143 Résultant. Applications.

Problématique: Résoudre un système d'équations algébriques

$$P(X)=a_pX^p+\dots+a_0=0 \quad (a_p\neq 0)$$
$$Q(X)=b_qX^q+\dots+b_0=0 \quad (b_q\neq 0)$$

par la méthode d'élimination des variables

I) Introduction au résultant

On désigne par A un anneau factoriel

Soit $P,Q\in A[X]$ non nuls: $P(X)=a_pX^p+\dots+a_0$ $(a_p\neq 0)$

$Q(X)=b_qX^q+\dots+b_0$ $(b_q\neq 0)$

Définition La matrice de Sylvester de P et Q est

$$Syl(P,Q)=\begin{pmatrix} \overbrace{\begin{matrix} a_p & & \\ \vdots & \ddots & \\ a_0 & & a_p \\ & \ddots & \vdots \\ & & a_0 \end{matrix}}^{q} & \overbrace{\begin{matrix} b_q & & \\ \vdots & \ddots & \\ b_0 & & b_q \\ & \ddots & \vdots \\ & & b_0 \end{matrix}}^{p} \end{pmatrix}\in M_{p+q}(A)$$

c'est la matrice de $\Phi: A_{q-1}[X]\times A_{p-1}[X]\to A_{p+q-1}[X]$

$$U,V \mapsto UP+VQ$$

dans les bases $((X^{q-1},0),\dots,(1,0),(0,X^{p-1}),\dots,(0,1))$ et $(X^{p+q-1},\dots,1)$

Définition Le résultant de P et Q est $Res(P,Q)=\det Syl(P,Q)$

exemple
- $Res(X^2+1,3X)=9$
- $Res(X^p,Q(X))=Q(0)^p$

Proposition $Res(P,Q)\neq 0$ ssi P et Q sont premiers entre eux

Corollaire $Res(P,Q)=0$ ssi P et Q ont une racine commu dans $\overline{Frac(A)}$

Proposition Il existe $U\in A_{q-1}[X]$ et $V\in A_{p-1}[X]$ tels que $UP+VQ=Res(P,Q)$

II) Méthodes de calculs

Proposition $Res(P,Q)=a_p^q\det\Psi_Q$

où $\Psi_Q: A[X]/(P)\to A[X]/(P)$

$$\bar{T}\mapsto \bar{T}\bar{Q}$$

Propriétés

i) $Res(P,Q)=(-1)^{pq}Res(Q,P)$

ii) $Res(\lambda P,Q)=\lambda^q Res(P,Q)$ $(\lambda\in A\setminus\{0\})$

iii) $Res(P,\mu Q)=\mu^p Res(P,Q)$ $(\mu\in A\setminus\{0\})$

iv) $Res(P(X-a),Q(X-a))=Res(P,Q)$ $(a\in A)$

Lien résultant-racines

$$R\left(\prod_{i=1}^{p}(X-a_i)\,P,Q\right)=R(P,Q)\prod_{i=1}^{p}(X-a_i)$$

Application: théorème de Kronecker

Soit $P\in\mathbb{Z}[X]$ unitaire dont les racines complexes sont non nulles et de module ≤ 1. Alors les racines de P sont des racines de l'unité

Algorithme d'Euclide

Soit R le reste de la division euclidienne de Q par P. Si $R=0$, $Res(P,Q)=0$

Si $R\neq 0$, $Res(P,Q)=a_p^{q-r}Res(P,R)$

où $r=\deg R$

Théorie de l'élimination

...artir d'ici K est un corps algébriquement clos

...héorème d'extension

...orème Soit $P, Q \in K[X_1 .. X_n]$ non nuls.

