RÉSULTANT. APPLICATIONS.

143

Cadre: Soit $A$ un anneau intègre; on note $\mathrm{Frac}(A)$ son corps de fractions. Si $K$ est un corps, $\overline{K}$ est sa clôture algébrique.

# I GÉNÉRALITÉS.

## 1 Matrice de Sylvester, Résultant

**Déf 1:**
Soient $P, Q \in A[X]$, de degrés $m$ et $n$.
On définit $\Phi_{P,Q} : \begin{cases} (\mathrm{Frac}(A))_n[X] \times (\mathrm{Frac}(A))_m[X] \to (\mathrm{Frac}(A))_{n+m}[X] \\ (U, V) \mapsto PU + QV \end{cases}$.
La matrice de Sylvester de $P$ et $Q$ est la matrice de $\Phi_{P,Q}$ dans les bases $((X^n,0), \dots, (X,0), (1,0), (0,X^m), \dots, (0,X), (0,1))$ et $(X^{n+m}, \dots, X, 1)$.

**Déf 2:**
Le résultant de $P$ et $Q$ est alors le déterminant de la matrice de Sylvester de $P$ et $Q$, on le note $\mathrm{Res}(P,Q)$.

**Rq 3:**
- La formule du déterminant en fonctions des coefficients de la matrice fournit: $\mathrm{Res}(P,Q) \in A$.
- On peut aussi prendre le déterminant de la transposée de la matrice de Sylvester.

**Ex 4:**
Soient $P = X^2+1 \in \mathbb{Z}[X]$ et $Q = 3X \in \mathbb{Z}[X]$
Alors
$$\mathrm{Res}(P,Q) = \begin{vmatrix} 1 & 3 & 0 \\ 0 & 0 & 3 \\ 1 & 0 & 0 \end{vmatrix} = 9$$

**Prop 5:**
Soient $P, Q \in A[X] \setminus \{0\}$, de degrés $m$ et $n$.
Alors $\mathrm{Res}(P,Q) = 0 \Leftrightarrow$ $P$ et $Q$ ont un multiple commun de degré $< m+n$, dans $A[X] \setminus A$.

## 2 Liens avec le PGCD

**Thm 6:**
On suppose $A$ factoriel, $P, Q \in A[X] \setminus \{0\}$, de degrés $m$ et $n$.
Alors $\mathrm{Res}(P,Q) = 0 \Leftrightarrow$ $P$ et $Q$ ont un multiple commun dans $A[X] \setminus A$.

**Cor 7:**
Sous les mêmes hypothèses,
$\mathrm{Res}(P,Q) = 0 \Leftrightarrow$ $P$ et $Q$ ont une racine commune dans $\overline{\mathrm{Frac}(A)}$.

**Ex 8:**
$\mathrm{Res}(X^2+1, X^4+2X^2+1) = 0$.

**C-ex 9**
Soit $A = \mathbb{Q}[X_1, X_2, Y_1, Y_2] / (X_1Y_2 - X_2Y_1)$; $A$ est intègre.
Soient $x_1, x_2, y_1, y_2$ les classes de $X_1, X_2, Y_1, Y_2$ dans le quotient $A$.
On note $P = x_1X + x_2$, $Q = y_1X + y_2 \in A_2[X]$.
Alors $\mathrm{Res}(P,Q) = 0$ mais $P$ et $Q$ n'ont pas de facteurs communs non-constants

**Thm 10:**
Si $A$ est intègre et $P, Q \in A[X] \setminus \{0\}$, de degrés $m$ et $n$.
Alors $\exists (U,V) \in A_{n-1}[X] \times A_{m-1}[X]$, $PU+QV = \mathrm{Res}(P,Q)$.

# II CALCUL EFFECTIF DU RÉSULTANT

## 1 Algorithme d'Euclide

**Prop 11:**
Soit $A$ intègre; $P, Q \in A[X]$ avec $\begin{cases} \deg P = m \geq 0 \\ \deg Q = n > 0 \end{cases}$; $\alpha \in A$.
On a les formules suivantes:
1) $\mathrm{Res}(\alpha, Q) = \alpha^n$
2) $\mathrm{Res}(Q,Q) = 0$
3) $\mathrm{Res}(\alpha P, Q) = \alpha^n \mathrm{Res}(P,Q)$
4) $\mathrm{Res}(P,Q) = (-1)^{nm} \mathrm{Res}(Q,P)$
5) $\mathrm{Res}(X^k P, Q) = q_0^k \mathrm{Res}(P,Q)$ où $k \in \mathbb{N}$ et $q_0$ est le coefficient constant de $Q$.

