Chapitre 6 - Partie 1

I Définition du résultant et du discriminant.

A anneau (commutatif, unitaire). Soit $P, Q \in A[X] \setminus \{0\}$. On note $m = \deg P$, $n = \deg Q$.
On suppose $(m,n) \neq (0,0)$.

Base anticanonique de $A[X]_{<n}$: $(X^{n-1}, X^{n-2}, \dots, X, 1)$.

Notation : $\varphi_{P,Q} : A[X]_{<n} \times A[X]_{<m} \longrightarrow A[X]_{<m+n}$
$(U, V) \longmapsto UP + VQ$

Notation : $Syl(P,Q)$ | transposée de la matrice de $\varphi_{P,Q}$ dans les bases anticanoniques "Matrice de Sylvester"

Base de départ : $\big((X^{n-1}, 0), \dots, (X, 0), (1, 0), (0, X^{m-1}), \dots, (0, X), (0, 1)\big)$.

Déf : Le résultant de P et Q est le déterminant de $Syl(P,Q) \in \mathcal{M}_{m+n}(A)$.
On le note $Res(P,Q)$. C'est un élément de A.

⚠ on suppose $\deg P = m$ et $\deg Q = n$ (PAS SEULEMENT $\leq$).

Notons $P(X) = v_m X^m + \dots + v_1 X + v_0$ et $Q(X) = w_n X^n + \dots + w_1 X + w_0$ avec $v_m, w_n \neq 0$. (2)

$$Syl(P,Q) = \begin{bmatrix} v_m & v_{m-1} & \cdots & v_0 & 0 & 0 & \cdots & 0 \\ 0 & v_m & v_{m-1} & \cdots & v_1 & v_0 & 0 & \cdots \\ & \ddots & & \ddots & & & \ddots & \\ & & & & & & & v_0 \\ w_n & w_{n-1} & \cdots & & & & & \\ 0 & w_n & w_{n-1} & \cdots & & & & \\ & \ddots & & \ddots & & & \ddots & \\ & & & & & & & w_0 \end{bmatrix} \begin{matrix} \} n \\ \\ \\ \\ \} m \\ \\ \\ \end{matrix}$$

Déf : Soit $P \in A[X]$ de degré $m \geq 1$ tel que $P' \neq 0$. Notons v_m son coefficient dominant. Alors on pose : $\mathrm{Disc}(P) = \frac{1}{v_m}(-1)^{m(m-1)/2} \mathrm{Res}(P,P')$. Si $\deg P' = m-1$ alors $\mathrm{Disc}(P) \in A$. $\mathrm{Disc}(P)$ s'appelle le discriminant de P.

Preuve : les coeff. dominants de P et P' sont v_m et $(\deg P) v_m$. Notons $Syl'(P,P')$ la matrice obtenue à partir de $Syl(P,P')$ en remplaçant dans la 1ère colonne v_m par 1 et $(\deg P) v_m = w_n$ par $\deg P$. Alors $\mathrm{Disc}(P) := (-1)^{m(m-1)/2} \det Syl'(P,P') \in A$.

Ex : calculer $\mathrm{Disc}(aX^2 + bX + c)$ pour $a, b, c \in A$, $a \neq 0$.

Chapitre 6 - Partie 2

$P(X) = aX^2 + bX + c$, $a, b, c \in A$, $a \neq 0$; $P'(X) = 2aX + b$; $m = 2$, $n = 1$ en supposant que A soit de caractéristique $\neq 2$.

$$\det Syl(P, P') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = ab^2 - 2a(b^2 - 2ac) = -a(b^2 - 4ac) \text{ donc } Disc(P) = b^2 - 4ac.$$

II Interprétation de la (non-) nullité du résultant.

A anneau, $P, Q \in A[X] \setminus \{0\}$, $m = \deg P$, $n = \deg Q$; $(m, n) \neq (0, 0)$.

Prop : Il existe $U \in A[X]_{<n}$ et $V \in A[X]_{<m}$ tels que $UP + VQ = Res(P, Q)$.

NB : si A est un corps et $Res(P, Q) \neq 0$ on peut diviser par $Res(P, Q)$: on obtient $P \wedge Q = 1$.

Preuve : Notons M la transposée de la comatrice de ${}^t Syl(P, Q)$.

Alors : ${}^t Syl(P, Q) \cdot M = Res(P, Q)\, I_{m+n}$ donc en notant W la dernière colonne de M on a : ${}^t Syl(P, Q) \cdot W = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ Res(P, Q) \end{bmatrix}$. Or ${}^t Syl(P, Q) = \underset{\text{antican.}}{Mat}\, \varphi_{P,Q}$ d'où

$$\varphi_{P,Q}(U, V) = UP + VQ = Res(P, Q).$$

Th : Supposons que $A = k$ est un corps. Alors les propriétés suivantes sont équivalents:

(i) $\mathrm{Res}(P,Q) \neq 0$.