...écrit $P = \sum_{k \leq p} a_k X^k$, $a_k \in K[X_1 .. X_{n-1}]$, $a_p \neq 0$

$$Q = \sum_{k \leq q} b_k X^k, \quad b_k \in K[X_1 .. X_{n-1}], \quad b_q \neq 0$$

...i $(\alpha_1, .., \alpha_n)$ est une racine commune à P ...& alors $Res_{X_n}(P, Q)|_{\alpha_1, .., \alpha_{n-1}} = 0$

...Soit $\beta \in A^{n-1}$ tel que $a_p(\beta) \neq 0$ où $b_q(\beta) \neq 0$ ...s $Res_{X_n}(P, Q)|_{\beta} = 0$ ssi $P(\beta, X_n)$ et $Q(\beta, X_n)$ ont une racine commune

...cipe (le cas de deux variables)

...) Calculer $R(X) = Res_Y(P, Q)$

...) Chercher les racines de $R(X)$

...) Pour chaque racine α de R, déterminer les ...ines éventuelles de $P(\alpha, Y)$ et $Q(\alpha, Y)$

... peut aussi calculer $S(Y) = Res_X(P, Q)$ et ...oler les racines de R et S.

...emple $P(X, Y) = X^2 - 2XY + Y^2$

$$Q(X, Y) = X^2 + Y^2 - 1$$

$$Res_X(P, Q) = (2Y^2 - 1)^2$$

...où l'ensemble des solutions $\{\pm(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})\}$

2) Transformation des équations algébriques

Principe Etudier $P(X) = 0$ en remplaçant X par une équation impli...te en Y ($Q(X, Y) = 0$)

Proposition Soit $P \in K[X]$ et $Q \in K[X, Y]$ non nuls. Quelquesoit $y \in K$, on a

$$Res_X(P, Q)|_y = 0 \text{ ssi } P(X) \text{ et } Q(X, y) \text{ ont une racine commune}$$

exemple

On cherche à résoudre $P(X) = X^4 + X^3 + X^2 + X + 1$ en posant $Y = \frac{1}{X} + X$ càd $Q(X, Y) = X^2 - XY + 1$

$$Res_X(P, Q) = (Y^2 + Y - 1)^2$$

3) Théorème de Bézout

Définition La courbe algébrique plane affine définie par un polynôme $A(X, Y)$ non constant de $K[X, Y]$ est le sous-ensemble

$$V(A) = \{(x, y) \in K^2 \mid A(x, y) = 0\}$$

On dit que $V(A)$ est irréductible si A l'est

Théorème (Bézout, 1779) Soit C_0, C_1 deux courbes algébriques irréductibles planes affines distinctes. et de degrés respectifs n_0, n_1. Alors $C_0 \cap C_1$ a au plus $n_0 \times n_1$ points d'intersection

DVT

Application • Deux coniques distinctes du plan ont au plus quatre points d'intersection

• Par cinq points du plan, passe au plus une conique

4) Nombres algébriques

Définition Un nombre complexe est dit algébrique s'il est racine d'un polynôme à coefficients rationnels non nul

Lemme Soit α, β deux nombres algébriques
Soit $P, Q \in \mathbb{Q}[X]$ non nuls tels que $P(\alpha) = Q(\beta) = 0$

i) $\alpha + \beta$ est racine de $\mathrm{Res}_X(P(X), Q(Y-X))$

ii) Si $\alpha \neq 0$, $1/\alpha$ est racine de $P^*(X) = \mathrm{Res}_X(P(X), XY-1)$

iii) Si $\alpha \neq 0$, $\alpha\beta$ est racine de $\mathrm{Res}_X(P^*(X), Q(XY))$

exemple polynôme minimal de $\sqrt{2}+\sqrt{3}$

$\mathrm{Res}_X(X^2-2, (Y-X)^2-3) = Y^4 - 10Y^2 + 1$

Proposition L'ensemble des nombres algébriques est un sous-corps de $\mathbb{C}$

5) Théorème des zéros faibles

Théorème (Nullstellensatz)
Considérons le système $\begin{cases} F_1(X_1 \dots X_n) = 0 \\ \vdots \\ F_r(X_1 \dots X_n) = 0 \end{cases}$

avec $F_i \in K[X_1 \dots X_n]$.
Pour que ce système n'admette aucune solution dans K^n, il faut et il suffit que l'idéal I engendré par $F_1, \dots, F_r$ soit égal à $K[X_1 \dots X_n]$

