Nullstellensatz et élimination

Tristan Vaccon

septembre 2012

L'essentiel du développement se trouve dans [1], pages 165 à 171, mais aussi en partie (ou dans une version légèrement différente), dans [2], et dans un document de Michel Coste ("Élimination, Résultant, Discriminant") sur le site de la prépa agreg de Rennes I.

1 Théorème d'extension

Soit k un corps algébriquement clos.

Théorème 1 (Théorème d'extension)**.** *Soit $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ un idéal, et $I_1 = I \cap k[x_2, \ldots, x_n]$ un idéal d'élimination. On écrit, pour $i \in [\![1, s]\!]$, $f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + h_i(x)$ avec $h_i(x)$ composé de termes de degré en x_1 plus petit que N_i, avec $N_i \geqslant 0$, $g_i \in k[x_2, \ldots, x_n] \setminus \{0\}$, $h \in k[x_1, \ldots, x_n]$.*

Alors, si $(c_2, \ldots, c_n) \in V(I_1)$ et $(c_2, \ldots, c_n) \notin V(g_1, \ldots, g_s)$, alors $\exists c_1 \in k$ tel que $(c_1, \ldots, c_n) \in V(I)$.

Démonstration. Reprenons les notations de l'énoncé.

Soit $\phi : k[X_1, \ldots, X_n] \to k[X_1]$, $f \mapsto f(x_1, c)$.

$\phi(I)$ est un idéal de $k[x_1]$. En effet, l'application ϕ est clairement surjective.

Maintenant, $k[x_1]$ est principal, donc il existe $u \in k[x_1]$ tel que $\phi(I) = (u)$.

Première possibilité : $d_{x_1}(u) \neq 0$, et alors (k est algébriquement clos !), il existe $c_1 \in k$ tel que $u(c_1) = 0$. Mais alors : $\forall f \in I, f(c_1, c) = 0$, ce que l'on souhaitait.

Seconde possibilité, maintenant : $u = u_0$, non nul. Ainsi, il existe $f \in I$ tel que $f(x_1, c) = u_0$. Soit g_i tel que $g_i(c) \neq 0$.

Notons $f_i == g_i(x_2, \ldots, x_n)x_1^l + h_i(x)$ comme dans l'énoncé, et $f = \sum_{j=0}^{m} a_j(x_2, \ldots, x_n)x_1^j$ avec $m = d_{x_1}(f)$. Nécessairement, $a_0(c) = u_0$ et $u_j(c) = 0$ pour $j \geqslant 1$.

On en déduit que si l'on écrit

$$R = Res_{x_1}(f_i, f) = \det \begin{bmatrix} g_i & & & a_m & & \\ & \ddots & & \vdots & \ddots & \\ & & g_i & \vdots & & a_m \\ & * & & a_0 & & \vdots \\ & & & & \ddots & \vdots \\ & & & & & a_0 \end{bmatrix},$$

la première partie de la matrice faisant m colonnes, et la seconde l, alors en évaluant en c, on trouve :

$$R(c) = Res_{x_1}(f_i, f)(c) = \det \begin{bmatrix} g_i(c) & & & 0 & \dots & 0 \\ & \ddots & & \vdots & & \vdots \\ & & g_i(c) & 0 & & \vdots \\ & * & & u_0 & \ddots & \vdots \\ & & & & \ddots & 0 \\ & & & & & u_0 \end{bmatrix},$$

et ainsi,

$$R(c) = [Res_{x_1}(f_i, f)(c) = u_0^l g_i(c) \neq 0.$$

Mais $R = Res_{x_1}(f_i, f) \in (f, f_i) \subset I$ et $Res_{x_1}(f_i, f) \in k[x_2, \dots, x_n$, donc $R(c) = 0$, par définition. Ce qui est absurde.

Enfin, troisième possibilité : $\phi(I) = (0)$, et alors, tout c_1 convient. □

2 Nullstellensatz

Théorème 2 (Weak Nullstellensatz)**.** *Soit $I = \langle f_1, \dots, f_r \rangle \subset k[X_1, \dots, X_n]$ un idéal tel que $V(I) = \emptyset$. Alors $I = k[X_1, \dots, X_n]$.*

Démonstration. Nous allons raisonner par récurrence sur n, le nombre de variables.

Pour $n = 1$, k étant un corps, on a nécessairement $I = \langle u \rangle$ pour un certain u. Si $deg(u) \geqslant 1$, comme k est algébriquement clos, alors $V(I) \neq \emptyset$, et cela est aussi vrai si $u = 0$. Sinon, u est une constante et $I = k[X_1, \dots, X_n]$. Ceci conclut l'initialisation de la récurrence.

