Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 21 (1975)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: INTRODUCTION A LA THÉORIE DES SURFACES DE RIEMANN
Autor: Guenot, J. / Narasimhan, R.
Kapitel: (1) Résultants et discriminants
DOI: https://doi.org/10.5169/seals-47334

Appendice III

(1) *Résultants et discriminants*

Désignons par A un anneau intègre (commutatif avec élément unité) et par K son corps des fractions.

Lemme 1. *Soit M un A-module libre de type fini et soit u un endomorphisme de M. Si u est surjectif, c'est un isomorphisme.*

L'application $u \otimes 1$ est un endomorphisme surjectif de $M \otimes_A K$, donc un isomorphisme puisque $M \otimes_A K$ est un espace vectoriel de dimension finie. On conclut en remarquant que l'application canonique de M dans $M \otimes_A K$ est injective.

Pour tout entier naturel m, on désigne par A_m l'ensemble des polynômes de $A\,[T]$ de degré strictement inférieur à m. C'est un A-module libre de rang m.

Soient p et q deux polynômes de $A\,[T]$ de degré m et n respectivement. On désigne par $\phi\,(p, q)$ l'application A-linéaire de $A_n \times A_m$ dans A_{m+n} définie par

$$\phi\,(p, q)\,(u, v) = up + vq\,.$$

Les polynômes

$$(1, 0), \ldots, (T^{n-1}, 0), (0, 1), \ldots, (0, T^{m-1}) \quad (\text{resp. } 1, \ldots, T^{m+n-1})$$

forment une base de $A_n \times A_m$ (resp. A_{m+n}). On appelle *résultant de p et q* et l'on désigne par Rés (p, q) le déterminant de l'application $\phi\,(p, q)$ exprimé dans ces bases. Si l'on pose

$$p = p_m + p_{m-1}\,T + \ldots + p_0 T^m \qquad \text{et} \qquad q = q_n + q_{n-1}\,T + \ldots + q_0 T^n$$

le résultant de p et q est donné par la formule

$$\text{Rés}(p,q) = \begin{array}{c} \left|\begin{array}{ccccccccc} p_m & 0 & \cdot & \cdot & 0 & q_n & \cdot & 0 & 0 \\ \cdot & p_m & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & q_n & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & q_n \\ p_0 & \cdot & \cdot & \cdot & p_m & \cdot & \cdot & \cdot & \cdot \\ 0 & p_0 & \cdot & \cdot & \cdot & q_0 & \cdot & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & q_0 & \cdot \\ 0 & 0 & \cdot & \cdot & p_0 & 0 & \cdot & 0 & q_0 \end{array}\right| \\ \underbrace{\hphantom{p_m\quad 0\quad \cdot\quad \cdot\quad 0}}_{n}\quad\underbrace{\hphantom{q_n\quad \cdot\quad 0\quad 0}}_{m} \end{array} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} m+1 \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n-1 \\ \vphantom{a} \end{array}$$

Il résulte de cette définition que Rés (p, q) est un polynôme homogène de degré n en $p_0, \ldots, p_m$, homogène de degré m en $q_0, \ldots, q_n$. Son terme de plus haut degré en p_m et q_0 est $p_m^n q_0^m$.

Pour tout homomorphisme ρ de A dans un anneau intègre B, on a

$$\text{Rés}\big(\rho(p), \rho(q)\big) = \rho\big(\text{Rés}(p,q)\big).$$

On dit que p et q sont *étrangers* (ou aussi *premiers entre eux*) s'ils engendrent l'anneau $A[T]$.

LEMME 2. *On suppose que l'un au moins des coefficients* p_0 *ou* q_0 *est inversible. Les conditions suivantes sont équivalentes :*

(1) Les polynômes p *et* q *sont étrangers.*

(2) L'application $\phi(p, q)$ *est un isomorphisme.*

(3) Le résultant de p *et* q *est inversible dans* A.

Il suffit de montrer que les conditions (1) et (2) sont équivalentes.

Supposons par exemple q_0 inversible et (1) vérifiée. En particulier, pour tout polynôme r de A_{m+n}, on a

$$r = up + vq$$

avec u et v dans $A[T]$. La division euclidienne des polynômes montre que l'on a

$$u = u'q + u'' \qquad \text{avec} \qquad \deg(u'') < n.$$

On a alors

$$r = u''p + (u' + v)\, q \qquad \text{avec} \qquad \deg(u' + v) < m.$$

Ceci montre que l'application $\phi(p, q)$ est surjective. Le lemme 1 montre que c'est un isomorphisme.

Réciproquement, supposons (2) vérifiée. On peut écrire

$$1 = up + vq$$

pour certains polynômes u et v de A_n et A_m respectivement. Ceci montre que p et q sont étrangers.