DVT

6) Équation implicite et paramétrisation

Soit une courbe γ décrite par une équation paramétrique rationnelle de la forme

$$x(t) = \frac{P_1(t)}{Q_1(t)}, \quad y(t) = \frac{P_2(t)}{Q_2(t)}$$

avec $P_1, Q_1, P_2, Q_2 \in \mathbb{R}[X]$ et Q_1, Q_2 sans racine réelle
Alors γ est contenu dans la courbe

$$R(X,Y) = \mathrm{Res}_T(Q_1(T)X - P_1(T), Q_2(T)Y - P_2(T)) = 0$$

IV) Discriminant

Définition On appelle discriminant du polynôme $P(X) = a_p \prod_{i=1}^{p}(X - \alpha_i)$, l'élément

$$\Delta(P) = a_p^{2p-2} \prod_{1 \leq i < j \leq p} (\alpha_i - \alpha_j)^2$$

Proposition Si $p = \deg P$ n'est pas divisible par car K, on a $\Delta(A) = \frac{(-1)^{p(p-1)/2}}{a_p} R(P, P')$

On a toujours

$$\Delta(A) \quad \Delta(A) = \begin{vmatrix} a_p & \dots & & p a_p & & \\ \vdots & & a_p & (p-1)a_{p-1} & \dots & p a_p \\ a_0 & \dots & a_0 & a_1 & \dots & a_1 \end{vmatrix}$$

Proposition P a une racine multiple ssi $\Delta(P) = 0$

Application

- théorème de Cayley-Hamilton
- intérieur des matrices diagonalisables de $M_n(\mathbb{C})$

1

Algèbre L3, Szpirglas
Risler - Boyer

Algèbre L3 Szpirglas

Développement : Nullstellensatz (version faible)

Référence : Exercice 10.17 (avec seulement des indications) du cours d'Ulm "Algèbre 2" par Olivier Debarre (disponible en ligne).

→ Théorème : Soit K un corps algébriquement clos.
Considérons le système :
$$(S)\quad \begin{cases} F_1(x_1, \dots, x_n) = 0 \\ \vdots \\ F_r(x_1, \dots, x_n) = 0 \end{cases}$$
avec $F_i \in K[X_1, \dots, X_n]$.
Pour que ce système n'admette aucune solution dans K^n il faut et il suffit que l'idéal I engendré par $F_1, \dots, F_r$ soit égal à $K[X_1, \dots, X_n]$ tout entier.

→ Énoncé équivalent : Les idéaux maximaux de $K[X_1, \dots, X_n]$ sont les idéaux :
$$m_x = (X_1 - x_1, \dots, X_n - x_n) \quad \text{pour } x = (x_1, \dots, x_n) \in K^n.$$

→ preuve. $\boxed{\Leftarrow}$ Si $I = K[X_1, \dots, X_n]$ il existe $G_1, \dots, G_r \in K[X_1, \dots, X_n]$ tels que :
$$\sum_{i=1}^{n} G_i F_i = 1,$$ donc (S) ne peut avoir de solution.

$\boxed{\Rightarrow}$ Montrons par récurrence sur n que si I est un idéal propre de $K[X_1, \dots, X_n]$, alors les éléments de I ont un zéro commun.

- Le cas $n = 1$ est trivial car $K[X]$ est principal et K est algébriquement clos.

• Supposons la propriété vraie au rang $n-1$, et soit I un idéal propre de $K[X_1, \_, X_n]$.

Remarquons que I n'est pas inclus dans $K[X_1, \_ X_{n-1}]$, car stable par multiplication par X_n.

Ensuite, quitte à faire un changement linéaire de coordonnées (par exemple pour $\tilde{X}_n = X_n$ et $\tilde{X}_i = X_n + X_i$ pour $1 \leq i \leq n-1$) on peut supposer que I contient un polynôme Q unitaire en X_n, de degré > 0 selon X_n.

▷ Soit $I' = I \cap K[X_1, \_, X_{n-1}]$. I' est un idéal propre de $K[X_1, \_, X_{n-1}]$, car sinon on aurait $1 \in I' \subset I$ donc I ne serait pas propre.

⟶ D'après l'hypothèse de récurrence, les éléments de I' ont un zéro commun $a = (a_1, \_, a_{n-1}) \in K^{n-1}$.

