

Cadre : A un anneau commutatif unitaire intègre. K un corps et $\bar{K}$ sa clôture algébrique, $A_d[X]$ l'ensemble des polynômes à coefficients dans A et de degré $\leq d$. $P = \sum_{i=0}^d a_i X^i$ et $Q = \sum_{j=0}^d b_j X^j$ avec $a_d \neq 0$ et $b_d \neq 0$

I - Définitions et premières propriétés

1) Matrice de Sylvester et résultant

Def 1 : La matrice de Sylvester de P et Q est la matrice carrée d'ordre $p+q$ définie par $Sylv(P, Q) = \begin{pmatrix} a_p & & & b_q & & \\ & \ddots & & & \ddots & \\ & & a_p & & & \\ & & & b_q & & \\ & & & & \ddots & \\ & & & & & b_q \\ & & & & & & \ddots \\ & & & & & & & b_q \\ & & & & & & & & \ddots \\ & & & & & & & & & b_q \end{pmatrix}$
On appelle résultant de P et Q le déterminant de cette matrice et on le note $\text{Res}(P, Q)$.

Prop 2 : $Sylv(P, Q)$ est la matrice de l'application $\Phi: A_{p+q-1}[X] \times A_{p+q-1}[X] \rightarrow A_{p+q-1}[X]$ dans les bases $(U, V) \mapsto PU + QV$
 $((X^{p+q-1}, 0), \dots, (X, 0), (0, X), \dots, (0, X^{p+q-1}))$ et $(X^{p+q-i})_{i \in \{1, \dots, p+q\}}$

Ex 3 : $\text{Res}(\Phi_3, \Phi_6) = \text{Res}(X^2 + X + 1, X^2 - X + 1) = 4$

Prop 4 : $\text{Res}(P, Q) \in \mathbb{Z}[a_0, \dots, a_p, b_0, \dots, b_q] \subset A$ donc le résultant est continu en les coefficients des polynômes.

Prop 5 : Soit $d \in A$ et Q de degré ≥ 1 ,

- $\text{Res}(d, Q) = d^q$
- $\text{Res}(Q, Q) = 0$
- $\text{Res}(dP, Q) = d^q \text{Res}(P, Q)$
- $\text{Res}(P, Q) = (-1)^{pq} \text{Res}(Q, P)$
- $\text{Res}(X^k P, Q) = b_0^k \text{Res}(P, Q) \quad (k \geq 0)$

2) Lien avec le PGCD

Thm 6 : Il existe $(U, V) \in \text{Frac}(A)[X] \times \text{Frac}(A)[X]$ tel que $P(X)U(X) + Q(X)V(X) = \text{Res}(P, Q)$

Thm 7 : Si A est factoriel, $\deg(\text{PGCD}(P, Q)) \geq 1 \Leftrightarrow \text{Res}(P, Q) = 0$

Ex 8 : Soit $B = \mathbb{Q}[X_1, X_2, Y_1, Y_2] / (X_1 Y_2 - X_2 Y_1)$, B est intègre mais n'est pas factoriel. Soit $P = x_1 X + x_2 Y$ et $Q = y_1 X + y_2 Y$ dans $B[X]$ où x_1, x_2, y_1, y_2 sont les classes de X_1, X_2, Y_1, Y_2 dans B . On a $\text{Res}(P, Q) = 0$ mais P et Q n'ont pas de facteurs communs non constants dans $B[X]$

Coro 9 : Soit $P, Q \in \mathbb{C}[X]$, (P, Q) sont premiers entre eux ssi $\text{Res}(P, Q) \neq 0$
(fonctionne aussi avec $A(X)$ factoriel)

Appli 10 : L'intérieur de l'ensemble des matrices diagonalisables de $M_n(\mathbb{C})$ est l'ensemble des matrices diagonalisables à valeurs propres distinctes.

II - Calcul effectif du résultant

1) Algorithme d'Euclide

Notation : On note $\text{Frac}(A)$ le corps des fractions de A , On a $\text{Frac}(A)[X]$ est un anneau euclidien

Prop 11 : Si $p = \deg(P) \geq q = \deg(Q)$ et si R est le reste de la division euclidienne de P par Q dans $\text{Frac}(A)[X]$, alors :

$$\text{Res}(P, Q) = (-1)^{pq} b_q^{p-r} \text{Res}(Q, R), \text{ où } r = \deg(R)$$

Ex 12 : $P = X^2 + 2X - XY + 2Y - 6$ et $Q = 3X^2 - 5X + 5 + XY - 2Y \in \mathbb{Z}[Y][X]$

