Nullstellensatz via le résultant

Thm: K algébriquement clos et $f_1, \dots, f_m \in K[X_1, \dots, X_n]$.
On suppose que $f_1, \dots, f_m$ n'ont pas de zéros communs dans K^n.
Alors il existe $h_1, \dots, h_m \in K[X_1, \dots, X_n]$ tq $\sum_{i=1}^{m} h_i f_i = 1$

1] <u>lemme</u>: Soit L un corps infini et $P \in L[X_1, \dots, X_n] \setminus \{0\}$ de degré d. Alors $\exists a_1, \dots, a_{n-1} \in L^{n-1}$ tq :
$P(a_1 X_n + X_1, a_2 X_n + X_2, \dots, a_{n-1} X_n + X_{n-1}, X_n)$ soit de la forme $c X_n^d + Q$ avec $d^\circ_{X_n} Q < d$ et $c \neq 0$.

$\hookrightarrow$ Soit Π la partie homogène de P de degré d.
Alors $P(a_1 X_n + X_1, \dots, a_{n-1} X_n + X_{n-1}, X_n) = \Pi(a_1, \dots, a_{n-1}, 1) X_n^d + Q$
avec $d^\circ_{X_n} Q < d$.

or K infini et $\Pi(X_1, \dots, X_{n-1}, 1)$ non nul $\Rightarrow \exists a_1, \dots, a_{n-1} \in K$ tq $c := \Pi(a_1, \dots, a_{n-1}, 1) \neq 0$. D'où le résultat.

2] On procède par récurrence sur n.

- Si $n = 1$, alors $K[X]$ est principal donc $\exists g \in K[X]$, $(g) = (f_1, \dots, f_m)$, $g = \operatorname{pgcd}(f_1, \dots, f_m)$. Mais alors une racine de g dans K est un zéro commun des $(f_i)_{i=1}^{m}$. Comme K est algébriquement clos, cela impose $d^\circ g \leq 1$ donc $g = cte \neq 0$ et le résultat.
- On suppose le résultat pour $n-1$ avec $n > 1$

via le lemme, OPS f_1 de la forme $X_n^d + Q$ avec $d^\circ_{X_n} Q < d$.

- Soit $g = f_2 + U f_3 + \dots + U^{m-2} f_m \in K[X_1, \dots, X_n, U]$

et $h = \mathrm{Rés}_{X_n}(f_1, g) \in K[X_1, \dots, X_{n-1}, U]$

et écrivons $h = D_0(X_1, \dots, X_{n-1}) + U D_1(X_1, \dots, X_{n-1}) + \dots$
$\dots + D_k(X_1, \dots, X_{n-1}) U^k$

- De plus, il existe $\Lambda, \Theta \in K[X_1, \dots, X_n, U]$ tq $h = \Lambda f_1 + \Theta g$

ce qui implique : $\forall i = 0 \dots k$, $D_i \in (f_1, \cancel{f_2}), \dots, f_m)$

3] Les $(D_i)_{i=0}^k$ n'ont pas de zéros communs :

Par l'absurde, soit $x=(x_1,\dots,x_{n-1}) \in K^{n-1}$ tq $\forall i=0,\dots k$, $D_i(x)=0$

Alors $\forall a \in K$, $h(x_1,\dots,x_{n-1},a)=0$.

Comme f_1 est unitaire en X_n (*), $f_1(x_1,\dots,x_{n-1},X_n)$ et $g(x_1,\dots,x_{n-1},X_n,a)$ ont une racine commune, dans K.

(et ce, pour tout $a \in K$).

Mais $f_1(x_1,\dots,x_{n-1},X_n)$ n'a qu'un nb fini de racines, donc $\exists x_n \in K$, $f_1(x_1,\dots,x_{n-1},x_n)=0$ et $\begin{cases} g(x_1,\dots,x_{n-1},x_n,a)=0 \\ \text{pour une infinité de } a\in K.\end{cases}$

On a alors $g(x_1,\dots,x_n,U)=0$

et donc $f_1(x_1,\dots,x_n)=f_2(x_1,\dots,x_n)=\dots=f_m(x_1,\dots,x_n)=0$

absurde par hypothèse.

4] Hypothèse de récurrence appliquée aux $(D_i)_{i=0}^k$.

$\rightsquigarrow$ $1 \in (D_0,\dots,D_k) \subset (f_1,\dots,f_m)$

et $1 \in (f_1,\dots,f_m)$.

(*) Du coup le résultant "ne s'annule pas pour rien"

Application : Si K est algébriquement clos,

Les idéaux maximaux de $K[X_1,\dots,X_n]$ sont exactement les $\langle X_1-a_1, X_2-a_2,\dots,X_n-a_n\rangle$ où $a=(a_1,\dots,a_n)\in K^n$.

- Ils sont maximaux (clairement). (passer au quotient)
- si $\mathfrak{m}$ est un idéal maximal, $\mathfrak{m}=\langle f_1,\dots,f_q\rangle$

car $K[X_1,\dots,X_n]$ est Noethérien.

Les $(f_i)_{i=1}^q$ ont un zéro commun noté $a\in K^n$ via le Nullstellensatz puisque $\mathfrak{m}\neq K[X_1,\dots,X_n]$. mais alors

$\mathfrak{m} \subset \langle X_1-a_1,\dots,X_n-a_n\rangle$ que l'on sait maximal

donc $=$.