Le théorème des zéros de Hilbert

Olivier Dodane

8 octobre 2007

Résumé

La démonstration du théorème des zéros de Hilbert qui est donnée ici est inspirée d'une idée de Zariski, reprise par Atiyah & MacDonald (*Introduction to Commutative Algebra*, Addison-Wesley, 1969, Ex. 18 p. 70) puis par Chambert-Loir (*Algèbre commutative et introduction à la géométrie algébrique*, Cours à l'Université Paris VI, 1999).

Rappels. — Soit A un anneau. Une *A-algèbre* est un anneau B muni d'un morphisme d'anneaux $f\colon A \to B$. On dit que B est *de type fini* s'il existe un entier $n \in \mathbf{N}$ et des éléments $x_1, \ldots, x_n \in B$ tels que tout élément de B s'écrit comme un polynôme en les variables $x_1, \ldots, x_n$ à coefficients dans $f(A)$. Autrement dit, B est de type fini si l'on a $B \simeq A[X_1, \ldots, X_n]/I$, où I est un idéal de $A[X_1, \ldots, X_n]$.

Soit B une A-algèbre. On dit que B est entière sur A si tout élément de B est entier sur A, c'est-à-dire si tout élément de B est solution d'une équation polynomiale unitaire à coefficients dans $f(A)$.

Lemme. — *Soient $A \subset B$ deux anneaux tels que B est entier sur A. Si B est un corps, alors A est un corps.*

Remarque. — Si B est intègre, on a aussi la réciproque : si A est un corps, alors B est un corps.

Démonstration. — Soit x un élément non nul de A. Son inverse y dans B est entier sur A, donc on a une relation

$$y^m + a_{m-1}y^{m-1} + \cdots + a_1 y + a_0 = 0 \quad (\text{avec } m \in \mathbf{N}^* \text{ et } a_i \in A).$$

En multipliant cette relation par x^{m-1}, on obtient

$$y = -(a_{m-1} + \cdots + a_1 x^{m-2} + a_0 x^{m-1}),$$

ce qui montre que $y \in A$. □

Théorème 1. — *Soit k un corps et soit B une k-algèbre de type fini. Si B est un corps, alors B est une extension algébrique finie de k.*

Démonstration. — Pour tout $n \in \mathbf{N}$, notons $\mathcal{P}(n)$ la propriété suivante : « Si k est un corps et si B est une k-algèbre de type fini engendrée par n éléments qui est un corps, alors B est une extension algébrique finie de k ». On raisonne par récurrence sur n.

La propriété $\mathcal{P}(0)$ est vraie car dans ce cas $B = k$. Si $n = 1$, on a $B = k[x_1]$. Si x_1 était transcendant sur k, on aurait $B \simeq k[X]$ qui n'est pas un corps. Donc x_1 est algébrique et par suite B est une extension algébrique finie de k.

Supposons maintenant que $n > 1$ et que $\mathcal{P}(n-1)$ est vraie. Soit B une k-algèbre de type fini engendrée en tant que k-algèbre par des éléments $x_1, \ldots, x_n \in B$. On a donc $B = k[x_1, \ldots, x_n]$. Soit $A = k[x_1]$ et soit K le corps des fractions de A ; on a $K \subset B$ (car B est un corps) de sorte que B est une K-algèbre de type fini engendrée par $n-1$ éléments. Par hypothèse de récurrence, B est une extension algébrique finie de K. En particulier, les éléments x_i, pour $2 \leqslant i \leqslant n$, sont algébriques sur K, donc il existe des polynômes unitaires $P_2, \ldots, P_n \in K[X]$ tels que $P_i(x_i) = 0$ pour tout $2 \leqslant i \leqslant n$. Soit $f \in k[x_1]$ le produit de tous les dénominateurs des coefficients des P_i, de sorte que les éléments $x_2, \ldots, x_n$ sont entiers sur $A_f = A[1/f]$. Ainsi, B est entier sur A_f (puisque ses générateurs le sont tous) et comme $A_f \subset B$ (car B est un corps), on déduit du lemme que A_f est un corps.

Maintenant, supposons que x_1 est transcendant sur k ; alors $A_f \simeq k[X][1/P]$, où $P \in k[X]$ est un polynôme non nul. L'élément $1 - XP$ est non nul dans A_f et il n'est pas inversible (car s'il existe $Q \in A_f$ tel que $(1 - XP)Q = 1$, en substituant $1/P$ à X on a une contradiction) : ceci contredit le fait que A_f est un corps. Donc x_1 est algébrique sur k ; par suite, K est une extension algébrique finie de k. Or on sait que B est un extension algébrique finie de K, d'où le résultat. □

Théorème 2 (Nullstellensatz faible, version 1). — *Soit k un corps algébriquement clos. Les idéaux maximaux de $k[X_1, \ldots, X_n]$ sont de la forme*

$$\langle X_1 - a_1, \ldots, X_n - a_n \rangle$$

où les a_i sont des éléments de k.

