Théorème de Bézout (intersection de zéros de polynômes)

Notation : Soient P, Q deux polynômes de degrés respectivement inférieurs à n, m. On définit $Res(P,Q)$ comme le déterminant de la matrice suivante :

$$C = \begin{bmatrix} p_0 & & & & q_0 & & & \\ p_1 & p_0 & & & q_1 & q_0 & & \\ p_2 & p_1 & p_0 & & q_2 & q_1 & q_0 & \\ p_n & . & . & . \; p_0 & q_m & . & . & . \; q_0 \\ & p_n & & & & q_m & & \\ & & p_n & . \; . & & & q_m & . \; . \\ & & & . \; p_n & & & & . \; q_m \end{bmatrix}$$

C'est-à-dire, en notant $(c_{i,j})_{0 \leq i,j \leq m+n-1}$ ses coefficients, $c_{i,j} = \begin{cases} p_{i-j} \text{ si } j < m \\ q_{i-(j-m)} \text{ si } m \leq j < n+m \\ 0 \text{ sinon} \end{cases}$.

Théorème. *Soit K un corps infini, $f, g \in K[X,Y]$ deux polynômes premiers entre eux, de degré total respectif n, m. On note $Z(f,g)$ leur zéros communs, alors $\#Z(f,g) \leq nm$.*

Démonstration. Pour x (resp y) fixé, on note $f(x,\cdot)$ (resp $f(\cdot,y)$) le polynôme $f(X,y)$ (resp $f(x,Y)$). La preuve part du constat que si (x_0,y_0) est une racine commune à f et g, alors $f(x_0,\cdot)$ et $g(x_0,\cdot)$ ont une racine en commun, donc ne sont pas premiers entre eux. En particulier, $Res(f(x_0,\cdot), g(x_0,\cdot)) = 0$.
On définit $R(X) = Res(f(X,\cdot), g(X,\cdot))$. On note

$$f(X,Y) = \sum_{i=0}^{n} f_i(X) Y^i \qquad f_i \in K_{n-i}[X]$$

$$g(X,Y) = \sum_{i=0}^{m} g_i(X) Y^i \qquad g_i \in K_{m-i}[X]$$

On forme alors la matrice $C(X)$ donnée par $c_{i,j}(X) = \begin{cases} f_{i-j}(X) \text{ si } j < m \\ g_{i-(j-m)}(X) \text{ si } m \leq j < n+m \\ 0 \text{ sinon} \end{cases}$
$R(X) = \det(C(X))$ et R est donc un polynôme en X, et selon les considérations ci dessus, tous les éléments de $\text{proj}_{K\times\{0\}}(Z(f,g))$ sont racines de R, donc $\#\text{proj}_{K\times\{0\}}(Z(f,g)) \leq \deg(R)$ si R est non identiquement nul.
On a $R = \sum_{\sigma \in S_{n+m}} \varepsilon(\sigma) F_\sigma(X)$, où

$$F_\sigma(X) = \prod_{j=0}^{m+n-1} c_{\sigma(j),j}$$

Si $j < m$, alors $\deg(c_{i,j}) \leq n - (i - j)$.
Si $m \leq j < n + m$, alors $\deg(c_{i,j}) \leq m - (i - (m - j)) = j - i$, d'où

$$\deg(F_\sigma) \leq \sum_{j=0}^{m-1} (n + j - \sigma(j)) + \sum_{j=m}^{n+m-1} (j - \sigma(j)) = nm$$

Reste à montrer que R est non nul. Si R est identiquement nul, alors f et g vu comme éléments de $K(X)[Y]$ ont un facteur commun $\frac{H(X,Y)}{D(X)}$ où H, D sont des polynômes premiers entre eux. Mais alors selon le lemme de Gauss, H divise P et Q dans $K[X,Y]$; c'est faux par hypothèse.

Donc $\#\mathrm{proj}_{K\times\{0\}}(Z(f,g)) \leq nm$. En faisant le même raisonnement selon y, on a la même majoration, d'où $\#Z(f,g) \leq (mn)^2$. On sait que c'est un ensemble fini, mais la majoration n'est pas suffisante.

Pour conclure, l'idée est de faire un changement de variable linéaire afin de projeter les racines sur un axe assez "générique" pour que deux racines n'aient pas la même image. C'est ici qu'on utilise le fait que K est infini.
Soit $k \in K$ que l'on fixera ensuite, on considère le changement de variable linéaire $\tilde{X} = X + kY, \tilde{Y} = Y$, c'est-à-dire qu'on considère les polynôme $\tilde{f}(X,Y) = f(X + kY, Y)$ et $\tilde{g}(X,Y) = g(X + kY, Y)$.
Soit (x, y_0) et (x, y_1) deux racines communes de $\tilde{f}$ et $\tilde{g}$. Alors y_0 et y_1 sont dans $\mathrm{proj}_{\{0\}\times K}(Z(f,g))$. De même, $x + ky_0 =: x_0$ et $x + ky_1 =: x_1$ sont dans $\mathrm{proj}_{K\times\{0\}}(Z(f,g))$. Si $y_0 \neq y_1$, on a alors

$$k = \frac{x_1 - x_0}{y_1 - y_0}$$

Il suffit de choisir k différents de tous les $\frac{x_1 - x_0}{y_1 - y_0}$ pour $x_0, x_1 \in \mathrm{proj}_{K\times\{0\}}(Z(f,g))$ et $y_0 \neq y_1 \in \mathrm{proj}_{\{0\}\times K}(Z(f,g))$, ce qui est possible car K est infini. Alors la projection sur la première coordonnée restreinte au racines communes de $\tilde{f}$ et $\tilde{g}$ est injective, et on peut donc majorer leur nombre comme précédemment par mn. $\square$