# Nullstellensatz (par le résultant)



Théorème (Nullstellensatz faible) : Soient $k$ un corps algébriquement clos et $I$ un idéal de $k[X_1,\dots,X_n]$ vérifiant $V(I)=\emptyset$. Alors $I = k[X_1,\dots,X_n]$.

Démonstration : On raisonne par récurrence sur $n \in \mathbb{N}^*$.

• $n=1$ : Soit $I$ un idéal de $k[X_1]$ tel que $V(I)=\emptyset$. Comme $k[X_1]$ est principal, on écrit $I=(P)$, ce qui donne $V(I)=\{x\in k \,/\, P(x)=0\}=\emptyset$, donc $P$ est constant non nul, car $k$ est algébriquement clos. Il vient alors $I=k[X_1]$.

• Soit $n\in\mathbb{N}$. On suppose que l'unique idéal $J$ de $k[Z_1,\dots,Z_n]$ vérifiant $V(J)=\emptyset$ est $J=k[Z_1,\dots,Z_n]$. Soit $I$ un idéal de $k[X_1,\dots,X_{n+1}]$ tel que $V(I)=\emptyset$.
Comme $k[X_1,\dots,X_{n+1}]$ est noethérien, on écrit $I=(P_1,\dots,P_r)$. On suppose que $P_1$ n'est pas constant, sans quoi le résultat est immédiat. On note alors $N\in\mathbb{N}^*$ le degré total de $P_1$. On pose

$$\begin{aligned} Y_1 &= X_1 \\ Y_2 &= X_2 - a_2X_1 \\ &\vdots \\ Y_{n+1} &= X_{n+1}-a_{n+1}X_1 \end{aligned}$$

, où les $a_i$ sont des éléments de $k$ à ajuster.

On a
$$\begin{aligned} P_1(X_1,\dots,X_n) &= P_1(Y_1, Y_2+a_2Y_1,\dots,Y_{n+1}+a_{n+1}Y_1) \\ &= c(a_2,\dots,a_{n+1})\,Y_1^N + Q(Y_1,\dots,Y_{n+1}), \text{ avec } \deg_{Y_1} Q < N. \end{aligned}$$

Le corps $k$ étant infini, car algébriquement clos, on choisit $a_2,\dots,a_{n+1}\in k$ tels que $c(a_2,\dots,a_{n+1})\neq 0$ (car $c$ est polynomiale). Pour tout $i\in[\![1,r]\!]$, on pose $\tilde{P}_i(Y_1,\dots,Y_{n+1}) = P_i(X_1,\dots,X_{n+1})$. On pose de plus $\tilde{I}=(\tilde{P}_1,\dots,\tilde{P}_r)$ et on remarque que $V(\tilde{I})=\emptyset$, car $V(I)=\emptyset$. On pose $J=\tilde{I}\cap k[Y_2,\dots,Y_{n+1}]$.

On va montrer que $V(J)=\emptyset$. On raisonne par l'absurde.

Soit $(y_2, \dots, y_{m+1}) \in V(J)$. Pour tout $i \in [\![1, n]\!]$, on pose $R_i(Y_1) = \tilde{P}_i(Y_1, y_2, \dots, y_{m+1})$, puis $\tilde{J} = (R_1, \dots, R_n)$, qui est un idéal de $k[Y_1]$, ce qui permet d'écrire $\tilde{J} = (u)$, avec $u \in k[Y_1]$.

- Si $u = 0$, un élément $y_1 \in k$ quelconque donne $(y_1, y_2, \dots, y_{m+1}) \in k$ tel que $\tilde{P}_i(y_1, y_2, \dots, y_{m+1}) = 0$ pour tout $i \in [\![1, n]\!]$.

- Si $u$ n'est pas constant, on fixe $y_1 \in k$ tel que $u(y_1) = 0$ (ce qui est possible car $k$ est algébriquement clos). Ceci est absurde, car on a alors $\tilde{P}_i(y_1, y_2, \dots, y_m) = 0$ pour tout $i \in [\![1, n]\!]$.

- On suppose à présent que $u = u_0$ est une constante non nulle.