LEMME 3. *Supposons A factoriel. Si les polynômes p et q sont moniques, irréductibles et distincts, ils sont étrangers.*

Raisonnons par l'absurde. Il existe alors des polynômes u et v non nuls de degré strictement inférieur à n et m respectivement tels que

$$up + vq = 0$$

(lemme 2). Le polynôme q étant irréductible, il n'appartient pas à l'idéal (p). Le polynôme v non plus pour des raisons de degré. Puisque $A[T]$ est factoriel et le polynôme p irréductible, l'idéal (p) est premier, ce qui est absurde.

Soit L une clôture algébrique de K. On peut écrire

$$p = p_0 \prod_{1 \leq j \leq m} (T - \alpha_j) \qquad \text{et} \qquad q = q_0 \prod_{1 \leq k \leq n} (T - \beta_k)$$

pour certains éléments $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ de L. La fonction

$$S = p_0^n q_0^m \prod_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m}} (\beta_k - \alpha_j)$$

est symétrique par rapport à $\alpha_1, \ldots, \alpha_m$ (resp. $\beta_1, \ldots, \beta_n$). C'est donc une fonction polynomiale de $p_0, \ldots, p_m$ et $q_0, \ldots, q_n$. Remarquons que l'on a

$$S = (-1)^{mn} p_0^n \prod_{1 \leq j \leq m} q(\alpha_j) = q_0^m \prod_{1 \leq k \leq n} p(\beta_k).$$

En particulier, le polynôme S est homogène de degré n en $p_0, \ldots, p_m$ et homogène de degré m en $q_0, \ldots, q_n$. Son terme de plus haut degré en p_m et q_0 est $p_m^n q_0^m$.

Les coefficients des polynômes p et q sont liés aux racines par les formules

$$p_j = (-1)^j \sigma_j(\alpha_1, \ldots, \alpha_m) \qquad \text{et} \qquad q_j = (-1)^j \sigma_j(\beta_1, \ldots, \beta_n)$$

où σ_j désigne la j^e fonction symétrique élémentaire à m ou n indéterminées. Ceci montre que Rés(p, q) est une fonction polynomiale en $p_0, \alpha_1, \ldots, \alpha_m$, $q_0, \beta_1, \ldots, \beta_n$. Cette fonction polynomiale est divisible par $\beta_k - \alpha_j$. En effet, si α_j est égal à β_k, les polynômes p et q ne sont pas étrangers (lemme 2).

Il résulte de toutes ces remarques que l'on a la formule

$$\boxed{\operatorname{Rés}(p, q) = p_0^n q_0^m \prod_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m}} (\beta_k - \alpha_j)}$$

En particulier, le résultant de p et q s'annule si et seulement si l'une des conditions suivantes est vérifiée:

(1) L'un des coefficients p_0 ou q_0 est nul.

(2) Les polynômes p et q ont une racine commune dans L.

Soit p un polynôme de $A[T]$ et soit p' le polynôme dérivé $\dfrac{\partial p}{\partial T}$. On appelle *discriminant de* p et l'on désigne par $\operatorname{Dis}(p)$ le résultant de p et p'.

Avec les notations précédentes, on a

$$p' = p_0 \sum_{1 \leq j \leq p} (T - \alpha_1) \dots \widehat{(T - \alpha_j)} \dots (T - \alpha_m)$$

et par conséquent,

$$p'(\alpha_k) = p_0 \prod_{\substack{1 \leq j \leq m \\ j \neq k}} (\alpha_k - \alpha_j) \, .$$

La formule précédente montre que l'on a

$$\boxed{\operatorname{Dis}(p) = p_0^{2m-1} \prod_{\substack{1 \leq j,\ k \leq m \\ j \neq k}} (\alpha_j - \alpha_k)}$$

En particulier, le discriminant de p s'annule si et seulement si l'une des conditions suivantes est vérifiée:

(1) Le coefficient dominant de p est nul.

(2) Le polynôme p a une racine double dans L.

LEMME 4. *Supposons* A *factoriel. Si le polynôme* p *est monique irréductible, le discriminant* $\operatorname{Dis}(p)$ *est non nul.*

Raisonnons par l'absurde en supposant que $\operatorname{Dis}(p)$ est nul, donc non inversible dans K. Le lemme 2 montre qu'il existe deux polynômes u et v de degré strictement inférieur à $m-1$ et m respectivement dans $K[T]$ tels que

$$up + vp' = 0 \, .$$

Quitte à multiplier cette égalité par un élément convenable de A, on peut supposer que u et v appartiennent à $A[T]$. On procède alors comme dans le lemme 3.