Démonstration. — Montrons d'abord que les idéaux de la forme $J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ sont maximaux. L'application $\phi\colon k[X_1, \ldots, X_n] \to k$ définie par $\phi(P) = P(a_1, \ldots, a_n)$ est un morphisme surjectif d'anneaux. Soit $P \in \operatorname{Ker}(\phi)$. En écrivant la division euclidienne de P par $X_1 - a_1$, puis celle du reste par $X_2 - a_2$, …, on obtient

$$P = (X_1 - a_1)Q_1 + \cdots + (X_n - a_n)Q_n + P(a_1, \ldots, a_n) \quad (\text{avec } Q_j \in k[X_j, \ldots, X_n]),$$

et comme $P \in \operatorname{Ker}(\phi)$, on en déduit que $P \in J$. Donc $\operatorname{Ker}(\phi) \subset J$. L'inclusion réciproque est évidente, donc $\operatorname{Ker}(\phi) = J$. On en déduit que $k[X_1, \ldots, X_n]/J \simeq k$, donc J est maximal.

Soit $\mathfrak{m}$ un idéal maximal de $k[X_1, \ldots, X_n]$. Alors $k[X_1, \ldots, X_n]/\mathfrak{m}$ est une k-algèbre de type fini qui est un corps. D'après le théorème précédent, c'est une extension finie de k et comme k est algébriquement clos, on a

$$k[X_1, \ldots, X_n]/\mathfrak{m} = k.$$

Pour tout $1 \leqslant i \leqslant n$, il existe donc $a_i \in k$ tel que $X_i - a_i \in \mathfrak{m}$. Ainsi, l'idéal $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ est contenu dans $\mathfrak{m}$. Comme on a déjà montré ci-dessus qu'il est maximal, il lui est égal. □

Théorème 3 (Nullstellensatz faible, version 2). — *Soit k un corps algébriquement clos et soit I un idéal de $k[X_1, \ldots, X_n]$. On a*

$$V(I) = \emptyset \quad \Longleftrightarrow \quad I = k[X_1, \ldots, X_n].$$

Démonstration. — Il est clair que $V(I) = \emptyset$ si $1 \in I$. Réciproquement, si $I \neq k[X_1, \ldots, X_n]$, il existe un idéal maximal $\mathfrak{m}$ qui contient I. D'après le théorème précédent, $\mathfrak{m}$ est de la forme $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ avec $a_i \in k$. Pour tout $P \in I$, on a $P \in \mathfrak{m}$, donc $P(a_1, \ldots, a_n) = 0$, ce qui montre que $(a_1, \ldots, a_n) \in V(I)$. Ainsi, $V(I) \neq \emptyset$. □

Théorème 4 (Nullstellensatz).— *Soit k un corps algébriquement clos et soit I un idéal de $k[X_1, \ldots, X_n]$. On a $I(V(I)) = \sqrt{I}$.*

Démonstration.— Soit $P \in \sqrt{I}$. Il existe un entier $r \geqslant 1$ tel que $P^r \in I$. Par conséquent, pour tout $x \in V(I)$, on a $P^r(x) = 0$ et donc $P(x) = 0$. Ainsi, $P \in I(V(I))$.

Réciproquement, soit $P \in I(V(I))$. Dans $k[X_1, \ldots, X_n, T]$, l'idéal J engendré par I et $1 - TP$ définit un ensemble algébrique *vide* car si $x \in V(J)$, on a $x \in V(I)$, donc $P(x) = 0$ (car $P \in I(V(I))$). Par suite, $(1 - TP)(x) = 1 \neq 0$. D'après le théorème précédent, on a $J = k[X_1, \ldots, X_n, T]$ et donc il existe des polynômes $Q_0, \ldots, Q_m \in k[X_1, \ldots, X_n, T]$ tels que

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

En substituant $1/P$ à T dans cette égalité, on obtient l'égalité suivante dans $k(X_1, \ldots, X_n)$:

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

Prenons un entier $r \geqslant 1$ assez grand pour que $P^r Q_j(X_1, \ldots, X_n, 1/P)$ soit dans $k[X_1, \ldots, X_n]$ pour tout j. On a alors

$$P^r = \sum_{j=1}^{m} P_j \cdot P^r Q_j(X_1, \ldots, X_n, 1/P),$$

donc $P^r \in I$. $\square$