Problématique : résoudre des systèmes d'équations polynômiales

Exemple
$$\begin{cases} X^3+Y+Z-1=0 \\ X+Y^3+Z-1=0 \\ X+Y+Z^3-1=0 \end{cases}$$

Méthode : "élimination" des variables

I - Introduction aux résultants et à la théorie de l'élimination

Cadre : A anneau unitaire, commutatif et intègre.

1) Définition et propriétés de base

Soient $P, Q \in A[X]$, $P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{i=0}^{m} b_i X^i$, $\deg P + \deg Q > 0$

Définition 1 : • la matrice de Sylvester de P et Q est la matrice de $\mathcal{M}_{n+m}(A)$:

$$Syl(P,Q) = \begin{array}{c} \left(\begin{array}{cccccccc} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_2 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 \end{array}\right) \end{array} \begin{array}{l} \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} m \text{ lignes} \\ \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} n \text{ lignes} \end{array}$$

• Résultant de P et Q : $Res(P,Q) := \det(Syl(P,Q))$

Remarques : • on note $A_d = \{P \in A[X] \mid \deg P < d\}$. $Res(P,Q)$ est le déterminant de
$$\begin{array}{ccc} A_{m-1} \times A_{n-1} & \to & A_{n+m-1} \\ (U,V) & \mapsto & UP+VQ \end{array}$$

• Si $P, Q \in A[X_1, \dots, X_d]$, on note $Res_{X_i}(P,Q)$ le résultant de P et Q comme polynômes en X_i ; c'est un élément de $A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_d]$: la variable X_i est "éliminée" !

Exemple 2 : $P = X+3$, $Q = 2X^2 - X + 1$, $A = \mathbb{Z}$
$$Res(P,Q) = \begin{vmatrix} 1 & 3 & 0 \\ 0 & 1 & 3 \\ 2 & -1 & 1 \end{vmatrix} = 14.$$

Proposition 3 : on suppose $\deg Q > 0$. Soit $\alpha \in A$.
a) $Res(\alpha, Q) = \alpha^m$ b) $Res(Q,Q) = 0$
c) $Res(\alpha P, Q) = \alpha^m Res(P,Q)$ d) $Res(P,Q) = (-1)^{mn} Res(Q,P)$
e) $Res(X^k P, Q) = b_0^k Res(P,Q)$ $(k \geq 0)$.

2) Lien avec le pgcd

Théorème 4 : il existe $U, V \in A[X]$ avec $\deg U < \deg Q$, $\deg V < \deg P$, tels que $UP + VQ = Res(P,Q)$

Remarque : autrement dit, $Res(P,Q) \in (P) + (Q) \subset A[X]$

Corollaire 5 : on suppose A factoriel. Alors $Res(P,Q) = 0$ ssi P et Q ont un facteur commun dans $A[X]$ non constant

Conséquence : $Res(P,Q) = 0$ ssi P et Q ont une racine commune dans une clôture algébrique de $Frac(A)$

Application 6 : méthode d'élimination. Soient $P, Q \in \mathbb{C}[X,Y]$. Si $(\alpha, \beta) \in \mathbb{C}^2$ est un zéro commun alors $P(\alpha, Y)$ et $Q(\alpha, Y)$ ont β comme racine commune, donc $Res(P(\alpha,Y), Q(\alpha,Y)) = 0$. Le polynôme $R(X) = Res_Y(P,Q)$ admet alors α pour racine.

Exemple 7 : $P = X^2 + 2X - XY + 2Y - 6$,
$Q = 3X^2 - 5X + 5 + XY - 2Y$, $P, Q \in \mathbb{Q}[X,Y]$.

$R(Y) = Res_X(P,Q) = (36Y - 103)(Y-3) \to \beta \in \{3, 103/36\}$

• $\beta = 3$: $pgcd(P(X,3), Q(X,3)) = X - 1 \to \alpha = 1$

• $\beta = 103/36 \to \alpha = -1/4$

Deux solutions : $(1,3)$ et $(-1/4, 103/36)$

Question : combien y a-t-il de solutions dans le cas général ?

(DEV 1)

Théorème 8 (borne de Bézout) soient k un corps infini, $P, Q \in k[X,Y]$ de degrés totaux respectifs d et d', premiers entre eux. Alors les courbes $C_P = \{(x,y) \in k^2 \mid P(x,y)=0\}$ et $C_Q = \{(x,y) \in k^2 \mid Q(x,y)=0\}$ ont au plus dd' points d'intersection.

Application 9: deux coniques distinctes ont au plus 4 points d'intersection $\rightarrow$ unicité de la conique passant par 5 points distincts.