La suite des restes successifs des divisions euclidiennes est $R_1 = (\frac{11}{3} - \frac{4}{3}Y)X - \frac{23}{3} + \frac{8}{3}Y$, $R_2 = 3 \frac{309 - 211Y + 36Y^2}{(4Y - 11)^2}$, $R_3 = 0$

$$\text{alors } \text{Res}_X(P, Q) = (-1)^4 \times 3^{2-1} \times \text{Res}_X(Q, R_1) = 3 \times \left(\frac{11}{3} - \frac{4}{3}Y\right)^2 \text{Res}_X(R_1, R_2) = 309 - 211Y + 36Y^2$$

2) Liens avec les racines des polynômes

Prop 13 : Soient P et $Q \in A[X]$, α_i les racines de P dans $\text{Frac}(A)$ et β_j les racines de Q dans $\text{Frac}(A)$, on a alors $P(X) = a_p \prod_{i=1}^p (X - \alpha_i)$ et $Q(X) = b_q \prod_{j=1}^q (X - \beta_j)$.

$$\text{Alors } \text{Res}(P, Q) = (-1)^{pq} b_q^p \prod_{j=1}^q P(\beta_j) = a_p^q \prod_{i=1}^p Q(\alpha_i) = a_p^q b_q^p \prod_{1 \leq i \leq p, 1 \leq j \leq q} (\alpha_i - \beta_j)$$

Ex 14 : $\text{Res}(\Phi_p, \Phi_{2p}) = 2^{p-1}$

Prop 15 : Multiplicativité du résultant. Si $P = \sum_{i=0}^p a_i X^i$, $Q_1 = \sum_{i=0}^q b_i X^i$ et $Q_2 = \sum_{i=0}^r c_i X^i$ avec $a_p b_q b'_r \neq 0$ alors $\text{Res}(P, Q_1 Q_2) = \text{Res}(P, Q_1) \text{Res}(P, Q_2)$

Appli 16 : (Thm de Kronecker). Soit $P \in \mathbb{Z}[X]$ unitaire de degré $n \geq 1$. Si $P(0) \neq 0$ et si les racines de P dans $\mathbb{C}$ sont de module ≤ 1 , alors les racines de P sont des racines de l'unité

Coro 17 : Si $P \in \mathbb{Z}[X]$ est unitaire, irréductible, avec des racines toutes de module ≤ 1 , alors $P = X$ ou P est un polynôme cyclotomique.

[GOU] p208

[GOU] p208

[SP] p144

[S-P] p145

[SP] p146

[SZP] p587

[SZP] p567

[SZP] p573

[GOU] p89

III- Applications algébriques

1) Discriminant

[SZP]
p567

Def 18 On appelle discriminant de $P(X) = a \prod_{i=1}^p (X - d_i) \in A[X]$ avec $a \neq 0$ et $d_i \in \text{Frac}(A)$, la quantité $\Delta(P) = a^{2p-2} \prod_{1 \leq i < j \leq p} (d_i - d_j)^2$

[SZP]
p569

Ex 19 Si $P(X) = aX^2 + bX + c$ avec $a \neq 0$ alors $\Delta(P) = b^2 - 4ac$

[SZP]
p568

Thm 20 Si $P(X) = \sum_{i=0}^p a_i X^i$ avec $p \neq 0$ [car(K)] alors on a

$$\Delta(P) = \frac{(-1)^{\frac{p(p-1)}{2}}}{a_p} \text{Res}(P, P')$$

[SZP]
p569

Prop 21 Si $P(X) \in K[X]$ avec K un corps. Supposons qu'il existe $d_1, \dots, d_m \in K$ tels que $P(X) = (X - d_1) \dots (X - d_m)$ alors

$$\Delta(P) = \prod_{1 \leq i < j \leq m} (d_i - d_j)^2 = (-1)^{\frac{m(m-1)}{2}} \prod_{i=1}^m P'(d_i) = (-1)^{\frac{m(m-1)}{2}} \text{Res}(P, P')$$

[SZP]
p569

Cor 22 Si K est algébriquement clos et $P \in K[X]$ alors P a une racine multiple ssi $\Delta(P) = 0$

[SZP]
p791

Ex 23 : $\Delta(X^3 + pX + q) = -(4p^3 + 27q^2)$
 $\Delta(X^5 + pX^2 + q) = 108qp^5 + 5^5 q^4$

2) Eléments algébriques

[SZP]
p714
ou p571

Def 24 Soit $K(d)/K$ une extension simple. S'il existe $P \in K[X]$ tq $P(d) = 0$, on dit que d est algébrique sur K .

