Version faible du th de Bézout

Leçons : 142, 144, 152, 191.

Énoncés :
- Lemme : A factoriel, $K = \mathrm{Frac}\, A$, $P, Q \in A[X]$. Les pgcd de P et Q sur A et sur K sont associés dans $K[X]$.
- Th : Soient k un corps infini et $P, Q \in K[X,Y]$ non nuls tq $P \wedge Q = 1$. On note $d_1 = \deg P$, $d_2 = \deg Q$, $V(F) = \{(x,y) \in k^2 \mid F(x,y) = 0\}$ pour $F \in K[X,Y]$. Alors $V(P) \cap V(Q)$ est fini, de cardinal $\leq d_1 d_2$.

⊛ Lemme.

On note $P \underset{A}{\wedge} Q$ et $P \underset{K}{\wedge} Q$ les deux pgcd. Puisqu'une division dans $A[X]$ est une division dans $K[X]$, $P \underset{A}{\wedge} Q \mid P \underset{K}{\wedge} Q$ sur K. Réciproquement notons $D = P \underset{K}{\wedge} Q$. Il existe $a \in A \setminus \{0\}$ tq $aD \in A[X]$. Sur K, aD divise P et Q ; en multipliant les deux égalités par un certain $b \in A \setminus \{0\}$ pour les ramener sur A, on obtient que sur A, aD divise bP et bQ. Alors toujours sur A, aD divise $(bP) \underset{A}{\wedge} (bQ) = b(P \underset{A}{\wedge} Q)$. Donc $D \mid P \underset{A}{\wedge} Q$ sur K. □

⊛ Th.

- Notons $m = \deg_Y P \leq d_1$ et $n = \deg_Y Q \leq d_2$. Si $m = n = 0$, $P, Q \in K[X]$ et y sont premiers entre eux (car $K[X] \subset K[X,Y]$). Ils n'ont donc pas de racine commune, et $V(P) \cap V(Q) = (\mathrm{Roc}\, P \cap \mathrm{Roc}\, Q) \times K = \emptyset$ est de cardinal 0. On peut donc sq $m \geq 1$ ou $n \geq 1$.

  Le résultant en Y de P et Q, $R = \mathrm{Res}_Y(P,Q) \in K[X]$, est alors défini. De plus P et Q sont premiers entre eux dans $K[X,Y]$ donc dans $K(X)[Y]$ d'après le lemme, d'où $R \neq 0$.

- Mq $\deg R \leq d_1 d_2$.

  On écrit $P = \sum_{k=0}^{m} a_k Y^k$ et $Q = \sum_{k=0}^{n} b_k Y^k$ avec $a_k, b_k \in K[X]$ tq $\deg a_k \leq d_1 - k$, $\deg b_k \leq d_2 - k$.

  La matrice de Sylvester en Y de P et Q est alors

$$S = \mathrm{Syl}_Y(P,Q) = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & \\ & \ddots & & & \ddots & \ddots & \\ & & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \ddots & \\ & & b_n & b_{n-1} & \cdots & b_1 & b_0 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \end{matrix} \in M_{n+m}(K[X]).$$

  Si $1 \leq i \leq n$ et $i \leq j \leq m+i$, $S_{i,j} = a_{m+i-j}$ est de degré $\leq d_1 - m + j - i$.
  Si $n+1 \leq i \leq n+m$ et $i-n \leq j \leq i$, $S_{i,j} = b_{i-j}$ est de degré $\leq d_2 + j - i$.
  Autrement $S_{i,j} = 0$.

On a $R = \det S = \sum_{\sigma \in \mathfrak{S}_{m+n}} \varepsilon(\sigma) \prod_{i=1}^{m+n} S_{i,\sigma(i)}$. Fixons $\sigma \in \mathfrak{S}_{m+n}$: $\deg\left(\varepsilon(\sigma) \prod_{i=1}^{m+n} S_{i,\sigma(i)}\right)$

$= \sum_{i=1}^{n} \deg S_{i,\sigma(i)} + \sum_{i=m+1}^{n+m} \deg S_{i,\sigma(i)} \leq \sum_{i=1}^{n} (d_1 - m + \sigma(i) - i) + \sum_{i=m+1}^{n+m} (d_2 + \sigma(i) - i)$

$\leq \sum_{i=1}^{m+n} (\sigma(i) - i) + n(d_1 - m) + m d_2 = n(d_1 - m) + m d_2$ car $\sigma \in \mathfrak{S}_{m+n}$. Comparons :

$n(d_1 - m) + m d_2 - d_1 d_2 = n(d_1 - m) + (m - d_1) d_2 = (n - d_2)(d_1 - m) \leq 0$ car $\begin{cases} n - d_2 \leq 0 \\ d_1 - m \geq 0 \end{cases}$.

