

Théorème: Soient k un corps infini, puis $P, Q \in k[X, Y]$. On note d le degré total de P et d' le degré total de Q . Alors l'ensemble $V(P) \cap V(Q)$ est de cardinal au plus dd' .

Démonstration:

* On note p le degré de P en Y . On écrit $P(X, Y) = \sum_{k=0}^p P_k(X) Y^{p-k}$,
 $Q(X, Y) = \sum_{k=0}^q Q_k(X) Y^{q-k}$,

avec $\deg P_k \leq d - p + k$. On pose $R(X) = \text{Res}_Y(P(X, Y), Q(X, Y))$.

$\deg Q_k \leq d' - q + k$

On va montrer que le degré de R est majoré par dd' .

On a $R(X) = \begin{vmatrix} P_0(X) & \dots & P_p(X) & 0 & \dots & 0 \\ 0 & \dots & 0 & P_0(X) & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & Q_0(X) & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & Q_q(X) & \dots & 0 \end{vmatrix} = \det((R_{ij}(X))_{i,j})$,

où $R_{ij}(X) = \begin{cases} P_{j-i}(X) & \text{si } 1 \leq i \leq q, 0 \leq j-i \leq p \\ 0 & \text{si } 1 \leq i \leq q, (j < i \text{ ou } j > p+i) \\ Q_{j-i+q}(X) & \text{si } q+1 \leq i \leq p+q, 0 \leq j-i+q \leq q' \\ 0 & \text{si } q+1 \leq i \leq p+q, (j < i-q' \text{ ou } j > i) \end{cases}$

On a alors $\deg R_{ij}(X) \leq d - p + j - i$ si $1 \leq i \leq q$

$d' - q + j - i + q = d' + j - i$ si $q+1 \leq i \leq p+q$

De plus, $R(X) = \sum_{\sigma \in \mathcal{G}_{p+q}} \epsilon(\sigma) \prod_{i=1}^{p+q} R_{i, \sigma(i)}(X)$. Soit $\sigma \in \mathcal{G}_{p+q}$.

On a $\deg R_\sigma = \sum_{i=1}^{p+q} \deg R_{i, \sigma(i)} \leq \sum_{i=1}^q (d - p + (\sigma(i) - i)) + \sum_{i=q+1}^{p+q} (d' + \sigma(i) - i)$
 $\leq q(d - p) + pd' + \sum_{i=1}^{p+q} (\sigma(i) - i)$
 $\leq q(d - p) + d'(p - d) + dd' \leq dd'$

ce qui donne $\deg R \leq dd'$. De même, le degré de $S(Y) = \text{Res}_x(P(x, Y), Q(x, Y))$ est majoré par dd' .

Finalement, on a $|V(P) \cap V(Q)| \leq (dd')^2$. On va chercher à affiner cette majoration. On note $(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n)$ les éléments de $V(P) \cap V(Q)$. Si tous les α_i sont distincts, alors $n \leq dd'$, car les α_i sont racines de R , qui est de degré majoré par dd' .

On va se ramener à cela dans le cas général.

On commence par remarquer que les droites d'équation $y = \alpha_i + u\beta_i$ ont deux à deux au plus un point d'intersection. Comme k est infini, on fixe alors $u \in k$ tel que pour tous $i, j \in \{1, \dots, n\}$, avec $i \neq j$, on ait

$$\alpha_i + u\beta_i \neq \alpha_j + u\beta_j. \text{ On pose ensuite } \tilde{P}(X, Y) = P(X - uY, Y) \\ \tilde{Q}(X, Y) = Q(X - uY, Y)$$

$$\begin{aligned} \text{Alors } (\alpha, \beta) \in V(P) \cap V(Q) &\Leftrightarrow P(\alpha, \beta) = 0 \text{ et } Q(\alpha, \beta) = 0 \\ &\Leftrightarrow P((\alpha + u\beta) - u\beta, \beta) = 0 \text{ et } Q((\alpha + u\beta) - u\beta, \beta) = 0 \\ &\Leftrightarrow \tilde{P}(\alpha + u\beta, \beta) = 0 \text{ et } \tilde{Q}(\alpha + u\beta, \beta) = 0 \\ &\Leftrightarrow (\alpha + u\beta, \beta) \in V(\tilde{P}) \cap V(\tilde{Q}) \end{aligned}$$

En particulier, on a $|V(P) \cap V(Q)| = |V(\tilde{P}) \cap V(\tilde{Q})|$, ce qui permet de conclure.