VI. Nous allons maintenant aborder la théorie des équivalences de la forme

$$(1) \qquad F(X) \equiv 0,$$

dans lesquelles $F(X)$ est une fonction de X, et X un polynôme réduit à déterminer. Soit p le degré de $F(X)$; il est facile de voir que l'équivalence (1) a plus de p solutions ou, si l'on veut, plus de p racines; en effet, la formule (1) peut se mettre sous la forme

$$A(X - a_1)(X - a_2)\ldots(X - a_p) \equiv 0,$$

$a_1, a_2, \ldots$ désignant les racines de l'équation $F(X) = 0$; on peut satisfaire à cette équivalence en prenant

$$X_1 = a_1,\ a_2,\ \ldots,\ a_p,$$

mais on peut y satisfaire encore de bien d'autres manières. Par exemple, soit U un polynôme réduit égal à a_1 pour $x_1 = \alpha_{11}$, $x_2 = \alpha_{21}$, ..., égal à a_2 pour $x_1 = \alpha_{12}$, $x_2 = \alpha_{22}$, ... Cè polynôme U sera déterminé par ces conditions et égal à

$$\sum a_i \frac{\Delta_i}{\Delta} = U.$$

[1] Voir même Tome. p. 432.

Il est clair alors que $X \equiv U$ sera une solution de l'équivalence (1). Il sera, d'ailleurs, facile de former ainsi toutes les solutions de l'équivalence (1). On peut considérablement simplifier la théorie des équivalences algébriques au moyen du théorème suivant :

Théorème. — *Soit* X *une racine convenablement choisie de l'équivalence binôme*

$$X^\mu - 1 \equiv 0. \tag{2}$$

Tout polynôme entier en $x_1, x_2, \ldots, x_n$ *sera équivalent à une expression de la forme*

$$A_0 + A_1 X + A_2 X^2 + \ldots + A_{\mu-1} X^{\mu-1}. \tag{3}$$

Pour que cela ait lieu, il faut évidemment que X contienne $x_1, x_2, \ldots, x_n$. Mettons alors la formule (2) sous la forme

$$(X - j)(X - j^2)\ldots(X - j^\mu) \equiv 0,$$

j désignant l'expression $\cos\frac{2\pi}{\mu} + \sqrt{-1}\sin\frac{2\pi}{\mu}$ ou toute autre racine primitive de $x^\mu - 1 = 0$. Nous pourrons prendre pour X un polynôme réduit prenant les valeurs $j, j^2, \ldots, j^\mu$ quand les x passent successivement par tous les systèmes de solutions des équations $\varphi_1 = 0$, $\varphi_2 = 0, \ldots$; par exemple, on pourra supposer

$$X = \sum j^i \frac{\Delta_i}{\Delta}.$$

La formule (3) pourra alors s'identifier avec un polynôme réduit quelconque augmenté, s'il le faut, de multiples de $\varphi_1, \varphi_2, \ldots, \varphi_n$. $A_0, A_1, \ldots$ seront alors déterminés au moyen d'équations du premier degré, et il faut prouver que, en général, le déterminant de ces équations ne sera pas nul.

Le déterminant en question ne dépend pas du polynôme que l'on veut identifier avec l'expression (3), après l'avoir réduite ; il est clair que l'identification est possible avec certains polynômes, par exemple avec ceux qui sont le développement d'une expression (3) choisie à l'avance; si donc on démontre qu'il n'y a qu'une seule manière de choisir les coefficients A_0, A_1, ..., le déterminant en question ne sera pas nul.

Or supposons que, f désignant un polynôme réduit, on puisse avoir à la fois

$$f \equiv A_0 + A_1 X + \ldots + A_{\mu-1} X^{\mu-1},$$
$$f \equiv B_0 + B_1 X + \ldots + B_{\mu-1} X^{\mu-1};$$

on en conclurait

$$0 \equiv (A_0 - B_0) + X(A_1 - B_1) + \ldots + X^{\mu-1}(A_{\mu-1} - B_{\mu-1});$$

si, dans cette formule, on donne à x_1, x_2, ..., x_n les divers systèmes de valeurs qui annulent les φ ou, ce qui revient au même, si l'on fait successivement $X = j$, $X = j^2$, ..., $X = j^\mu$, on trouve