On en déduit que $\deg R \leq d_1 d_2$.

- Vérifions enfin que si $(x,y) \in V(P) \cap V(Q)$, $R(x) = 0$.

  On a $R(x) = \det(S(x))$. Notons $m' = \deg P(x,Y)$ et $n' = \deg Q(x,Y)$.
  Si $\begin{cases} m' < m \\ n' < n \end{cases}$, la première colonne de S_x est nulle et $R(x) = 0$. Sinon quitte à échanger
  P et Q on peut sq $m' = m$. Nécessairement, $m \geq 1$ (sinon $P \in K[X]$ et $P(x) = 0$, ce qui donne
  $m' = -\infty < m$: absurde). Si $Q(x,Y) = 0$, la dernière ligne de $S(x)$ est alors nulle,
  et $R(x) = 0$. Sinon par spécialisation on a $R(x) = a_m(x)^{n-n'} \cdot \mathrm{Res}(P(x,Y), Q(x,Y))$.
  Mais y est racine de $P(x,Y)$ et $Q(x,Y) \in K[Y]$ donc leur résultant est nul ; là encore,
  $R(x) = 0$. (De même $\mathrm{Res}_X(P,Q)(y) = 0$, ce dont on déduit $V(P) \cap V(Q)$ fini.)

- On écrit $V(P) \cap V(Q) = \{(x_1,y_1), \dots, (x_r,y_r)\}$ 2à2 $\neq$. Si $i \neq j$ implique $x_i \neq x_j$, on déduit du point précédent $r \leq \deg R \leq d_1 d_2$. Lorsque ce n'est pas le cas, on s'y ramène.
  Soient $i \neq j$ et $t \in K$: $x_i + t y_i = x_j + t y_j \Leftrightarrow x_i - x_j = t(y_j - y_i) \Leftrightarrow \left(y_i \neq y_j \text{ et } t = \frac{x_i - x_j}{y_j - y_i}\right)$ (en effet si $y_i = y_j$ on en tire $x_i = x_j$, et c'est impossible comme $i \neq j$).
  K étant infini, il est possible de fixer un $t \notin \left\{ \frac{x_i - x_j}{y_j - y_i} \,;\, y_i \neq y_j \right\}$.
  On considère alors l'automorphisme $\sim$ de la K-algèbre $K[X,Y]$ défini par $\begin{cases} \tilde{X} = X - tY \\ \tilde{Y} = Y \end{cases}$.
  Alors $\tilde{P}$ et $\tilde{Q}$ vérifient les hypothèses et $\deg \tilde{P} = d_1$, $\deg \tilde{Q} = d_2$. De plus
  $\begin{cases} V(P) \cap V(Q) \longrightarrow V(\tilde{P}) \cap V(\tilde{Q}) \\ (x,y) \longmapsto (x + ty, y) \end{cases}$ est une bijection. Par choix de t, les points de $V(\tilde{P}) \cap V(\tilde{Q})$
  ont des premières coordonnées 2à2 $\neq$, et ce qui précède s'applique : $r \leq d_1 d_2$. □

Complément 1 : Détails du dernier point.

- L'endomorphisme de K-algèbre $\tilde{\cdot}$ est bijectif car sa bij réciproque est l'endomorphisme de K-algèbre $\hat{\cdot}$ de $K[X,Y]$ déf par $\begin{cases} \hat{X} = X + tY \\ \hat{Y} = Y \end{cases}$.

- Vérifions que $\tilde{P}, \tilde{Q}$ vérifient les hyp du th. Il est évident qu'ils sont non nuls. Ensuite $\tilde{P} \wedge \tilde{Q} = \widetilde{P \wedge Q} = \tilde{1} = 1$.

- Mq si $F \in K[X,Y]$, $\deg \tilde{F} = \deg F$. On écrit $F = \sum_{i,j} c_{i,j} X^i Y^j$, $c_{i,j} \in K$. Alors $\tilde{F} = \sum_{i,j} c_{i,j} (X - tY)^i Y^j = \sum_{i,j} \sum_{k=0}^{i} c_{i,j} \binom{i}{k} (-t)^{i-k} X^k Y^{i+j-k}$ et $k + (i+j-k) = i+j$: $\deg \tilde{F} \leq \deg F$. De même $\deg F = \deg \hat{\tilde{F}} \leq \deg \tilde{F}$, d'où l'égalité.