On fixe $\tilde{P} \in \tilde{I}$ tel que $\tilde{P}(Y_1, y_2, \dots, y_{m+1}) = u_0$, et on pose $R = \mathrm{Res}_{Y_1}(\tilde{P}_1, \tilde{P})$.

On fixe ensuite $U, V \in k[Y_1, \dots, Y_{m+1}]$ tels que $R = U\tilde{P}_1 + V\tilde{P}$.

On a alors $R \in \tilde{I}$, car $\tilde{P}_1, \tilde{P} \in \tilde{I}$, et $R \in k[Y_2, \dots, Y_{m+1}]$ car $R = \mathrm{Res}_{Y_1}(\tilde{P}_1, \tilde{P})$, donc $R \in J$, ce qui donne $R(y_2, \dots, y_{m+1}) = 0$.

Cependant, on a
$$\begin{aligned} R(y_2, \dots, y_{m+1}) &= \mathrm{Res}_{Y_1}(\tilde{P}_1(Y_1, y_2, \dots, y_{m+1}), \tilde{P}(Y_1, y_2, \dots, y_{m+1})) \\ &= \mathrm{Res}_{Y_1}(\tilde{P}_1(Y_1, y_2, \dots, y_{m+1}), u_0) \\ &= c(a_2, \dots, a_{m+1})\, u_0^N \neq 0 \end{aligned}$$

ce qui produit une contradiction. Le cas $u = u_0$ constante non nulle est donc impossible.

Finalement, on a $V(J) = \emptyset$. Par hypothèse de récurrence, on a donc $J = k[Y_2, \dots, Y_{m+1}]$, donc $k[Y_2, \dots, Y_{m+1}] \subset \tilde{I}$. En particulier, $1 \in \tilde{I}$, donc $\tilde{I} = k[Y_1, \dots, Y_{m+1}]$.

Il vient alors $I = k[X_1, \dots, X_{m+1}]$, ce qui achève la récurrence.

Corollaire (Nullstellensatz fort) : Soit $I$ un idéal de $k[X_1,\dots,X_n]$.

On pose $\sqrt{I} = \{ f \in k[X_1,\dots,X_n] \,/\, \exists m>0, f^m \in I \}$. On a $I(V(I)) = \sqrt{I}$.

Démonstration : On pose $R = k[X_1,\dots,X_n]$. Comme $R$ est noethérien, on écrit $I = (P_1,\dots,P_r)$.

• L'inclusion $\sqrt{I} \subset I(V(I))$ est immédiate. En effet, si $f \in \sqrt{I}$ et $m \in \mathbb{N}^*$ est tel que $f^m \in I$, on a $f^m(x_1,\dots,x_n) = 0$ pour tout $(x_1,\dots,x_n) \in V(I)$, d'où $f(x_1,\dots,x_n) = 0$ pour tout $(x_1,\dots,x_n) \in V(I)$.

• Soit $F \in I(V(I))$. On va montrer que $F^m \in I$ pour $m$ assez grand.

On remarque que ceci revient à montrer que l'idéal $IR_F$ engendré par $I$ dans $R_F$ (anneau localisé) est égal à $R_F$, car on pourrait alors écrire $1 = \sum_i \frac{P_i Q_i}{F^m}$, ce qui donnerait $F^m = \sum_i P_i Q_i \in I$. Pour ce faire, on commence par rappeler que l'anneau $R_F$ est isomorphe à $k[X_1,\dots,X_n,T]/(1-TF)$, donc montrer que $IR_F = R_F$ revient à montrer qu'il existe $A, Q_i \in k[X_1,\dots,X_n,T]$ tels que $1 = \sum_i P_i Q_i + A(1-TF)$.

On note $J$ l'idéal $(P_1,\dots,P_r, 1-TF)$ de $k[X_1,\dots,X_n,T]$, qui vérifie $V(J) = \emptyset$.

En effet, si l'on disposait de $(x_1,\dots,x_n,t) \in V(J)$, on aurait $(x_1,\dots,x_n) \in V(I)$, donc $F(x_1,\dots,x_n) = 0$, mais on aurait aussi $1 - tF(x_1,\dots,x_n) = 0$, ce qui serait absurde.

Par Nullstellensatz faible, on a alors $J = k[X_1,\dots,X_n,T]$, ce qui achève la preuve.