113

146

Résultant. Applications.

DVI

Motivation : * Résolution de systèmes polynômiaux.

Cadre : A anneau commutatif intègre.

$\forall d \geq 0$, $A_d[X]$ est l'anneau des poly de deg $\leq d$.

I DEFINITIONS, PREMIÈRES PROPRIÉTÉS

Définition 1 : soient $P(X) = a_p X^p + \dots + a_1 X + a_0 \in A[X]\setminus\{0\}$
$Q(X) = b_q X^q + \dots + b_1 X + b_0$, $a_p b_q \neq 0$.

on appelle matrice de Sylvester associée à P, Q, la matrice notée $Sylv(P,Q)$ de l'application linéaire :

$$R_{p,q} : \begin{cases} A_q[X] \times A_p[X] \longrightarrow A_{p+q}[X] \\ (U, V) \longmapsto PU + QV \end{cases}$$

c'est :

$$\begin{pmatrix} a_p & a_{p-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ & a_p & a_{p-1} & \cdots & a_1 & a_0 & 0 \cdots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \cdots & 0 & a_p & & \cdots & & a_0 \\ \hline b_q & \cdots & & & b_0 & 0 & \cdots & 0 \\ & \ddots & & & & \ddots & & \\ & & & b_q & & \cdots & & b_0 \end{pmatrix}$$

dans la base : $(X^{q-1},0), \dots (1,0), (0,X^{p-1}), \dots (0,1)$.
Son déterminant est appelé résultant $R(P,Q)$ de P et Q.

Proposition 1 : $Rg(R) = d^0 P + d^0 Q - d^0(P \wedge Q)$. A corps

Corollaire 1 : R surjective $\Leftrightarrow R(P,Q) \neq 0 \Leftrightarrow P$ et Q sont 1ers entre eux

Application : $n \in \mathbb{N}^*$, D_n l'ensemble des matrices diagonalisables de $M_n(\mathbb{C})$. Alors : $\mathring{D_n}$ est l'ensemble des matrices diag à valeurs propres distinctes.

Corollaire 2 : si $A = K$ un corps algébriquement clos, P et Q ont une racine commune $\Leftrightarrow R(P,Q) = 0$.

Proposition 2 $P, Q \in A[X]$, $\alpha \in A$.

* $R(\alpha, Q) = \alpha^q$ * $R(Q,Q) = 0$ si Q non constant
* $R(\alpha P, Q) = \alpha^q R(P,Q)$
* $R(P,Q) = (-1)^{pq} R(Q,P)$
* $\forall k \geq 0$ $R(X^k P, Q) = b_0^k R(P,Q)$.

Corollaire 3. P n'a que des racines simples si et seulement si $R(P,P') \neq 0$.
si $A = K$, alg clos :

Exemple 1. $X^2 + pq - (p+q)X = P$ $\forall p,q \in \mathbb{R}$ a deux racines distinctes ssi $R(P,P') = -(p-q)^2 \neq 0$
ssi $p \neq q$

II CALCULS

1. Méthode d'Abaissement.

L'algorithme est basé sur la proposition suivante

Proposition 3 Avec les mêmes notations (avec $p \geq q$),
et si R est le reste de la division Euclidienne de P par Q
où b_q est supposé inversible dans A.

Alors $R(P,Q) = (-1)^{pq} b_q^{p-r} R(Q,R)$
$d^0 R = r$.

__Remarque :__ + cette propriété permet facilement de construire un algorithme de calcul du résultant.

Si on note $R_0 = P$, $R_1 = Q$, ..., $R_i = R(R_{i-2}, R_{i-1})$, ... R_k la suite des restes obtenue.

$R_k = c \neq 0 \Rightarrow R(R_{k-1}, R_k) = c^{d^\circ R_{k-1}}$

sinon. $R_k = 0$, $R_{k-1} \mid R_{k-2}$ et $\mathrm{Res}(R_{k-1}, R_{k-2}) = 0$.

+ la proposition 3 fournit une autre façon de prouver que $P \wedge Q = 1 \Leftrightarrow R(P,Q) \neq 0$.