$$A_0 - B_0 + j\,(A_1 - B_1) + \ldots + j^{\mu-1}\,(A_{\mu-1} - B_{\mu-1}) = 0,$$
$$A_0 - B_0 + j^2(A_1 - B_1) + \ldots + j^{2\mu-2}(A_{\mu-1} - B_{\mu-1}) = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots;$$

d'où l'on tire

$$A_0 = B_0, \qquad A_1 = B_1, \qquad \ldots,$$

car le déterminant

$$\begin{vmatrix} 1 & j & j^2 & \ldots & j^{\mu-1} \\ 1 & j^2 & j^4 & \ldots & j^{2\mu-1} \\ . & .. & .. & \ldots & \ldots.. \end{vmatrix}$$

est égal au produit des différences des quantités j, j^2, j^3, ..., j^μ qui sont toutes distinctes, et, par suite, il n'est pas nul.

Ainsi *tout polynôme, à des multiples des diviseurs* *près, peut se mettre sous la forme*

$$A_0 + A_1 X + A_2 X^2 + \ldots + A_{\mu-1} X^{\mu-1}.$$

Cette forme est précieuse, en effet, en vertu de l'équivalence

$$X^\mu - 1 \equiv 0;$$

on pourra, dans le calcul, traiter la variable X comme si elle avait pour puissances successives $1, X, \ldots, X^{\mu-1}, 1, X, \ldots, X^{\mu-1}, 1, \ldots$, en sorte que, dans bien des cas, l'étude des équivalences algébriques pourra être ramenée à celle des équivalences relatives au diviseur unique $X^\mu - 1$.

Lorsque l'on a ramené un polynôme à la forme

$$A_0 + A_1 X + \ldots + A_{\mu-1} X^{\mu-1},$$

son module prend une forme remarquable : multiplions-le, en effet, par

$$B_0 + B_1 X + \ldots + B_{\mu-1} X^{\mu-1},$$

le résultat est

$$\begin{aligned} & A_0 B_0 + A_{\mu-1} B_1 + \ldots + A_1 B_1 \\ + & (A_1 B_0 + A_0 B_1 + \ldots + A_2 B_{\mu-1}) X \\ + & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + & (A_{\mu-1} B_0 + A_{\mu-2} B_1 + \ldots + A_0 B_{\mu-1}) X^{\mu-1}. \end{aligned}$$

Le déterminant des équations obtenues en égalant les coefficients des diverses puissances de X à zéro, à savoir :

$$(4) \qquad \begin{vmatrix} A_0 & A_{\mu-1} & \ldots & A_1 \\ A_1 & A_0 & \ldots & A_2 \\ \ldots & \ldots & \ldots & \ldots \\ A_{\mu-1} & A_{\mu-2} & \ldots & A_0 \end{vmatrix} = M,$$

est le module cherché, ce qui montre que :

La résultante de plusieurs équations peut se mettre sous la forme d'un déterminant cyclique.

Considérons le déterminant (4) et désignons par j une racine primitive $\mu^{\text{ième}}$ de l'unité. Ce déterminant pourra se mettre sous la forme

$$F(j)\,F(j^2)\ldots F(j^\mu), \tag{5}$$

$F(x)$ désignant, pour abréger, le polynôme

$$A_0 + A_1 x + A_2 x^2 + \ldots + A_{\mu-1} x^{\mu-1}.$$

Pour effectuer le produit (5), on peut opérer comme si j était une quantité quelconque et faire usage des formules de réduction

$$j^\mu = 1, \qquad j^{\mu+1} = j, \qquad \ldots, \qquad j^{2\mu} = 1, \qquad j^{2\mu+1} = j, \qquad \ldots;$$

on peut aussi le former en calculant le produit

$$F(X)\,F(X^2)\ldots F(X^\mu)$$

et en faisant usage de l'équivalence $X^\mu - 1 \equiv 0$, pour éliminer les puissances de X supérieures à $\mu - 1$. On peut donc écrire

$$M \equiv F(X)\,F(X^2)\ldots F(X^\mu).$$

Les polynômes $F(X)$, $F(X^2)$, ..., $F(X^\mu)$ *sont ce que l'on peut appeler des expressions réduites conjuguées; de pareilles expressions ont toutes le même module, leur produit est égal à leur module commun.*