- Notons φ la bij donnée de $V(P) \cap V(Q)$ dans $V(\tilde{P}) \cap V(\tilde{Q})$. Elle est bien déf car si $F \in K[X,Y]$ et $(x,y) \in K^2$, $\tilde{F}(x+ty, y) = F((x+ty) - ty, y) = F(x,y)$. Elle est bijective car $(x,y) \mapsto (x - ty, y)$ est sa bijection réciproque. □

Complément 2 : Propriétés du résultant utilisées ici. On note $m = \deg P$, $n = \deg Q$.

(i) Sur K un corps, $P \wedge Q = 1 \Leftrightarrow \mathrm{Res}(P,Q) \neq 0$.

(ii) Spécialisation : $\varphi : A \to B$ un morphisme d'anneaux (commutatifs) que l'on étend de $A[X]$ sur $B[X]$, $P, Q \in A[X]$ tq $\begin{cases} \deg \varphi(P) = \deg P \\ \varphi(a) \neq 0 \end{cases}$. On a $\varphi(\mathrm{Res}(P,Q)) = \varphi(a)^{n-n'} \cdot \mathrm{Res}(\varphi(P), \varphi(Q))$ avec $a \in A$ le coef dominant de P et $n' = \deg \varphi(Q)$.

Preuve.

(i) : rappel : $\mathrm{Syl}(P,Q)$ est déf comme la transposée de la matrice de l'appli K-linéaire $\beta_{P,Q} : \begin{cases} K[X]_{<n} \times K[X]_{<m} \to K[X]_{<m+n} \\ (U,V) \mapsto UP + VQ \end{cases}$ dans les bases anti-canoniques. Ainsi $\mathrm{Res}(P,Q) \neq 0 \Leftrightarrow \beta_{P,Q}$ surjective. Si $\beta_{P,Q}$ est surjective, on peut écrire $UP + VQ = 1$, d'où $P \wedge Q = 1$. Réciproquement si $P \wedge Q = 1$ et soit $S \in K[X]_{<m+n}$: on peut écrire $UP + VQ = S$ avec $U, V \in K[X]$. On fait la DE de U par Q : $U = TQ + U'$, $\deg U' < n$. On pose aussi $V' = V + TP$. Alors $U'P + V'Q = (U - TQ)P + (V + TP)Q = UP + VQ = S$. De plus $V'Q = S - U'P$ est, comme S et $U'P$, de deg $< m+n$; donc $\deg V' < m$. On a bien $S = \beta_{P,Q}(U', V')$.

(ii) : Les $n - n'$ premières colonnes de $\varphi(\mathrm{Syl}(P,Q))$ ont $\varphi(a)$ sur la diagonale et sont nulles en dessous : le déterminant est $\varphi(a)^{n-n'}$ multiplié par le déterminant du bloc de taille $m+n'$ en bas à droite ; or ce bloc est $\mathrm{Syl}(\varphi(P), \varphi(Q))$, d'où la formule. □

Réf :

- Sauve Picard – Cours de calcul formel : ↑ 157 (énoncé + indications), ↑ 143 (résultant).
- Perrin-Riou – Algèbre, arithmétique et Maple : ↑ 94 (résultant).
- Mignotte – Mathématiques pour le calcul formel : ↑ 126 (résultant).
- Isenmann, Pécatte : ↑ 46 (th avec preuve).

↳ Pas de réf dans la BA officielle (Trennenn, Perdu et Sauve Picart n'y sont pas) pour le th.
Les propriétés du résultant sont dans Sauve Picart ; elles sont aussi partiellement dans Trennenn, Perdu et les deux autres réfs (qui elles sont dans la BA officielle).

↳ Inclure le lemme : trop long : pour 144, 152, 191, faire uniquement le th. Pour 142 le lemme est important : le faire, et ± zapper le 2e point de la preuve ($\deg R \leq d_1 d_2$).

↳ Ici par degré on entend, lorsque $F = \sum_{i,j} c_{i,j} X^i Y^j$, $\deg F = \max_{c_{i,j} \neq 0} (i+j)$.

↳ Dans le dernier point de la preuve il manque qq détails faciles. Ils sont précisés dans le complément 1.

↳ Les propriétés du résultant que l'on utilise sont prouvées dans le complément 2. Attention la première n'est plus vraie si on remplace K par A (on utilise le th de en et la principalité de $K[X]$). Elle peut aussi se déduire de la formule qui relie le résultant à l'algo d'Euclide (elle aussi utilise le fait que K est un corps), comme le fait Sauve Picart.

↳ Le "vrai" th de Bézout affirme que si K est algébriquement clos, alors le nb de points d'intersection de $V(P)$ et $V(Q)$, comptés avec multiplicité et en tenant compte des points "à l'infini" (plan projectif), est égal à $d_1 d_2$.