▷ Soit $J = \{P(a_1, \_, a_{n-1}, X_n), P \in I\} \subset K[X_n]$. Montrons que J est un idéal propre de $K[X_n]$. Supposons par l'absurde que il existe $P \in I$ tel que :

$$P(a_1, \_, a_{n-1}, X_n) = 1$$

On a : $\mathrm{Res}_{X_n}(Q, P) \in K[X_1, \_, X_{n-1}]$

• D'autre part il existe $U, V \in K[X_1, \_, X_n]$ tels que :

$$UQ + VP = \mathrm{Res}_{X_n}(Q, P)$$

Ainsi : $\mathrm{Res}_{X_n}(Q, P) \in I \cap K[X_1, \_, X_{n-1}] = I'$ et donc il est annulé par $(a_1, \_, a_{n-1})$.

<u>Écrivons</u> : $P = P_r X_n^r + \dots + P_1 X_n + P_0$

$\qquad\qquad Q = X_n^s + Q_{s-1} X_n^{s-1} + \dots + Q_0$

avec $P_i, Q_j \in K[x_1, \dots, x_{n-1}]$

On a : $\begin{cases} P_0(a) = 1 & \text{car } P(a, x_n) = 1 \\ P_i(a) = 0 & \text{si } i \geq 1 \end{cases}$

$$\mathrm{Res}_{X_n}(Q,P) = \begin{vmatrix} 1 & & P_r & \\ \vdots & \ddots 1 & \vdots & \ddots \quad P_r \\ Q_0 & \vdots & P_0 & \vdots \\ & \ddots \quad Q_0 & & \ddots \quad P_0 \end{vmatrix}$$

On évalue en a : $$\mathrm{Res}_{X_n}(Q,P)(a) = \begin{vmatrix} 1 & & \\ \vdots \ddots 1 & & 0 \\ Q_0(a) \vdots & 1 & \\ \ddots Q_0(a) & & \ddots \; 1 \end{vmatrix} = 1.$$

On obtient une contradiction, donc J est un idéal propre de $K[X_n]$, donc annulé par un $a_n \in K$.

<u>Bilan</u> : $(a_1, \dots, a_n)$ annule tous les éléments de I.

$\longrightarrow$ <u>Montrons l'équivalence des 2 énoncés</u> :

$\triangleright$ Soit I un idéal de $K[x_1, \dots, x_n]$. Comme $K[x_1, \dots, x_n]$ est noethérien, I est engendré par un nombre fini d'éléments $F_1, \dots, F_r$. Pour que x soit solution du système associé aux F_i, il faut et il suffit que I i.e. $I \subset \mathrm{Ker}(e_x)$ où e_x désigne l'évaluation en x. Or $\mathrm{Ker}(e_x) = m_x$ et m_x est maximal car on a un isomorphisme d'anneaux suivant résultant de la factorisation de e_a :

$$K[X_1, \dots, X_n]/m_a \simeq K \text{ qui est un corps.}$$

Le théorème s'écrit donc :

$$\left\{ \begin{array}{l} I \text{ n'est contenu dans aucun} \\ \quad \text{des } m_x \end{array} \right\} \Longleftrightarrow I = K[X_1, \dots, X_n]$$

Et cela revient à dire que les idéaux maximaux de $K[X_1, \dots, X_n]$ sont exactement les m_a pour $a \in K^n$.

Développement : Théorème d'intersection de Bezout (version faible)

Référence : • Szpirglas : Algèbre L3

→ **Théorème** : Soit k un corps et C_0, C_1 deux courbes algébriques irréductibles planes affines distinctes de degrés respectif m_0 et m_1.

Alors $C_0 \cap C_1$ a au plus $m_0 . m_1$ éléments.

Remarque : Dire que C_0 et C_1 sont deux courbes algébriques irréductibles planes affines distinctes de degrés m_0 et m_1 signifie qu'il existe deux polynômes $P_0, P_1 \in k[X,Y]$ irréductibles, non proportionnels de degrés m_0 et m_1, tels que :

$$\begin{cases} C_0 = V(P_0) := \{(x,y) \in k^2, P_0(x,y) = 0\} \\ C_1 = V(P_1) := \{(x,y) \in k^2, P_1(x,y) = 0\} \end{cases}$$

⟶ preuve : Si $(x,y) \in C_1 \cap C_0$ alors :

$P_0(x,y) = P_1(x,y) = 0$ donc en particulier x est racine de $Res_Y(P_0, P_1) \in k[X]$.