(ii) $\forall R \in k[X]_{<m+n}$ $\exists U \in k[X]_{<n}$ $\exists V \in k[X]_{<m}$ $UP + VQ = R$.

(iii) $\exists U \in k[X]_{<n}$ $\exists V \in k[X]_{<m}$ $UP + VQ = 1$

(iv) P et Q sont premiers entre eux.

En outre si $\mathbb{E}$ est une extension de k sur laquelle P ou Q est scindé alors ces propriétés sont équivalentes à :

(v) P et Q n'ont aucune racine commune dans $\mathbb{E}$.

Preuve : (i) $\Leftrightarrow$ $\varphi_{P,Q}$ bijective $\Leftrightarrow$ $\varphi_{P,Q}$ surjective $\Leftrightarrow$ (ii) ; on a (ii) $\Rightarrow$ (iii) et (iii) $\Rightarrow$ (iv).

Montrons (iv) $\Rightarrow$ (ii). Soit $R \in k[X]_{<m+n}$. Il existe $U_0, V_0 \in k[X]$ tels que $U_0 P + V_0 Q = 1$. Alors $(RU_0)P + (RV_0)Q = R$. Notons $RU_0 = SQ + U$ la division euclidienne de RU_0 par Q ; alors $U \in k[X]_{<n}$. On a $\underline{SQP} + UP + \underline{RV_0 Q} = R$ d'où $UP + VQ = R$ en posant $V = SP + RV_0$. On a $\deg(VQ) = \deg(R - UP) < m+n$ d'où $V \in k[X]_{<m}$.

(iv) $\Leftrightarrow$ (v) $\mathrm{pgcd}(P,Q)$ calculé dans $k[X]$ est le même que celui calculé dans $\mathbb{E}[X]$. Dans $\mathbb{E}$: P et Q premiers entre eux $\Leftrightarrow$ P et Q n'ont aucune racine commune.

NB : Pour $P, Q \in k[X]$ avec k sous-corps de $\mathbb{C}$:

$\mathrm{Res}(P,Q) \neq 0 \iff$ P et Q ont une racine commune dans $\mathbb{C}$.

III Spécialisation

1.) La propriété de spécialisation et ses applications.

Prop : Soit $\varphi : A \to B$ un homomorphisme d'anneaux, et $P, Q \in A[X] \setminus \{0\}$.
On note P^φ et Q^φ les polynômes obtenus à partir de P et Q en appliquant φ aux coefficients.
Si $\deg P^\varphi = \deg P$ et $\deg Q^\varphi = \deg Q$ alors $\mathrm{Res}(P^\varphi, Q^\varphi) = \varphi(\mathrm{Res}(P,Q))$.

Preuve : $\mathrm{Syl}(P^\varphi, Q^\varphi) = \varphi(\mathrm{Syl}(P,Q))$ car $\deg P^\varphi = \deg P$ et $\deg Q^\varphi = \deg Q$.

Ex : k corps, $A = k[Y]$, $B = k$, $\varphi : \begin{array}{ccc} k[Y] & \to & k \\ S & \mapsto & S(y_0) \end{array}$ évaluation en $y_0 \in k$.
Ici $P, Q \in k[Y][X] = k[X,Y]$ et $P^\varphi = P(X, y_0) \in k[X]$. Or $\mathrm{Res}(P,Q) \in k[Y]$, et
$\varphi(\mathrm{Res}(P,Q)) = (\mathrm{Res}(P,Q))(y_0)$.

Prop : Soient p un nombre premier et $P, Q \in \mathbb{Z}[X] \setminus \{0\}$. Supposons que p ne divise ni le coefficient dominant de P ni celui de Q. Alors : $\overline{\mathrm{Res}(P,Q)} = \mathrm{Res}(\overline{P}, \overline{Q}) \in \mathbb{Z}/p\mathbb{Z}$ ($\overline{P}, \overline{Q} \in (\mathbb{Z}/p\mathbb{Z})[X]$).
En particulier : $p \mid \underbrace{\mathrm{Res}(P,Q)}_{\in \mathbb{Z}} \iff \overline{\mathrm{Res}(P,Q)} = 0$
$\iff \mathrm{Res}(\overline{P}, \overline{Q}) = 0 \iff \overline{P}$ et $\overline{Q}$ ne sont pas premiers entre eux dans $\mathbb{F}_p[X]$.

Preuve : $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Prop : Soient k un corps et $P \in k[X]$ tel que $P' \neq 0$. Alors : P séparable $\iff \mathrm{Res}(P,P') \neq 0$
$\iff \mathrm{Disc}(P) \neq 0$.