__Exemple 2.__ $P = X^2 + 2X - XY + 2Y - 6$.
$Q = 3X^2 - 5X + 5 + XY - 2Y$ $\in (\mathbb{Q}[Y])[X]$

La suite des restes :

$$\begin{cases} R_1 = \left(\frac{11}{3} - \frac{4}{3}Y\right)X - \frac{23}{3} + \frac{8}{3}Y \\ R_2 = 3\,\dfrac{309 - 211Y + 36Y^2}{(4Y-11)^2} \\ R_3 = 0 \end{cases}$$

$$R_X(P,Q) = 309 - 211Y + 36Y^2 = (36Y - 103)(Y-3)$$

2. Expression en fonction des racines.

Soit K un corps contenant A dans lequel P et Q se décomposent :

$P(X) = a_p (X - \alpha_1) \dots (X - \alpha_p)$. $\alpha_i \in K$ $\forall i$.
$Q(X) = b_q (X - \beta_1) \dots (X - \beta_q)$. $\beta_i \in K$.

__Proposition 4.__ $R(P,Q) = (-1)^{pq} b_q^p \prod_{j=1}^{q} P(\beta_j)$

$$= a_p^q \prod_{j=1}^{p} Q(\alpha_j) = b_q^p a_p^q \prod_{\substack{1 \le i \le p \\ 1 \le j \le q}} (\alpha_i - \beta_j)$$

__Corollaire 4.__ Soient $P, Q_1, Q_2 \in K[X]$, K corps décomposant P, Q_1, Q_2. Alors :

$$R(P, Q_1 Q_2) = R(P, Q_1) R(P, Q_2).$$

III APPLICATIONS.

1. Résolution de systèmes polynomiaux.

__Exemple :__ $P, Q \in K[X,Y]$. K algébriquement clos on souhaite résoudre $\begin{cases} P(X,Y) = 0 \\ Q(X,Y) = 0 \end{cases}$

__Méthode :__ si (α, β) est solution, $P(X, \beta)$, $Q(X, \beta)$ ont une racine commune α. Donc $\mathrm{Res}_X(P(X,\beta), Q(X,\beta)) = 0$.

Ainsi β est racine de $\mathrm{Res}_X(P(X,Y), Q(X,Y)) = 0$. (en Y).

On en déduit ensuite les solutions.

__Application :__ $\begin{cases} X^2 + 2X - XY + 2Y - 6 = 0 \\ 3X^2 - 5X + 5 + XY - 2Y = 0 \end{cases}$ a pour solutions $(1,3)$ et $\left(-\frac{1}{4}, \frac{103}{36}\right)$, 3 et $\frac{103}{36}$ sont bien les racines trouvées en ex. 2. Néanmoins la résolution de telles équations (en terme de résultants) donne aussi des solutions parasitaires.

__Proposition 5 :__ K corps algébriquement clos, $P, Q \in K[Y_1, \dots Y_k][X]$

$P = \sum_{i=1}^{n} a_i X^i$, $Q = \sum_{i=1}^{n} b_i X^i$, $a_i, b_i \in K[Y_1, \dots Y_k]$ $\forall i$.

- Si $(\alpha_1, \dots \alpha_k, \alpha) \in K^{k+1}$ vérifie $P(\alpha_1, \dots \alpha_k, \alpha) = Q(\alpha_1, \dots \alpha_k, \alpha) = 0$ alors $\mathrm{Res}_X(P(\alpha_1, \dots \alpha_k, X), Q(\alpha_1, \dots \alpha_k, X)) = 0$ et condition que $P(\alpha_1, \dots \alpha_k, X), Q(\alpha_1, \dots \alpha_k, X) \neq 0$. (*)
- __Inversement :__ si $(\alpha_1, \dots \alpha_k)$ vérifie (*). L'une des quatre éventualités peut se produire :

(i) $\exists \alpha \in K / (\alpha_1, \ldots \alpha_k, \alpha)$ soit effectivement solution du système polynomial.

(ii) $P(\alpha_1, \ldots \alpha_k, X) = 0$ } inutile

(iii) $Q(\alpha_1, \ldots \alpha_k, X) = 0$

(iv) $a_m(\alpha_1, \ldots \alpha_k) = b_n(\alpha_1, \ldots \alpha_k) = 0$.

<u>Exemple</u>: $\begin{cases} XY = 0 \\ XY - 1 = 0 \end{cases}$ n'a trivialement pas de solution. et pourtant $Res_X(XY, XY-1) = -Y = 0$ a une solution en Y.