Supposons le résultat vrai pour $n - 1$ variables. On peut supposer que $f_1 \neq 0$ et on pose N son degré total.

Nous allons, pour $a_2, \dots, a_n \in k$ effectuer le changement de variables : $x_1 = \widetilde{x_1}$, $x_2 = \widetilde{x_2} + a_2 x_1$, …, $x_n = \widetilde{x_n} + a_n x_n$.

On a alors $f_1(x_1,\dots,x_n) = c(a_2,\dots,a_n)\widetilde{x_1}^N + g_1 = \widetilde{f_1}(x_1,\dots,x_n)$ avec g_1 constitués de termes de degré en $\widetilde{x_1}$ strictement inférieur à N.

Remarquons que $f_i(b_1,\dots,b_n) = 0$ si et seulement si $\widetilde{f_i}(\widetilde{b_1},\dots,\widetilde{b_n})$. On remarque aussi que par définition $c(a_2,\dots,a_n) \neq 0$ vu dans $k[a_2,\dots,a_n]$.

Comme k est infini (puisque algébriquement clos), il existe bien $a_2,\dots,a_n \in k$ tel que $c(a_2,\dots,a_n) \neq 0 \in k$.

Nous pouvons alors appliquer le théorème d'extension démontré plus haut.

En effet, si il existe $\widetilde{b_2},\dots,\widetilde{b_n} \in V(\tilde{I} \cap k[\widetilde{x_2},\dots,\widetilde{x_n}])$, comme $c(a_2,\dots,a_n)$ est une constante non nulle, il existe $\widetilde{x_1}$ tel que $(\widetilde{x_1},\dots,\widetilde{x_n}) \in V(\tilde{I})$. Or ceci est absurde puisque $V(\tilde{I}) = \emptyset = V(I)$ par hypothèse.

On en déduit que $V(\tilde{I} \cap k[\widetilde{x_2},\dots,\widetilde{x_n}]) = \emptyset$. Appliquons alors l'hypothèse de récurrence, $1 \in \tilde{I} \cap k[\widetilde{x_2},\dots,\widetilde{x_n}]$, et donc $1 \in \tilde{I}$ et $1 \in I$. Ce que l'on souhaitait démontrer.

□

Définition 2.1. Let I be an ideal of $k[X_1,\dots,X_n]$. We define its **radical ideal** $\sqrt{I}$ by

$$\sqrt{I} = \{f \in k[X_1,\dots,X_n] \,/\, \exists m \in \mathbb{N}^*, f^m \in I\}.$$

An ideal I such that $I = \sqrt{I}$ is called radical.

Théorème 3 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field. Let J be an ideal of $k[X_1,\dots,X_n]$. Then*

$$\sqrt{J} = I(V(J)).$$

Démonstration. First, let $P \in \sqrt{J}$, then there exist $r \in \mathbb{N}^*$ such that $P^r \in J$. Then, if $x \in V(J)$, then $P^r(x) = 0$ and k is a field so $P(x) = 0$. Thus, $P \in I(V(J))$ and $\sqrt{J} \subset I(V(J))$.

Conversely, let $P \in I(V(J)$. In $k[X_1,\dots,X_n,T]$, let J' be the ideal generated by J and $1 - TP$.

If $V(J') \neq \varnothing$, let $z = (x_1,\dots,x_n,t) = (x,t) \in V(J')$. Then $(1-PT)(z) = 0$ and also $x \in V(J)$, so $P(x) = 0$. Thus $(1-PT)(z) = 1 - P(x)t = 1 - 0 = 1 \neq 0$ which is absurd. So $V(J') = \varnothing$.

With the previous theorem, $J' = k[X_1,\dots,X_n,T]$, so there exist $m \in \mathbb{N}^*$, $Q_0,\dots,Q_m$ in $k[X_1,\dots,X_n,T]$, $(P_1,\dots,P_j) \in J^m$ such that

$$(1-TP)Q_0 + \sum_{j=1}^{m} Q_j P_j = 1.$$

In $k(X_1,\dots,X_n)$, we can substitute T by $\frac{1}{P}$ and we find

$$\sum_{j=1}^{m} Q_j(X_1,\dots,X_n,\frac{1}{P})P_j(X_1,\dots,X_n) = 1.$$

With r large enough (for instance, larger than the maximum over j of the maximum of the degree in T of the Q_j), we have the equality in $k[X_1, \ldots, X_n]$: $P^r = \sum_{j=1}^{m} P^r Q_j(X_1, \ldots, X_n, \frac{1}{P}) P_j(X_1, \ldots, X_n)$. Hence, $P^r \in J$, and the result is proven. $\square$

Références

[1] Cox, Little, O'Shea Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra

[2] Van der Waerden Modern Algebra tome 2