Université Claude Bernard LYON 1
Préparation à l'agrégation de Mathématiques

Le théorème des zéros de Hilbert

Michel CRETIN

Lemme 1 *Pour tout corps commutatif K infini et toute K-algèbre L de type fini qui est un corps, la K-extension L est de degré fini.*

$\triangledown$ Soient $x_1, \cdots, x_n \in L$ tels que $L = K[x_1, \cdots, x_n]$; si $n = 1$, comme $K[x_1]$ est un corps, x_1 est algébrique sur K et $L = K[x_1]$ est une K-extension de degré fini. Procédons alors par récurrence sur n et supposons que les générateurs $x_1, \cdots, x_n$ ne soient pas tous algébriques sur K *eg.* supposons x_n non algébrique sur K ; alors $R = K[x_n]$ est une sous algèbre de L (isomorphe à un algèbre de polynômes à une indéterminée) et son corps des fractions $F = K(x_n)$ (isomorphe à un corps de fractions rationnelles à une indéterminée) est un sous-corps de L. On a alors $L = F[x_1, \cdots, x_{n-1}]$ et par hypothèse de récurrence $x_1, \cdots, x_{n-1}$ sont algébriques sur F. On peut donc écrire, pour $1 \leq i \leq n-1$, $x_i^{n_i} + \sum_{j_i=1}^{n_i-1} a_{i,j_i} x_i^{n_i-j_i} = 0$ avec les coefficients $a_{i,j_i} \in F$. Soit $c \in R$, *non nul*, tel que $ca_{i,j_i} \in R$, $1 \leq i \leq n-1$, $1 \leq j_i \leq n_i$; les cx_i, $1 \leq i \leq n-1$, sont alors des éléments *entiers* sur R, de sorte que, pour tout $x \in L$, il existe un entier $k \geq 0$ tel que $c^k x$ soit entier sur R. En particulier, puisque R est *intégralement clos*, pour tout $x \in F$, il existe $k \geq 0$ tel que $c^k x \in R$, mais ce n'est pas possible comme on le voit en prenant par exemple $x = \dfrac{1}{x_n - a}$ où $a \in K$ n'est pas racine de c. $\triangle$

Pour tout idéal I de $\mathbb{C}[X_1, \cdots, X_n]$ soit $Z(I)$ l'ensemble des $(x_1, \cdots, x_n) \in \mathbb{C}^n$ tels que $f(x_1, \cdots, x_n) = 0$ pour tout $f \in I$.
Tout idéal I de $\mathbb{C}[X_1, \cdots, X_n]$ est engendré par un nombre fini de polynômes $f_1, \cdots, f_r$ (théorème de l*a base finie* de Hilbert) de sorte que l'on on a $Z(f_1, \cdots, f_r) = Z(I)$.

Exemple : Pour tout $x = (x_1, \cdots, x_n) \in \mathbb{C}^n$, *l'idéal* $\mathfrak{m}_x$ formé des polynômes $f \in \mathbb{C}[X_1, \cdots, X_n]$ tels que $f(x) = 0$ est maximal, est engendré par les polynômes $X_i - x_i$ pour $1 \leq i \leq n$ et l'on a $Z(\mathfrak{m}_x) = \{x\}$.
$\triangledown$ Soit $\mathfrak{m}'$ l'idéal engendré par les polynômes $X_i - x_i$ pour $1 \leq i \leq n$; on a évidemment $\mathfrak{m}' \subset \mathfrak{m}_x$. Réciproquement soit $f \in \mathfrak{m}_x$; puisque $X_1 - x_1$ est unitaire, on peut effectuer la division euclidienne de f par $X_i - x_i$ dans l'anneau $\mathbb{C}[X_2, \cdots, X_n][X_1]$; de sorte que $f = (X_1 - x_1)q_1 + f_1$ avec $f_1 \in \mathbb{C}[X_2, \cdots, X_n]$. On obtient finalement $f = \sum_{i=1}^{n} (X_i - x_i)q_i + c$ avec $c \in \mathbb{C}$ et l'on a $c = f(x) = 0$ donc $f \in \mathfrak{m}'$.
On a évidemment $x \in Z(\mathfrak{m}_x)$. Pour $y \neq x$, il existe i, $1 \leq i \leq n$ tel que $x_i \neq y_i$; si $f = X_i - x_i$ on a $f \in \mathfrak{m}_x$ et $f(y) \neq 0$ et $y \notin Z(\mathfrak{m}_x)$. $\triangle$.

Proposition 1 (th des zéros de Hilbert) *L'application $x \longrightarrow \mathfrak{m}_x$ de $\mathbb{C}^n$ dans l'ensemble des idéaux maximaux de $\mathbb{C}[X_1, \cdots, X_n]$ est une bijection.*

$\triangledown$ Si $\mathfrak{m}_x = \mathfrak{m}_y$ on a $\{x\} = Z(\mathfrak{m}_x) = Z(\mathfrak{m}_y) = \{y\}$. Il faut donc établir la surjectivité de l'application $x \longrightarrow \mathfrak{m}_x$. Considérons un idéal maximal $\mathfrak{m}$ de $\mathbb{C}[X_1, \cdots, X_n]$. Alors $L = \mathbb{C}[X_1, \cdots, X_n]/\mathfrak{m}$ est une $\mathbb{C}$-algèbre de type fini qui est un corps ; c'est donc une $\mathbb{C}$-extension algébrique et comme $\mathbb{C}$ est algébriquement clos $\mathbb{C} \overset{\varphi}{\simeq} L$. Pour $1 \leq i \leq n$ on pose $x_i = \varphi(\overline{X_i})$ de sorte que $X_i - x_i \in \mathfrak{m}$ donc $\mathfrak{m}_x \subset \mathfrak{m}$ et $\mathfrak{m}_x = \mathfrak{m}$ $\triangle$