[SZP]
p714
ou p571

Prop 25 Soit L/K une extension de corps. Soient $\alpha, \beta \in L$ algébriques sur K avec $\beta \neq 0$ alors $\alpha + \beta$ et α/β sont algébriques sur K . Plus précisément, si $P \in K[X]$ annule α et $Q \in K[X]$ annule β alors
 $S(Y) = \text{Res}_X(P(X), Q(Y-X))$ annule $\alpha + \beta$
 $P(Y) = \text{Res}_X(P(X), X^q Q(Y/X))$ annule α/β

[SZP]
p572

Ex 26 Si $\alpha = \frac{\sqrt{5}-1}{2}$ et $\beta = \sqrt{3}$ alors $P(X) = X^2 + X - 1$ annule α et $Q(X) = X^2 - 3$ annule β . On a $S(\alpha + \beta) = P(\alpha/\beta) = 0$ avec $S(Y) = Y^4 + 2Y^3 - 8Y^2 - 10Y + 2$ et $P(Y) = Y^4 - 9Y^2 + 9$

Coro 27 : L'ensemble des entiers algébriques est un anneau (c'est même un corps)

3) Elimination dans les systèmes polynomiaux

Le principe de la méthode d'élimination est le suivant : pour trouver les racines communes à deux polynômes à plusieurs variables, on fait "disparaître" une variable grâce au résultant.

Méthode 28 Dans le cas où $P, Q \in \mathbb{C}(X, Y)$ alors si (d, β) est une solution alors $P(X, \beta)$ et $Q(X, \beta)$ ont une solution commune d donc $\text{Res}_X(P(X, \beta), Q(X, \beta)) = 0$ donc β est une racine de $\text{Res}_X(P, Q) \in \mathbb{C}(Y)$. Donc on fait :

- calcul de $\text{Res}_X(P, Q) \in \mathbb{C}(Y)$
- on détermine ses racines
- pour chaque racine $\beta \in \mathbb{C}$, on détermine les racines de $P(X, \beta)$ et $Q(X, \beta)$ dans $\mathbb{C}$. Chaque racine commune $d \in \mathbb{C}$ donne (d, β) racine commune de P et Q dans $\mathbb{C}(X, Y)$.

Thm 29 Soit K corps algébriquement clos, $P, Q \in K(Y_1, \dots, Y_k)[X]$
 $P = \sum_{i=0}^p a_i X^i$ et $Q = \sum_{i=0}^q b_i X^i$ avec $a_i, b_i \in K(Y_1, \dots, Y_k)$ et $m \neq 0$
 Si $P(d_1, \dots, d_k, d) = Q(d_1, \dots, d_k, d) = 0$ alors $\text{Res}_X(P, Q)(d_1, \dots, d_k) = 0$
 Réciproquement, si $(d_1, \dots, d_k)$ annule $\text{Res}_X(P, Q)(d_1, \dots, d_k) = 0$ alors une des 4 conditions est vérifiée :

- $\exists d \in K, Q(d_1, \dots, d_k, d) = P(d_1, \dots, d_k, d) = 0$
- $P(d_1, \dots, d_k)(X) = 0$
- $Q(d_1, \dots, d_k)(X) = 0$
- $a_m(d_1, \dots, d_k) = b_n(d_1, \dots, d_k) = 0$

Ex 30 $\begin{cases} P = X^2 + 2X - XY + 2Y - 6 = 0 \\ Q = 3X^2 - 5X + 5 + XY - 2Y = 0 \end{cases}$

$\text{Res}_X(P, Q) = (36Y - 103)(Y - 3)$

La seule racine commune de $\begin{cases} P(X, 3) \text{ et } Q(X, 3) \text{ est } 1 \\ P(X, \frac{103}{36}) \text{ et } Q(X, \frac{103}{36}) \text{ est } -\frac{1}{4} \end{cases}$

Donc le système a 2 solutions $(1, 3)$ et $(-\frac{1}{4}, \frac{103}{36})$

Rmq 31 : Avec le thm comme les racines de $\text{Res}_X(P, Q)$ sont 3 et $\frac{103}{36}$ et que le coefficient dominant de P en X est 1 et celui de Q est 3 qui n'ont pas de racines communes. Donc on a l'existence de $\alpha, \beta \in \mathbb{Q}$ tels que $(\alpha, 3)$ et $(\beta, \frac{103}{36})$ soient racines communes de P et Q .

