PGCD avec la matrice de Sylvester

Théorème: Soient $A, B \in \mathbb{K}[X]$ avec $\mathbb{K}$ un corps. On pose $n := \deg A$ et $m := \deg B$ et :

$$\varphi_{n,m} : \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] \longrightarrow \mathbb{K}_{n+m-1}[X]$$
$$(U, V) \longmapsto AU + BV$$

Alors $\mathrm{Im}\, \varphi_{n,m} = \langle D \rangle \cap \mathbb{K}_{n+m-1}[X]$ avec $D = \mathrm{pgcd}(A, B)$

Preuve: Posons $\varphi : \mathbb{K}[X]^2 \longrightarrow \mathbb{K}[X]$, $(U,V) \longmapsto AU+BV$. Alors, par caractérisation du pgcd dans un anneau principal, $\mathrm{Im}\, \varphi = \langle D \rangle$. On veut mq. $\mathrm{Im}\, \varphi_{n,m} = \langle D \rangle \cap \mathbb{K}_{n+m-1}[X] := \langle D \rangle_{n+m-1}$

On montre $\subseteq$.

Soit $P \in \mathrm{Im}\, \varphi_{n,m}$, alors $\exists (U,V) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$ tq.

$$P = AU + BV$$

Or, $D | A$ et $D | B$ donc $D | P$ et $P \in \langle D \rangle \cap \mathbb{K}_{n+m-1}[X]$.

On montre l'égalité des dimensions ($\mathrm{Im}\, \varphi_{n,m}$ et $\langle D \rangle_{n+m-1}$ sont des e.v)

$\dim \langle D \rangle_{n+m-1}$:

Notons $\delta := \deg D$. Mq. $\mathcal{B} = (D, XD, \dots, X^{n+m-1-\delta} D)$ est une base de $\langle D \rangle_{n+m-1}$:
La famille est libre car elle est échelonnée en degré, et elle est génératrice car si $P \in \langle D \rangle_{n+m-1}$, $\exists Q \in \mathbb{K}_{n+m-1}[X]$ tq. $P = QD$. Or,

$$Q = \sum_{k=0}^{n+m-1-\delta} q_k X^k, \ q_k \in \mathbb{K}$$

Donc,

$$P = \sum_{k=0}^{n+m-1-\delta} q_k X^k D \in \mathrm{Vect}(\mathcal{B})$$

Donc $\boxed{\dim \langle D \rangle_{n+m-1} = n+m-\delta.}$

$\dim \mathrm{Im}\, \varphi_{n,m}$:

On utilise le thm du rang : $\ker \varphi_{n,m} = \ker \varphi \cap (\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X])$.
On écrit : $A = A'D$ et $B = B'D$, $A' \wedge B' = 1$. Alors, on mq.

$$\ker \varphi = \{ (HB', -HA'), H \in \mathbb{K}[X] \} \qquad (1)$$

On a, pour $(U,V) \in \ker \varphi$: $AU + BV = 0 \iff A'U = -B'V$ ($\mathbb{K}[X]$ intègre). Donc par le lemme de Gauss, $A' | V$ donc $\exists H \in \mathbb{K}[X]$ tq. $V = HA'$ alors $A'U = -B'HA'$ donc $U = -B'H$. D'où l'inclusion directe dans (1). La réciproque est un simple calcul.

On va en déduire que $\ker \varphi_{n,m} = \{ (HB', -HA'), H \in \mathbb{K}_{\delta-1}[X] \}$. A nouveau $\supseteq$ est facile. Ensuite, si $(HB', -HA') \in \ker \varphi_{n,m}$ avec $H \in \mathbb{K}[X]$ (on sait que les éléments du noyau ont cette forme car $\ker \varphi_{n,m} \subseteq \ker \varphi$). Alors $\deg H + \deg B' \leq m-1$ et $\deg H + \deg A' \leq n-1$. Or, $\deg B' = m - \delta$ et $\deg A' = n - \delta$ par construction. Donc, $\deg H \leq \delta - 1$. Donc $H \in \mathbb{K}_{\delta-1}[X]$.
Donc, $\dim \mathrm{Im}\, \varphi_{n,m} = n+m - \dim \ker \varphi_{n,m} = n+m-\delta$. On a bien égalité des dimensions donc, $\mathrm{Im}\, \varphi_{n,m} = \langle D \rangle_{n+m-1}$.

Application : En échelonnant la matrice de Sylvester par rapport aux colonnes on obtient une matrice de la forme : (on note $k := n+m-\delta$)

$$\begin{array}{c} \left[\begin{array}{c|c|c|c|c|c} 0 & 0 & & & & \\ \vdots & \vdots & P_1 & P_2 & \cdots & P_k \\ 0 & 0 & & & & \end{array}\right] \end{array} \begin{array}{l} 1 \\ X \\ \vdots \\ X^{n+m-1} \end{array}$$

NB : En échelonnant par rapport aux colonnes, on change la base de départ, pas la base d'arrivée. On a $\delta \leq \deg P_1 < \dots < \deg P_k \leq n+m-1 = k-1+\delta$

On a donc k polynômes de degré tous différent et k degré possible. Donc, par le principe des tiroirs, $\deg P_1 = \delta$, donc P_1 est un pgcd de A et de B.

Corollaire : $\mathrm{res}(A,B) \neq 0 \iff A \wedge B = 1$.

Remarques :

▷ Un développement très inhabituel, fait maison avec un prof. Très intéressant, mais très dangereux : résultant, matrice de Sylvester sont des notions hors programme bien qu'accessibles, très riches et intéressantes

▷ Niveau temps, il ne faut pas traîner sur le caractère générateur de la base de $\langle D\rangle_{n+m-1}$, mais sinon ça va. Je ne parlais pas du tout du corollaire, qui peut en plus se montrer d'une autre manière, beaucoup plus efficace.

▷ Le but est de montrer pourquoi on trouve un pgcd de A et B en échelonnant la matrice de Sylvester. Attention au passage à la déf de la matrice de Sylvester que vous choisissez : étant donnée ma définition, il fallait que j'échelonne en colonne, mais si votre matrice de Sylvester est la transposée, il faudra échelonner en ligne.

▷ Notez que bien qu'évident à première vue, le thm donne un résultat assez remarquable : si on n'impose pas de degré à nos polynômes de départ et d'arrivée dans la fonction φ, le résultat est clair, $\mathrm{Im}\,\varphi = \langle D\rangle$. Le thm nous dit que si on restreint les degrés, on ne perdra que les polynômes de degré trop haut, mais aucun polynôme de degré $\leq n+m-1$. Et c'est pas évident ! D'où l'utilité de la preuve.

▷ Petit ~~thm des~~ principes des tiroirs de derrière les fagots pour finir le dev, ça fait toujours sourire :)