Corollaire 1 *Pour tout idéal I de $\mathbb{C}[X_1, \cdots, X_n]$ on a $Z(I) = \emptyset$ si et seulement si $I = \mathbb{C}[X_1, \cdots, X_n]$.*

$\triangledown$ Considérons un idéal I de $\mathbb{C}[X_1, \cdots, X_n]$ tel que $I \neq \mathbb{C}[X_1, \cdots, X_n]$. Puisque $\mathbb{C}[X_1, \cdots, X_n]$ est *noethérien*, l'ensemble des idéaux J de $\mathbb{C}[X_1, \cdots, X_n]$ tel que $I \subset J \underset{\neq}{\subset} \mathbb{C}[X_1, \cdots, X_n]$ a un élément maximal $\mathfrak{m}$. Ainsi $\mathfrak{m}$ est un idéal *maximal* de $\mathbb{C}[X_1, \cdots, X_n]$ et il existe $x \in \mathbb{C}^n$ tel que $\mathfrak{m} = \mathfrak{m}_x$. On a donc $x \in Z(I)$ et $Z(I) \neq \emptyset$. $\triangle$

La *racine* d'un idéal I de $\mathbb{C}[X_1, \cdots, X_n]$ est l'idéal $\mathrm{rac}(I)$ formé des polynômes $f \in \mathbb{C}[X_1, \cdots, X_n]$ pour lesquels il existe un entier $k \geq 1$ tel que $f^k \in I$. On a évidemment $I \subset \mathrm{rac}(I)$.

Corollaire 2 *Pour tout idéal I de $\mathbb{C}[X_1, \cdots, X_n]$, $\mathrm{rac}(I)$ est l'ensemble des $f \in \mathbb{C}[X_1, \cdots, X_n]$ pour lesquels $f|_{Z(I)} = 0$.*

$\triangledown$ Soit $f \in \mathrm{rac}(I)$; on $f^k \in I$ pour un entier $k \geq 1$, d'où $f^k(x) = 0$ et donc $f(x) = 0$ pour tout $x \in Z(I)$.
Réciproquement supposons que $f(x) = 0$ pour tout $x \in Z(I)$ et considérons l'idéal :

$$J = (I, 1 - X_{n+1}f)$$

de $\mathbb{C}[X_1, \cdots, X_n, X_{n+1}]$.
On a $Z(J) = \emptyset$; il existe donc $f_1, \cdots, f_m \in I$, $g_1, \cdots, g_m, g_{m+1} \in \mathbb{C}[X_1, \cdots, X_n, X_{n+1}]$ tels que :

$$\sum_{i=1}^{m} g_i(X_1, \cdots, X_n, X_{n+1}) f_i(X_1, \cdots, X_n) + g_{m+1}(X_1, \cdots, X_n, X_{n+1})(1 - X_{n+1} f(X_1, \cdots, X_n)) = 1$$

il vient alors :

$$\sum_{i=1}^{m} g_i(X_1, \cdots, X_n, \frac{1}{f(X_1, \cdots, X_n)}) f_i(X_1, \cdots, X_n) = 1$$

et finalement :

$$\sum_{i=1}^{m} \widetilde{g_i}(X_1, \cdots, X_n) f_i(X_1, \cdots, X_n) = f(X_1, \cdots, X_n)^k$$

avec $\widetilde{g_i}(X_1, \cdots, X_n) \in \mathbb{C}[X_1, \cdots, X_n]$ pour $1 \leq i \leq m$ de sorte que $f^k \in I$. $\triangle$

Corollaire 3 *Pour I et J idéaux de $\mathbb{C}[X_1, \cdots, X_n]$, on a $Z(I) = Z(J)$ si et seulement si $\mathrm{rac}(I) = \mathrm{rac}(J)$.*

$\triangledown$ On a $Z(\mathrm{rac}(I)) = Z(I)$; en effet comme $I \subset \mathrm{rac}(I)$ on a $Z(\mathrm{rac}(I)) \subset Z(I)$; réciproquement soit $x \in Z(I)$ alors pour tout $f \in \mathrm{rac}(I)$ on a donc $f(x) = 0$ de sorte que $x \in Z(\mathrm{rac}(I))$.
On a de même $Z(\mathrm{rac}(J)) = Z(J)$, de sorte que si $\mathrm{rac}(I) = \mathrm{rac}(J)$ on a $Z(I) = Z(J)$.
Réciproquement supposons que $Z(I) = Z(J)$. Pour $f \in \mathrm{rac}(I)$, on a donc $f(x) = 0$ pour tout $x \in Z(J)$ de sorte que $f \in \mathrm{rac}(J)$ et donc $\mathrm{rac}(I) \subset \mathrm{rac}(J)$. De même $\mathrm{rac}(J) \subset \mathrm{rac}(I)$ $\triangle$