[S-P]
p147

[S-P]
p148

[S-P]
p147

[S-P]
p147

avant
thm
29

[S-P] p148 Lem 32 : Si $P, Q \in A[X]$ et φ un morphisme d'anneaux de A dans B . On note φ son extension en un morphisme de $A[X]$ dans $B[X]$. On a $\varphi(\text{Res}(P, Q)) = (\varphi(\text{am}))^{n-k} \text{Res}(\varphi(P), \varphi(Q))$ où $k = \deg(\varphi(Q))$

[S-P] p149 Ex 33 $\begin{cases} P(X, Y) = Y^2 X^2 - Y X^2 - 2YX + 5 = 0 \\ Q(X, Y) = XY^2 + YX - 2X + 2Y - 7 = 0 \end{cases}$
 $\text{Res}_X(P, Q) = 13Y^4 + 40Y^2 - 32Y^3 - 41Y + 20$ dont une racine évidente est 1. Or $Q(X, 1) = -5$ donc pas de solutions en $(1, 1)$. Situation d) du théorème 29.

IV - Applications géométriques

1) Equation implicite d'une courbe paramétrée

[NER] p385 Pbm 34 Soit k corps algébriquement clos et soient F et $G \in k[T]$ de degrés respectifs n et m . On considère la courbe plane paramétrée par $C = \{(x, y) \in k^2 \mid \exists t \in k, x = F(t) \text{ et } y = G(t)\}$. On cherche à trouver un polynôme $R \in k[X, Y]$ tel que :
 $C = \{(x, y) \in k^2 \mid R(x, y) = 0\}$

[NER] p385 Méthode 35 : On pose $\tilde{F}(X, Y, T) = F(T) - X$ et $\tilde{G}(X, Y, T) = G(T) - Y$ polynômes de $k[X, Y][T]$ de degrés respectifs n et m . Le résultant de ces 2 polynômes est un élément $R(X, Y) \in k[X, Y]$. Ainsi $R(x, y)$ est le résultant de $F(T) - x$ et $G(T) - y$. Comme k est algébriquement clos, ce résultant s'annule en (x, y) ssi il existe une racine commune $t \in k$ à $F(T) - x$ et $G(T) - y$ i.e $x = F(t)$ et $y = G(t)$. Ainsi $R(x, y) = 0$ ssi $(x, y) \in C$

Ex 36 : Soit $C = \{(t^3 - 1, t^2 + 1) \in \mathbb{C}^2 \mid t \in \mathbb{C}\}$ alors on pose $\tilde{F}(X, Y, T) = T^3 - 1 - X \in \mathbb{C}[X, Y][T]$ et $\tilde{G}(X, Y, T) = T^2 + 1 - Y \in \mathbb{C}[X, Y][T]$, on a alors
 $C = \{(x, y) \in \mathbb{C}^2 \mid (1 - y)^3 + (1 + x)^2 = 0\}$

2) Intersection de courbes planes

Def 37 La courbe affine plane $V(A)$ définie par un polynôme $A(X, Y)$ non constant de $\mathbb{C}[X, Y]$ est le sous-ensemble de $\mathbb{C}^2$:
 $V(A) = \{(x, y) \in \mathbb{C}^2 \mid A(x, y) = 0\}$

Thm 38 : Soient $P, Q \in \mathbb{C}[X, Y]$ irréductibles et non proportionnels. On a alors $V(P) \cap V(Q)$ est formée d'un nombre fini de points. Alors les éléments (x, y) de $V(P) \cap V(Q)$ vérifient :
 $\begin{cases} \text{Res}_Y(P, Q)(x) = 0 \\ \text{Res}_X(P, Q)(y) = 0 \end{cases}$ donc $V(P) \cap V(Q)$ est de cardinal au plus $\deg(P)\deg(Q)$.

Ex 39 : Les coniques d'équations $X^2 - Y^2 = 1$ et $X^2 + Y^2 = 3$ ont 4 points d'intersection $(\pm\sqrt{2}, \pm 1)$

Appl 40 Deux coniques distinctes ont au plus 4 points d'intersection

[SZP] : Szpirglas, Mathématiques, Algèbre L3

[SP] : Saux-Picart, Cours de calcul formel, Algorithmes fondamentaux.

[NER] : Néerindop, Nombres et algèbre

[Gau] : Gourdon, Algèbre

[SZP]
p588

[SZP]
p589

[SZP]
p590

[SZP]
p589