Prop : Soit $P \in \mathbb{Z}[X]$ non constant, et p un nombre premier. On suppose que p ne divise pas le coefficient dominant de P. Alors : $p \mid \mathrm{Disc}(P) \iff \overline{P} \in \mathbb{F}_p[X]$ n'est pas séparable.

2°) Un raffinement.

Prop : Soit $\varphi : A \to b$ un hom. d'anneaux, et $P, Q \in A[X] \setminus \{0\}$. Supposons $\deg P^\varphi = \deg_{\mathbb{Q}} P$ et notons v_m le coeff. dominant de P. Alors :

$$\varphi(\mathrm{Res}(P,Q)) = \begin{cases} 0 & \text{si } Q^\varphi = 0 \text{ et } \deg P \geq 1 \\ \varphi(v_m)^n & \text{si } Q^\varphi = 0 \text{ et } \deg P = 0 \\ \varphi(v_m)^{n-\deg(Q^\varphi)} \mathrm{Res}(P^\varphi, Q^\varphi) & \text{si } Q^\varphi \neq 0. \end{cases}$$

Corollaire : Si on note A intègre et $Q^\varphi \neq 0$, alors :
$\varphi(\mathrm{Res}(P,Q)) = 0 \iff \mathrm{Res}(P^\varphi, Q^\varphi) = 0$.

Preuve : $\varphi(\mathrm{Syl}(P,Q))$ a sa dernière ligne nulle si $Q^\varphi = 0$ et $\deg P \geq 1$. On a $\varphi(\mathrm{Res}(P,Q)) = \det(\varphi(\mathrm{Syl}(P,Q)))$.

Si $Q^\varphi \neq 0$: les $n - \deg Q^\varphi$ premières colonnes de $\varphi(\mathrm{Syl}(P,Q))$ ont chacune $\varphi(v_m)$ comme coefficient diagonal, et des zéros en-dessous. On développe $\det(\varphi(\mathrm{Syl}(P,Q)))$ par rapport à ces colonnes.

Corollaire : Soient p premier et $P, Q \in \mathbb{Z}[X] \setminus \{0\}$. Supposons que p ne divise pas à la fois le coeff. dominant de P et celui de Q. Alors : $p \mid \mathrm{Res}(P,Q) \iff \mathrm{Res}(\overline{P}, \overline{Q}) = 0$
$\iff \overline{P}$ et $\overline{Q}$ ne sont pas premiers entre eux dans $\mathbb{F}_p[X]$.

Chapitre 6 - Partie 4

III bis. Formules.

Soient A un anneau (commutatif, unitaire), $P, Q \in A[X] \setminus \{0\}$, $m = \deg P$, $n = \deg Q$, $(m,n) \neq (0,0)$.

Prop : $\mathrm{Res}(Q,P) = (-1)^{mn}\,\mathrm{Res}(P,Q)$.

Th : Si $P(X) = \lambda \prod_{i=1}^{m}(X-a_i)$ et $Q(X) = \mu \prod_{j=1}^{n}(X-b_j)$ avec $a_i, b_j \in A$ alors :

$$\begin{aligned}\mathrm{Res}(P,Q) &= \lambda^n \mu^m \prod_{i,j}(a_i - b_j)\\ &= \lambda^n \prod_{i=1}^{m} Q(a_i)\\ &= (-1)^{mn} \mu^m \prod_{j=1}^{n} P(b_j).\end{aligned}$$

Cor : Si $\deg P' = \deg P - 1 = m-1$ alors $\mathrm{Disc}(P) = \lambda^{2(m-1)} \prod_{1 \le i < j \le m} (a_i - a_j)^2$.

NB : $P(X) = aX^2 + bX + c$, $a_1 = \dfrac{-b \pm \sqrt{\Delta}}{2a}$, $(a_1 - a_2)^2 = \left(\dfrac{-2\sqrt{\Delta}}{2a}\right)^2 = \dfrac{4\Delta}{4a^2} = \dfrac{\Delta}{a^2}$ et $\lambda = a$.

IV Calcul efficace du résultant.

Prop : Supposons $m \geq n \geq 1$ et $S \in A[X]_{\leq m-n}$ est tel que $P + SQ \neq 0$. Notons $r = \deg(P+SQ)$.

Alors $\mathrm{Res}(P,Q) = (-1)^{(m-r)n}\, w_n^{m-r}\, \mathrm{Res}(P+SQ, Q)$ où w_n est le coeff. dominant de Q.

Th : On peut calculer $\mathrm{Res}(P,Q)$ en $O(mn)$ opérations arithmétiques dans k, si $A=k$ est un corps. (avec $m=\deg P$, $n=\deg Q$).