3) Morphismes et théorème d'extension

Théorème 10 soit $\Phi : A \to B$ un morphisme d'anneaux intègres étendu à $\Phi : A[X] \to B[X]$, $X \mapsto X$. On suppose que $\deg \Phi(P) = \deg P$ et que $\deg \Phi(Q) = \deg Q - k$ avec $k \geq 0$.

Alors $\boxed{\Phi(\mathrm{Res}(P,Q)) = \Phi(a_n)^k \mathrm{Res}(\Phi(P), \Phi(Q))}$

Théorème 11 (d'extension) soient k un corps algébriquement clos, $P, Q \in k[X_1, \dots, X_d]$, $P = \sum_{i=0}^{n} a_i X_d^i$, $Q = \sum_{i=0}^{m} b_i X_d^i$, $a_i, b_j \in k[X_1, \dots, X_{d-1}]$

1) Si $(\alpha_1, \dots, \alpha_d) \in k^d$ est zéro commun à P et Q alors $(\alpha_1, \dots, \alpha_{d-1})$ est racine de $\mathrm{Res}_{X_d}(P,Q)$.

2) Si $\mathrm{Res}_{X_d}(P,Q)(\alpha_1, \dots, \alpha_{d-1}) = 0$ et si $(\alpha_1, \dots, \alpha_{d-1})$ n'est pas zéro commun à a_n et b_m, alors il existe $\alpha_d \in k$ tel que $(\alpha_1, \dots, \alpha_d)$ soit zéro commun à P et Q.

Exemple 12: Reprenons l'exemple 7. $\beta = 3$ est racine de $R(Y) = \mathrm{Res}_X(P,Q)$. Le terme de tête en X de P est 1, qui n'annule pas β : il existe $\alpha \in \overline{\mathbb{Q}}$ tel que (α, β) soit zéro commun à P et Q (en l'occurrence $\alpha = 1$)

II - Calcul effectif du résultant et conséquences

1) Algorithme d'Euclide

Proposition 13: soient $P, Q \in A[X]$, soit R le reste de la division euclidienne de P par Q dans $\mathrm{Frac}(A)[X]$. Alors, en notant $r = \deg R$, $\boxed{\mathrm{Res}(P,Q) = (-1)^{mn} b_m^{n-r} \mathrm{Res}(Q,R)}$

Remarques: • pour effectuer la division euclidienne il faut travailler avec un anneau euclidien. On peut calculer dans $\mathrm{Frac}(A)[X]$, et effectuer des divisions euclidiennes successives, jusqu'à ce que $\deg R = 0$ ou $R = 0$, sachant que le résultat final est bien dans A.

• on pourrait aussi utiliser la pseudo-division dans A.

Exemple 14: Reprenons de nouveau l'exemple 7

$R_1 = (11/3 - 4/3\,Y)X - 23/3 + 8/3\,Y$, reste de P par Q ;

$R_2 = 3\dfrac{309 - 211Y + 36Y^2}{(4Y-11)^2}$, reste de Q par R_1. $\deg_X R_2 = 0$.

D'où $\mathrm{Res}_X(P,Q) = 3\,\mathrm{Res}_X(Q, R_1) = 3 \cdot (4Y-11)^2 \mathrm{Res}_X(R_1, R_2)$.
$= 309 - 211Y + 36Y^2$

2) Lien résultant - racines

Théorème 15: Écrivons $\begin{cases} P = a_n(X-\alpha_1) \dots (X-\alpha_n) \\ Q = b_m(X-\beta_1) \dots (X-\beta_m) \end{cases}$ dans $\overline{\mathrm{Frac}(A)}$

$$\boxed{\begin{aligned} \mathrm{Res}(P,Q) &= b_m^n a_n^m \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) \\ &= a_n^m \prod_{i=1}^{n} Q(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} P(\beta_j) \end{aligned}}$$

Proposition 16 (théorème de Kronecker) soit $P \in \mathbb{Z}[X]$ unitaire de degré ≥ 1. On suppose que les racines de P sur $\mathbb{C}$ sont de module inférieur ou égal à 1 et non nulles. Alors les racines de P sont des racines de l'unité. (DEV 2)

3) Discriminant d'un polynôme

Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, soient $\alpha_1, \dots, \alpha_n \in \overline{\mathrm{Frac}(A)}$ ses racines.

