LE THÉORÈME DES ZÉROS DE HILBERT

par

Stef Graillat

Le théorème des zéros de Hilbert (aussi appelé *Nullstellensatz*) décrit les idéaux maximaux de l'anneau des polynômes à plusieurs indéterminées sur un corps algébriquement clos. Lorsque ce dernier est en plus non dénombrable (il est nécessairement infini car un corps fini n'est jamais algébriquement clos), par exemple $\mathbf{C}$, la démonstration du résultat est plus simple. Nous nous contenterons ici de ce cas. Ce résultat trouve naturellement sa place dans les leçons :

- 111 : Idéaux d'un anneau commutatif unitaire. Exemples et applications.
- 116 : Algèbres des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques.

La démonstration que nous donnons ici est tirée de [**Art91**, p.371] et de [**CL01**, **CL04**]. On pourra aussi regarder dans [**Gob01**] pour le cas ou le corps est juste supposé algébriquement clos.

On va tout d'abord s'intéresser aux idéaux maximaux de $\mathbf{C}[X]$ qui est un anneau principal (il est même euclidien).

PROPOSITION. — *Les idéaux maximaux de* $\mathbf{C}[X]$ *sont les* $(X-a)$ *pour* $a \in \mathbf{C}$.

Démonstration. — Soit $I = (P)$ un idéal maximal de $\mathbf{C}[X]$. Comme I est maximal, $I \neq \mathbf{C}[X]$ et donc $\deg P \geqslant 1$. Comme $\mathbf{C}$ est algébriquement clos, P est divisible par un polynôme du type $X-a$ pour un $a \in C$ (en effet, P a au moins une racine dans $\mathbf{C}$). Par conséquent $(X-a) \supset (P) = I$. Comme $(X-a) \neq \mathbf{C}[X]$ et comme I est maximal, on en déduit que $I = (X-a)$.

Réciproquement, si $a \in \mathbf{C}$, il nous faut montrer que l'idéal $(X-a)$ est bien un idéal maximal. Soit $\varphi : \mathbf{C}[X] \to \mathbf{C}$ l'homomorphisme d'anneaux défini par $\varphi(P) = P(a)$. Il est surjectif (En effet pour tout $b \in \mathbf{C}$, le polynôme $P = X - a + b$ vérifie $\varphi(P) = b$.). Il est clair que $X - a \in \operatorname{Ker}\varphi$ et donc $(X-a) \subset \operatorname{Ker}\varphi$ car $\operatorname{Ker}\varphi$ est un idéal. Réciproquement, si $P \in \operatorname{Ker}\varphi$, alors P possède a comme racine. Il est donc divisible par $X-a$ et alors $P \in (X-a)$. En résumé, $\operatorname{Ker}\varphi = (X-a)$. Par passage au quotient, on a $\mathbf{C}[X]/\operatorname{Ker}\varphi \simeq \mathbf{C}$ c'est-à-dire $\mathbf{C}[X]/(X-a) \simeq \mathbf{C}$. Il en résulte que $\mathbf{C}[X]/(X-a)$ est un corps et donc que l'idéal $(X-a)$ est bien maximal. □

Grâce à ce résultat, on va pouvoir généraliser au cas de plusieurs indéterminées.

THÉORÈME. — *Soient* $n \geqslant 1$ *et* I *un idéal maximal de l'anneau* $\mathbf{C}[X_1, \ldots, X_n]$. *Alors il existe un* unique *élément* $(a_1, \ldots, a_n) \in \mathbf{C}^n$ *tel que* $I = (X_1 - a_1, \ldots, X_n - a_n)$.