**Thm 12: Division euclidienne**
Si $P$ et $Q$ sont deux polynômes de degrés $m$ et $n$ avec $m \geq n$, dans $A[X]$,
Si $R$ est le reste dans la division euclidienne de $P$ par $Q$ dans $(\mathrm{Frac}(A))[X]$,
Alors $\mathrm{Res}(P,Q) = (-1)^{nm} q_n^{m-r} \mathrm{Res}(Q,R)$ où $r$ désigne le degré de $R$ et $q_n$ le coefficient dominant de $Q$.

**Ex 13**: Dans $\mathbb{Z}[X]$,

$\operatorname{Res}(X^4+1, X^3-X+2) = \operatorname{Res}(X^3-X+2, X^2-2X+1)$
$= \operatorname{Res}(X^2-2X+1, 2X) = 4\operatorname{Res}(X^2-2X+1, X)$
$= 4\operatorname{Res}(X, 1) = 4.$

→ Le thm 12 nous fournit donc un algorithme de calcul du résultant, basé sur la division euclidienne dans $(\mathrm{Frac}(A))[X]$.

## 2 Liens avec les racines

**Thm 14**:
Soient $P, Q \in A[X]\setminus A$, de degrés $m$ et $n$.
On note $\alpha_i$ les racines de $P$ dans $\overline{\mathrm{Frac}(A)}$, où $i \in [\![1, m]\!]$
$\beta_j$ les racines de $Q$ dans $\overline{\mathrm{Frac}(A)}$, où $j \in [\![1, n]\!]$.
Soient $p_m$ et $q_n$ les coefficients dominants de $P$ et $Q$.
On a alors :

$$\operatorname{Res}(P,Q) = (-1)^{mn} q_n^m \prod_{j=1}^{n} P(\beta_j) = p_m^n \prod_{i=1}^{m} Q(\alpha_i) = p_m^n b_n^m \prod_{\substack{1\le i\le m \\ 1\le j\le n}} (\alpha_i - \beta_j)$$

**Ex 15**:

$\operatorname{Res}(X^2+X+1, X^2+1) = (-1)^4 1^2 (i^2+i+1)(i^2-i+1) = -i^2 = 1.$

**Cor 16**:
Soient $P, Q_1, Q_2 \in A[X]\setminus A$.
Alors on a : $\operatorname{Res}(P, Q_1Q_2) = \operatorname{Res}(P, Q_1)\operatorname{Res}(P, Q_2)$
et $\operatorname{Res}(Q_1Q_2, P) = \operatorname{Res}(Q_1, P)\operatorname{Res}(Q_2, P)$.

**Thm 17**: Kronecker
Soit $P \in \mathbb{Z}[X]$ unitaire, dont les racines complexes sont dans $\overline{D(0,1)}$.
On suppose $P(0) \neq 0$.
Alors les racines de $P$ sont des racines de l'unité.

**App 18**:
- Soit $P \in \mathbb{Z}[X]$, unitaire, irréductible à racines dans $\overline{D(0,1)}$.
  Alors $P = X$ ou $P$ est un polynôme cyclotomique.
- Si on ne suppose plus $P$ irréductible,
  Alors $P$ est produit d'une puissance de $X$ et de polynômes cyclotomiques.

DEVELOPPEMENT N°1

# III APPLICATIONS EN ALGÈBRE

## 1 Discriminant

**Déf 19**:
Si $P \in A[X]$ est unitaire de degré $m \geq 1$,
Alors $\Delta(P) = (-1)^{m(m-1)/2} \operatorname{Res}(P, P')$ est appelé discriminant de $P$.

**Prop 20**:
Soit $P \in A[X]$, unitaire de degré $m \geq 1$,
Alors $\Delta(P) = 0 \Leftrightarrow P$ a une racine multiple dans $\overline{\mathrm{Frac}(A)}$.

**Ex 21**: Discriminants usuels
$\Delta(X^2+bX+c) = b^2-4c$ et $\Delta(X^3+pX+q) = -4p^3-27q^2$.

**App 22**: Cayley-Hamilton
Soit $n \in \mathbb{N}^*$, $K$ un corps, $M \in \mathcal{M}_n(K)$.
Alors $\chi_M(M) = 0$, où $\chi_M$ est le polynôme caractéristique de $M$.

**App 23**:
Soit $n \in \mathbb{N}^*$,
L'intérieur de l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$ est l'ensemble des matrices diagonalisables à valeurs propres distinctes.

## 2 Éléments algébriques

**Déf 24**:
- Soit $K$ un corps ; $x \in \overline{K}$ est dit algébrique sur $K$ s'il est racine d'un polynôme de $K[X]$.
- $x \in \mathbb{C}$ est appelé entier algébrique s'il est racine d'un polynôme unitaire de $\mathbb{Z}[X]$.

**Prop 25**:
Soient $\alpha, \beta$ algébriques sur $K$ (resp. entiers algébriques)
Alors $\alpha+\beta$ et $\alpha\beta$ sont algébriques sur $K$ (resp. entiers algébriques)

**Cor 26**:
- L'ensemble des éléments algébriques sur $K$ est un corps.
- L'ensemble des entiers algébriques est un anneau.

