Borne de Bézout

2013 – 2014

Théorème.
Soit k un corps infini et $P, Q \in k[X,Y]$ deux polynômes de degrés totaux respectifs d et d'. On suppose que P et Q sont premiers entre eux. Alors $|V(P) \cap V(Q)| \leq dd'$, avec $V(P) := \{(x,y) \in k^2 \mid P(x,y) = 0\}$.

Démonstration. Définissons $R(X) := \mathrm{Res}_Y(P,Q)$ et $S(Y) := \mathrm{Res}_X(P,Q)$. Montrons d'abord que $|V(P) \cap V(Q)| < +\infty$.

Si $(\alpha, \beta) \in V(P) \cap V(Q)$, alors $R(\alpha) = 0$ et $S(\beta) = 0$. Or P et Q sont premiers entre eux donc les polynômes R et S sont non nuls. On en déduit $|V(P) \cap V(Q)| \leq \deg(R)\deg(S)$.

Montrons que $\deg(R) \leq dd'$. On commence par écrire

$$P(X,Y) = \sum_{k=0}^{p} P_k(X) Y^{p-k} \quad \text{et} \quad Q(X,Y) = \sum_{k=0}^{q} Q_k(X) Y^{q-k}$$

avec p et q les degrés en Y respectifs de P et Q. On a

$$\begin{cases} \deg P_k \leq d - p + k, & 0 \leq k \leq p \\ \deg Q_k \leq d' - q + k, & 0 \leq k \leq q. \end{cases}$$

Notons M la matrice de Sylvester de P et Q comme polynômes en Y, on a

$$M = \begin{pmatrix} P_0 & \cdots & \cdots & \cdots & \cdots & P_p & 0 & \cdots & 0 \\ 0 & P_0 & \cdots & \cdots & \cdots & \cdots & P_p & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & P_0 & \cdots & \cdots & \cdots & \cdots & P_p \\ Q_0 & \cdots & \cdots & \cdots & Q_q & 0 & \cdots & \cdots & 0 \\ 0 & Q_0 & \cdots & \cdots & \cdots & Q_q & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & Q_0 & \cdots & \cdots & \cdots & Q_q \end{pmatrix}.$$

Pour $1 \leq i \leq q$, on a

$$M_{i,j} = \begin{cases} P_{j-i} & \text{si } 0 \leq j - i \leq p \\ 0 & \text{sinon} \end{cases}$$

donc pour tout $j \in \{1, \dots, p+q\}, \deg(M_{i,j}) \leq d - p + j - i$.

De même, pour $q+1 \leq i \leq p+q$, on a

$$M_{i,j} = \begin{cases} Q_{j-i+q} & \text{si } 0 \leq j - i + q \leq q \\ 0 & \text{sinon} \end{cases}$$

donc pour tout $j \in \{1, \dots, p+q\}, \deg(M_{i,j}) \leq d' - q + j - i + q = d' + j - i$.

On applique alors la formule du déterminant :

$$R = \sum_{\sigma \in \mathfrak{S}_{p+q}} \varepsilon(\sigma) \underbrace{\prod_{i=1}^{q} M_{i,\sigma(i)} \prod_{i=q+1}^{p+q} M_{i,\sigma(i)}}_{R_\sigma}.$$

Or, pour tout $\sigma \in \mathfrak{S}_{p+q}$, on a

$$\begin{aligned} \deg(R_\sigma) &\leq \sum_{i=1}^{q} (d - p + \sigma(i) - i) + \sum_{i=q+1}^{p+q} (d' + \sigma(i) - i) \\ &= q(d-p) + pd' + \underbrace{\sum_{i=1}^{p+q} (\sigma(i) - i)}_{=0} \\ &= q(d-p) + (p-d)d' + dd' \\ &= (q - d')(d-p) + dd' \\ &\leq dd'. \end{aligned}$$

On en déduit que $\deg(R) \leq dd'$ et, par le même raisonnement, $\deg(S) \leq dd'$. Donc $|V(P) \cap V(Q)| \leq (dd')^2$.

Nous allons maintenant affiner cette borne. Notons $(\alpha_1, \beta_1), \dots, (\alpha_r, \beta_r)$ les différents points d'intersection de $V(P)$ et $V(Q)$. Si tous les α_i sont distincts alors, puisque les α_i sont racines de R, $|V(P) \cap V(Q)| = r \leq \deg(R) \leq dd'$. Si ce n'est pas le cas, on va effectuer un changement de variables pour s'y ramener.

Soit $u \in k$ tel que

$$\forall i \neq j \in \{1, \dots, r\}, \quad \alpha_i + u\beta_i \neq \alpha_j + u\beta_j.$$

Un tel u existe car les droites d'équation $y = \alpha_i + x\beta_i$ ont deux à deux au plus un point d'intersection donc il existe un nombre fini de points dans l'intersection de deux droites, et k est infini.

Effectuons alors le changement de variables

$$\begin{cases} X' = X + uY \\ Y' = Y \end{cases}$$

et notons $\tilde{P}(X', Y') = P(X, Y), \tilde{Q}(X', Y') = Q(X, Y)$. On a alors

$$\begin{aligned} (\alpha, \beta) \in V(P) \cap V(Q) &\iff P(\alpha, \beta) = Q(\alpha, \beta) = 0 \\ &\iff \tilde{P}(\alpha + u\beta, \beta) = \tilde{Q}(\alpha + u\beta, \beta) = 0 \\ &\iff (\alpha + u\beta, \beta) \in V(\tilde{P}) \cap V(\tilde{Q}), \end{aligned}$$

d'où $|V(P) \cap V(Q)| = |V(\tilde{P}) \cap V(\tilde{Q})|$.

Soit $(x, y) \in V(\tilde{P}) \cap V(\tilde{Q})$, alors $(x - uy, y) \in V(P) \cap V(Q)$ donc il existe $i \in \{1, \ldots, r\}$ tel que $\alpha_i = x - uy$ et $\beta_i = y$, *i.e.* $x = \alpha_i + u\beta_i$ et $y = \beta_i$. Par définition de u, pour un tel x il y a unicité de i et donc de y. Les abscisses des points d'intersection de $V(\tilde{P})$ et $V(\tilde{Q})$ sont donc distinctes et on a

$$|V(P) \cap V(Q)| = |V(\tilde{P}) \cap V(\tilde{Q})| \leq dd'.$$

$\square$

Références

[1] Philippe Saux Picart, *Cours de calcul formel : Algorithmes fondamentaux*, Ellipses, 1999, page 157 exercice 8.