Démonstration. — Soit $I = (X_1 - a_1, \dots, X_n - a_n)$. Montrons que I est un idéal maximal. Le morphisme d'anneaux $\varphi : \mathbf{C}[X_1, \dots, X_n] \to \mathbf{C}$ défini par $\varphi(P) = P(a_1, \dots, a_n)$ est surjectif (En effet, pour tout $b \in \mathbf{C}$, le polynôme $P = (X - a_1) \cdots (X - a_n) + b$ vérifie $P(a_1, \dots, a_n) = b$.). On va montrer que $\operatorname{Ker}\varphi = I$. Il est clair que $I \subset \operatorname{Ker}\varphi$. Soit $P \in \operatorname{Ker}\varphi$. En effectuant la division euclidienne de P par $X_1 - a_1$, on obtient $P = (X_1 - a_1)Q_1 + P_1$ avec $\deg_{X_1} P_1 < 1$; par conséquent $P_1 \in \mathbf{C}[X_2, \dots, X_n]$. En itérant le procédé, on obtient $P = (X_1 - a_1)Q_1 + (X_2 - a_2)Q_2 + \cdots + (X_n - a_n)Q_n + P_n$ avec $P_n \in \mathbf{C}$. En évaluant au point $(a_1, \dots, a_n)$, on obtient $P(a_1, \dots, a_n) = 0 = P_n$; donc $P \in (X_1 - a_1, \dots, X_n - a_n)$. On a donc $\operatorname{Ker}\varphi = I$. En passant au quotient, on obtient $\mathbf{C}[X_1, \dots, X_n]/I \simeq \mathbf{C}$ et donc $I = (X_1 - a_1, \dots, X_n - a_n)$ est un idéal maximal.

Réciproquement, soit I un idéal maximal de $\mathbf{C}[X_1, \dots, X_n]$. Considérons le morphisme de $\mathbf{C}$-algèbre composé

$$\varphi_1 : \mathbf{C}[X_1] \hookrightarrow \mathbf{C}[X_1, \dots, X_n] \twoheadrightarrow \mathbf{C}[X_1, \dots, X_n]/I = \mathbf{K}.$$

L'anneau $\mathbf{C}[X_1, \dots, X_n]$ est une $\mathbf{C}$-algèbre et sa dimension en tant que $\mathbf{C}$-espace vectoriel est infinie dénombrable. En effet, il admet comme base la famille $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ indexée par $\mathbf{N}^n$, donc dénombrable. *A fortiori*, l'anneau quotient $\mathbf{K} = \mathbf{C}[X_1, \dots, X_n]/I$ est une $\mathbf{C}$-algèbre de dimension au plus dénombrable.

Si φ_1 est injective, le fait que $\mathbf{K}$ soit un corps nous permet d'étendre φ_1 en une injection de $\mathbf{C}(X_1)$ dans $\mathbf{K}$ (*cf.* [Goz97, p.2]). Ainsi une sous-algèbre de $\mathbf{K}$ est isomorphe à $\mathbf{C}(X_1)$. Or, ce corps admet la famille libre formée des $1/(X_1 - a)$ pour $a \in \mathbf{C}$. Comme $\mathbf{C}$ est non dénombrable, $\mathbf{C}(X_1)$ est un $\mathbf{C}$-espace vectoriel de dimension non dénombrable, ce qui est absurde. Donc φ_1 n'est pas injective et $\operatorname{Ker}\varphi_1 \neq \{0\}$. Or $\operatorname{Ker}\varphi_1$ est un idéal premier comme image réciproque d'un idéal premier ((0) est premier car $\mathbf{C}[X_1, \dots, X_n]$ est intègre). L'anneau $\mathbf{C}[X_1]$ étant principal, idéaux premiers et maximaux coïncident. D'après la proposition précédente $\operatorname{Ker}\varphi_1$ est un idéal (maximal) de la forme $(X_1 - a_1)$.