**Ex 27**:
Le polynôme minimal de $\sqrt{2}+\sqrt[3]{3}$ sur $\mathbb{Q}$ est : $X^6-6X^4-6X^3+12X^2-36X+1$

## 3 Élimination dans les systèmes polynomiaux.

**Lem 28:**
Soient $P, Q \in A[X]$ et $\varphi : A \to B$ un morphisme d'anneaux intègres, qu'on étend en un morphisme de $A[X] \to B[X]$.
Alors $\varphi(\mathrm{Res}(P,Q)) = (\varphi(p_m))^{n-k} \mathrm{Res}(\varphi(P), \varphi(Q))$ où $p_m$ est le coef. dom. de $P$ et $k = \deg(\varphi(Q))$.

**Thm 29:**
Soit $K$ un corps algébriquement clos, $P, Q \in K[Y_1, \dots, Y_k][X]$, on note $P = \sum_{i=0}^{m} p_i X^i$ et $Q = \sum_{j=0}^{n} q_j X^j$ avec $p_m, q_n \neq 0$.
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 $\mathrm{Res}_X(P,Q)(\alpha_1, \dots, \alpha_k) = 0$.
Réciproquement, si $\mathrm{Res}_X(P,Q)(\alpha_1, \dots, \alpha_k) = 0$,
Alors une des assertions suivante est vérifiée :
1) $\exists \alpha \in K,\ P(\alpha_1, \dots, \alpha_k, \alpha) = Q(\alpha_1, \dots, \alpha_k, \alpha) = 0$
2) $P(\alpha_1, \dots, \alpha_k)(X) = 0$ ou $Q(\alpha_1, \dots, \alpha_k)(X) = 0$
3) $p_m(\alpha_1, \dots, \alpha_k) = q_n(\alpha_1, \dots, \alpha_k) = 0$.

**Ex 30:**
- Les solutions de $\begin{cases} X^2 + 2X - XY + 2Y - 6 = 0 \\ 3X^2 - 5X + 5 + XY - 2Y = 0 \end{cases}$ sont $(1,3)$, $(-1/4, 103/56)$
- Apparition de "solutions parasites" :
$\mathrm{Res}_X(Y^2X^2 - YX^2 - 2YX + 5,\ XY^2 + YX - 2X + 2Y - 7) = 13Y^4 + 40Y^2 - 32Y^3 - 41Y + 20$
1 en est une racine mais $Q(X,1) = -5$.

# IV APPLICATIONS EN GÉOMÉTRIE

## 1 Intersections de courbes algébriques planes.

**Déf 31:**
La courbe algébrique plane $V(A)$ définie par $A \in K[X,Y]$ est :
$$V(A) := \{(x,y) \in K^2 \mid A(x,y) = 0\}.$$

DÉVELOPPEMENT N°2

**Thm 32:**
Soient $A, B \in K[X,Y]$ ; on suppose $\#K = \infty$ et $A \wedge B = 1$.
On note $m = \deg A$, $n = \deg B$ (degré total maximal de leurs monômes non-nuls.)
Alors $\#(V(A) \cap V(B)) \leqslant mn$.

**Rq 33:** L'hypothèse $\#K = \infty$ n'est pas nécessaire.

**App 34:** Deux coniques de $\mathbb{R}^2$ s'intersectent en au plus 4 points.

**Ex 35:**
$$\#\left(\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \cap \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 2\}\right) = 0.$$
$$\#\left(\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \cap \{(x,y) \in \mathbb{R}^2 \mid y = x^2\}\right) = 2.$$
$$\#\left(\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \cap \{(x,y) \in \mathbb{R}^2 \mid xy = \tfrac{1}{10}\}\right) = 4.$$

Annexe

## 2 Équations implicites

**Méthode 36:**
Soit $K$ un corps algébriquement clos, $F, G \in K[T]$.
On considère $\mathcal{C} := \{(x,y) \in K^2 \mid \exists t \in K,\ x = F(t) \text{ et } y = G(t)\}$.
On cherche $R \in K[X,Y]$, tq : $\mathcal{C} = \{(x,y) \in K^2 \mid R(x,y) = 0\}$.
Le polynôme $R$ qui convient vaut :
$$R := \mathrm{Res}_T(F(T) - X,\ G(T) - Y) \in K[X,Y].$$

**Ex 37:**
Cherchons une équation implicite de :
$$\mathcal{C} := \{(x,y) \in \mathbb{C}^2 \mid \exists t \in \mathbb{C},\ x = t^2 + 1,\ y = t^2 - 1\},$$
On obtient :
$$\mathcal{C} := \{(x,y) \in \mathbb{C}^2 \mid x^2 - 2xy + y^2 - 4x + 4y + 4 = 0\}.$$

Annexe :