Quel est le degré de $Res_Y(P_0,P_1)$?

Écrivons : $\begin{cases} P_0(X,Y) = a_{m_0} Y^{m_0} + \dots + a_1 Y + a_0 \\ P_1(X,Y) = b_{m_1} Y^{m_1} + \dots + b_1 Y + b_0 \end{cases}$

avec $a_i, b_j \in k[X]$ et : $\begin{cases} d^{\circ}(a_i) \leq m_0 - i \\ d^{\circ}(b_j) \leq m_1 - j \end{cases}$

$$\mathrm{Syl}_y(P_0,P_1)=\begin{pmatrix} a_{m_0} & & b_{m_1} & \\ \vdots & \ddots \quad a_{m_0} & \vdots & \ddots \quad b_{m_1} \\ a_0 & \vdots & b_0 & \vdots \\ & \ddots \quad a_0 & & \ddots \quad b_0 \end{pmatrix} = \left[C_{ij}(x)\right]_{1\leq i,j\leq m_0+m_1}$$

en passant au degré :
$$\begin{pmatrix} \leq 0 & -\infty & \leq 0 & -\infty \\ \vdots & \leq 0 & \vdots & \\ \leq m_0 & \vdots & \leq m_1 & \leq 0 \\ -\infty & \leq m_0 & -\infty & \leq m_1 \end{pmatrix}$$

Ainsi : $d^\circ(C_{ij}) \leq \begin{cases} i-j & \text{si } j\leq m_1 \\ i-j+m_1 & \text{sinon} \end{cases}$

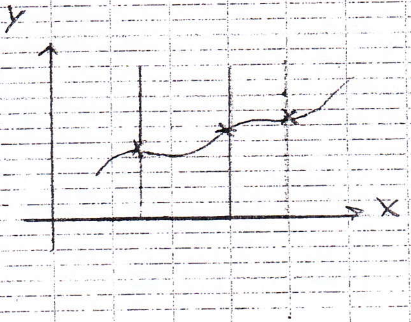
$$\mathrm{Res}_y(P_0,P_1)=\sum_{\sigma\in S_{m_0+m_1}} \prod_{j=1}^{m_1} C_{\sigma(j),j}\cdot\prod_{j=m_1+1}^{m_0+m_1} C_{\sigma(j),j}$$

donc $d^\circ(\mathrm{Res}_y(P_0,P_1)) \leq \sum_{j=1}^{m_1}(\sigma(j)-j) + \sum_{j=m_1+1}^{m_0+m_1}(\sigma(j)-j+m_1)$

$$= \underbrace{\sum_{j=1}^{m_0+m_1}(\sigma(j)-j)}_{=0} + m_0m_1 = m_0m_1$$

Par ailleurs $\mathrm{Res}_y(P_0,P_1)$ est non nul car P_0 et P_1 sont irréductibles non proportionnels, donc il y a au plus m_0m_1 possibilités pour x, et de même pour y car on a aussi : $d^\circ(\mathrm{Res}_x(P_0,P_1)) \leq m_0m_1$.

$\Rightarrow \# C_0\cap C_1 \leq (m_0m_1)^2$.



→ L'idée est maintenant de projeter dans une direction où on sait qu'il n'y a pas deux points de $C_0\cap C_1$ alignés.

Ici on a projeté $C_0 \cap C_1$ sur X dans la direction de Y, mais si D et Δ sont deux droites de k^2 non parallèles, alors on obtient par le même raisonnement que l'image de $C_1 \cap C_0$ par la projection sur Δ selon la direction D est de cardinal $\leqslant m_0 m_1$.

Quitte à étendre k (par exemple en prenant $\bar{k}$) on peut considérer k infini, et alors on peut considérer une droite D de k^2 non parallèle aux droites joignant deux points de $C_0 \cap C_1$. Soit Δ une droite non parallèle à D, et π la projection sur Δ selon la direction D.

Alors d'une part : $\pi_{|C_0 \cap C_1}$ est injective.

D'autre part : $\#(\pi(C_0 \cap C_1)) \leq m_0 m_1$.

Donc : $\boxed{\#(C_0 \cap C_1) \leq m_0 m_1}$.