Définition 17 : $\boxed{\mathrm{Disc}(P) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2}$

Remarque : $\mathrm{Disc}(P) = 0$ ssi P possède une racine double

Proposition 18 : $\boxed{\mathrm{Disc}(P) = \frac{(-1)^{n(n-1)/2}}{a_n} \mathrm{Res}(P, P')}$

Application 19 : L'ensemble des matrices de $\mathcal{M}_n(\mathbb{C})$ à n valeurs propres distinctes forme un ouvert de $\mathcal{M}_n(\mathbb{C})$

III - Quelques applications des résultants

1) Calcul de polynômes annulateurs

Problème : soient k un corps, $\alpha, \beta \in \overline{k}$ de polynômes annulateurs respectifs P et Q. Déterminer un polynôme annulateur de $\alpha+\beta$, $\alpha\beta$

Proposition 20 : • $R_1(X) = \mathrm{Res}_Y(P(Y), Q(X-Y))$, $R_2(X) = \mathrm{Res}_U(Q(U), \mathrm{Res}_T(P(T), X-(T+U)))$ sont des polynômes annulateurs de $\alpha+\beta$

• $R(X) = \mathrm{Res}_Y(P(Y), X^{\deg Q} Q(\frac{Y}{X}))$ est un polynôme annulateur de $\alpha\beta$

Corollaire 21 : l'ensemble des éléments algébriques sur k est un corps.

Exemple 22 : $k = \mathbb{Q}$, $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, $P = X^2 - 2$, $Q = X^2 - 3$

$R_1(X) = \mathrm{Res}_Y(Y^2 - 2, Y^2 - 2XY + X^2 - 3) = X^4 - 10X^2 + 1$ est un polynôme annulateur de $\alpha + \beta$

2) Formule de Héron

Problème : soit ABC un triangle. On pose $a = BC$, $b = AC$, $c = AB$, et $p = \frac{1}{2}(a+b+c)$ le demi-périmètre. Exprimer l'aire de ABC, $\mathcal{A}$, en fonction de a, b, c.

Proposition 23 : $\boxed{\mathcal{A} = \sqrt{p(p-a)(p-b)(p-c)}}$

Avec les résultants :

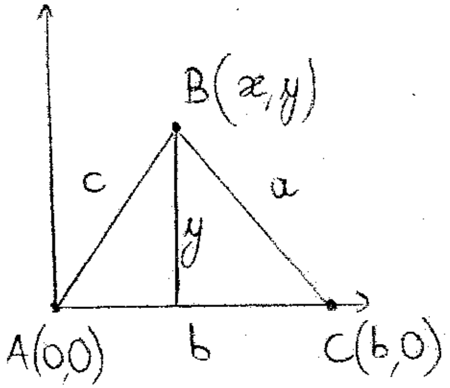
- poser les équations polynômiales correspondant au problème (voir figure 1)
- à l'aide du résultant, éliminer les variables x et y du système d'équations

3) Intégration des fractions rationnelles

Problème : soit $\frac{P}{Q} \in \mathbb{Q}(X)$ propre ($\mathrm{pgcd}(P, Q) = 1$, $\deg P < \deg Q$, Q unitaire de degré ≥ 1). Déterminer une primitive formelle de $\frac{P}{Q}$? Si $\alpha_1, \dots, \alpha_d$ sont les racines distinctes de Q dans $\mathbb{C}$, alors $\int \frac{P}{Q}$ est de la forme $\frac{G}{Q} + \sum_{i=1}^{d} \log(X - \alpha_i) c_i$, $G \in \mathbb{Q}[X]$, $c_1, \dots, c_d \in \mathbb{C}$.

Théorème 24 (Rothstein-Trager) Soient $P, Q \in \mathbb{Q}[X]$, $\mathrm{pgcd}(P,Q) = 1$, $\deg P < \deg Q$, Q sans facteur carré et unitaire. Soit K une extension de $\mathbb{Q}$ dans laquelle on puisse écrire $\int \frac{P}{Q} = \sum_{i=1} c_i \log P_i$ où les $c_i \in \mathbb{C}^*$ sont deux à deux distincts, $P_i \in K[X]$ unitaires non constants sans facteur carré. Alors les c_i sont les racines distinctes du polynôme $R(Y) = \mathrm{Res}_X(P - YQ', Q) \in K[Y]$, et pour tout i, $P_i = \mathrm{pgcd}(P - c_i Q', Q)$.

(DEV 3)



- $\mathcal{A} = \frac{1}{2} b y$
- $x^2 + y^2 - c^2 = 0$
- $(b-x)^2 + y^2 - a^2 = 0$

Figure 1 - Formule de Héron

Bibliographie : Saux Picart, Algorithmes fondamentaux.
Mérindol, Nombres et algèbre
Szpiglas, Algèbre L3