On est dans le cas pathogène (ii).

2. Résultants et Nombres algébriques

<u>Proposition 6</u>. l'ensemble des complexes algébriques sur $\mathbb{Q}$ forme un sous anneau de $\mathbb{C}$.

<u>Exemple</u>: le résultant, si α et β sont algébriques sur $\mathbb{Q}$ permet de construire un polynome annulateur du produit et de la somme.

Par exemple si $\alpha = \frac{\sqrt{5}-1}{2}$, $\beta = \sqrt{3}$, ils sont annulés par $X^2+X-1 = P(X)$ et $X^2-3 = Q(X)$. Alors $\alpha+\beta$ est racine de $S(Y) = R_X(P(X), Q(Y-X))$ étant donné que $P(X)$ et $Q(\alpha+\beta-X)$ ont α comme racine commune.

On obtient de même que $\alpha\beta$ est racine de

$$R_X\left(P(X), X^2 B\left(\frac{Y}{X}\right)\right).$$

3. Transformation des équations algébriques

<u>Principe</u>. soit K un corps algébriquement clos et deux polynomes: $P(X) = a_p X^p + \ldots + a_0 \in K[X]$, $Q(X,Y) = b_q(Y) X^q + \ldots + b_0(Y) \in (K[Y])[X]$.

on veut étudier $P(X) = 0$ en remplaçant X par une expression (implicite) en Y définie par $Q(X,Y) = 0$. Cela revient à chercher Y tel que : $P(X) = 0$ et $Q(X,Y) = 0$ aient une solution commune.

<u>Proposition 7</u>. $R_X(P(X), Q(X,Y)) \in K[Y]$ et pour toute racine $y \in K$ de ce polynôme, $P(X) = 0$ et $Q(X,y) = 0$ ont une racine commune.

<u>Exemple</u>. $P(X) = X^4 + X^3 + \ldots + 1$, $Q(X,Y) = X^2 - XY + 1$, on étudie $P(X) = 0$ en posant $X^2 - XY + 1 = 0 \Leftrightarrow Y = X + \frac{1}{X}$. Cela revient ensuite à résoudre : $(Y^2 + Y - 1)^2 = 0$ (via le résultant).

<u>Remarque</u>: la proposition n'est utile que si le polynôme en Y obtenu est plus simple que celui de départ.

<u>Théorème 1</u> (Kronecker). soit $P \in \mathbb{Z}[X]$ unitaire de degré n, tel que : * les racines de P dans $\mathbb{C}$ sont de module inférieur ou égal à 1.
* $P(0) \neq 0$.

Alors : les racines de P sont racines de l'unité.

4. Lien avec le discriminant.

<u>Prop / Déf 8</u>. K corps et $P \in K[X]$ unitaire tel que : $(a_p \neq 0)$. $P = a_p(X - \alpha_1) \ldots (X - \alpha_p)$. Alors on définit le discriminant de P par $\Delta(P) = \prod_{1 \le i < j \le p} (\alpha_i - \alpha_j)^2 \times a_p^{2p-2}$.

et $\Delta(P) = \frac{(-1)^{\frac{p(p-1)}{2}}}{a_p} \prod_{i=1}^{n} P'(\alpha_i) = \frac{(-1)^{\frac{p(p-1)}{2}}}{a_p} R(P, P')$

<u>Corollaire 5</u> P a une racine multiple $\Leftrightarrow \Delta(P) = 0$.

<u>Exemples</u>. * $P(X) = aX^2 + bX + c$, $a \neq 0$, $a, b, c \in K$ défini précédemment.
$\Delta(P) = \frac{-1}{a} \cdot R_X(aX^2 + bX + c, 2aX + b) = \frac{-1}{a} a(-b^2 + 4ac) = b^2 - 4ac$

* $P(X) = X^3 + pX + q$, $\Delta(P) = -4p^3 - 27q^2$. (on peut toujours se ramener à cette forme par changement de variable)

DVT

Références :

* Saux-Picard - "Cours de calcul formel, Algorithmes Fondamentaux".
* Gourdon - "Algèbre"
* Szpirglas "Toute l'Algèbre de la licence".
* Gobelot "Algèbre commutative".