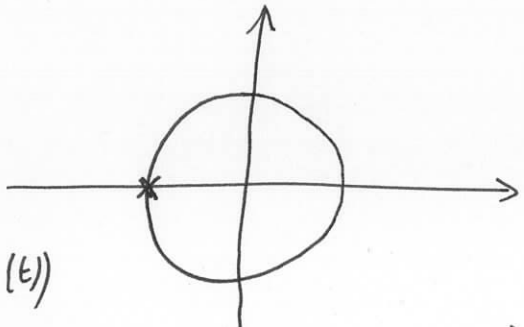
Preuve : Mener à bien l'algorithme d'Euclide pour le calcul de $\mathrm{pgcd}(P,Q)$.

V Applications géométriques du résultant.

1) Equation cartésienne d'une courbe paramétrée

$$\begin{cases} x(t) = \dfrac{1-t^2}{1+t^2} \\ y(t) = \dfrac{2t}{1+t^2} \end{cases} \qquad t \in \mathbb{C} \setminus \{\pm i\}$$

$\mathcal{C}$ ensemble des points de la forme $(x(t), y(t))$



Soit $(x,y) \in \mathbb{C}^2$. On a $(x,y) \in \mathcal{C} \iff \exists t \in \mathbb{C}$ (ou $\mathbb{C}\setminus\{\pm i\}$) $(1+t^2)x = 1-t^2$ et $(1+t^2)y = 2t$

$$P_{x,y}(T) = (x+1)T^2 + x - 1 \in \mathbb{C}[T]$$
$$Q_{x,y}(T) = yT^2 - 2T + y \in \mathbb{C}[T]$$

$\iff \exists t \in \mathbb{C} \quad P_{x,y}(t) = Q_{x,y}(t) = 0$

(car $\mathbb{C}$ est alg. clos) $\iff \mathrm{Res}(P_{x,y}, Q_{x,y}) = 0$

(si $x \neq -1$ et $y \neq 0$) $\iff 4(x^2+y^2-1) = 0$

2) Intersection de deux courbes planes.

$\mathcal{C} = \{(x,y) \in \mathbb{C}^2,\ P(x,y) = 0 \text{ et } Q(x,y) = 0\}$.

avec $P, Q \in \mathbb{C}[X,Y]$ fixés.

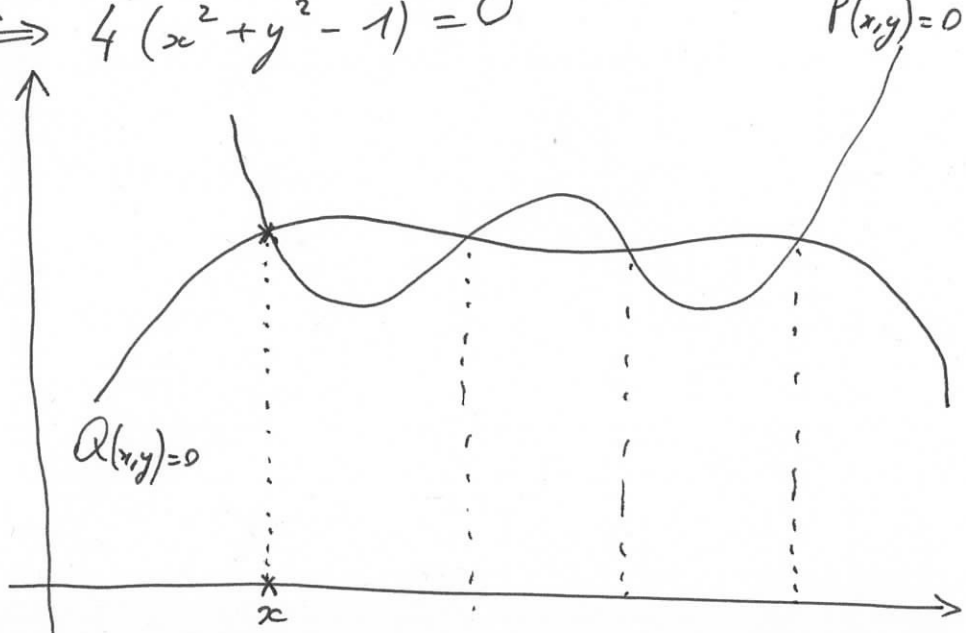
Soit $(x,y) \in \mathcal{C}$. Que dire de x ?

$\exists y \in \mathbb{C} \quad P(x,y) = Q(x,y) = 0$

donc $P(x,Y)$ et $Q(x,Y)$ ont une racine commune.

Donc $\mathrm{Res}(P(x,Y), Q(x,Y)) = 0$.

↳ équivalence sur $\mathbb{C}$



Spécialisation : racines de $\mathrm{Res}_Y(P(X,Y), Q(X,Y)) \in \mathbb{C}[X]$: on voit $P, Q \in (\mathbb{C}[X])[Y]$