Remarque. — Si l'on ne connaît pas les résultats utilisés ci-dessus, on peut quand même s'en tirer autrement. On a $\operatorname{Ker}\varphi_1 = (P)$ pour un polynôme $P \in \mathbf{C}[X_1]$ et $\deg P \geqslant 1$ car φ_1 est non nulle puisque $I \neq \mathbf{C}[X_1, \dots, X_n]$. Or $\mathbf{C}$ étant algébriquement clos, il existe $a_1 \in \mathbf{C}$ tel que $P = (X_1 - a_1)Q$ et alors $\varphi_1(P) = \varphi_1(X_1 - a_1)\varphi_1(Q)$. Comme $\mathbf{K}$ est intègre (car c'est un corps), on a $\varphi_1(X_1 - a_1) = 0$ ou $\varphi_1(Q) = 0$. Si $\varphi_1(X_1 - a_1) = 0$ alors $X_1 - a_1 \in \operatorname{Ker}\varphi_1$ et d'après la proposition précédente $\operatorname{Ker}\varphi_1 = (X_1 - a_1)$ car l'idéal $(X_1 - a_1)$ est maximal. Si $\varphi_1(X_1 - a_1) \neq 0$ c'est-à-dire si $\varphi_1(Q) = 0$, on raisonne par récurrence sur Q.

On a donc $\varphi_1(X_1 - a_1) = 0$ et par conséquent $X_1 - a_1 \in I$. Le même argument appliqué à X_2 puis X_3 et ceci jusqu'à X_n montre que $X_1 - a_1, \dots, X_n - a_n \in I$. L'idéal I contient donc l'idéal $(X_1 - a_1, \dots, X_n - a_n)$ qui est maximal donc $I = (X_1 - a_1, \dots, X_n - a_n)$.

Il reste à montrer l'unicité de $(a_1, \dots, a_n) \in \mathbf{C}^n$. Elle provient du fait que les idéaux $(X_1 - a_1, \dots, X_n - a_n)$ sont maximaux. En effet si $X_1 - b_1 \in (X_1 - a_1, \dots, X_n - a_n)$ alors $(X_1 - b_1) - (X_1 - a_1) = a_1 - b_1 \in I$. Si $b_1 \neq a_1$ alors $a_1 - b_1$ est inversible et appartient à I et donc $I = \mathbf{C}[X_1, \dots, X_n]$ ce qui est absurde. Donc $b_1 = a_1$. □

COROLLAIRE. — *Soient* $P_1, \dots, P_m$ *des polynômes de* $\mathbf{C}[X_1, \dots, X_n]$. *Si le système*

$$P_1(x_1, \dots, x_n) = \cdots = P_m(x_1, \dots, x_n) = 0$$

n'a pas de solutions dans $\mathbf{C}$*, alors il existe des polynômes* $Q_1,\dots,Q_m$ *tels que*

$$1 = P_1Q_1 + \cdots + P_mQ_m.$$

Démonstration. — Soit I l'idéal engendré par $P_1,\dots,P_m$. Si $I \neq \mathbf{C}[X_1,\dots,X_n]$, alors le théorème de Krull affirme l'existence d'un idéal maximal $\mathfrak{m}$ de $\mathbf{C}[X_1,\dots,X_n]$ vérifiant $I \subset \mathfrak{m}$. D'après le théorème des zéros de Hilbert, il existe un n-uplet $(a_1,\dots,a_n) \in \mathbf{C}^n$ tel que $\mathfrak{m} = (X_1 - a_1,\dots,X_n - a_n)$. Mais alors $(a_1,\dots,a_n)$ serait une solution du système $P_j(x_1,\dots,x_n) = 0$, $1 \leqslant j \leqslant m$ ce qui est contraire à l'hypothèse ; par conséquent, $I = \mathbf{C}[X_1,\dots,X_n]$. Ainsi $1 \in I$ et il existe $Q_1,\dots,Q_m$ dans $\mathbf{C}[X_1,\dots,X_n]$ tels que $1 = P_1Q_1 + \cdots + P_mQ_m$. □

Références

[Art91] M. ARTIN – *Algebra*, Prentice Hall, 1991.

[CL01] A. CHAMBERT-LOIR – « Algèbre commutative », Polycopié de maîtrise de l'université Paris 6, disponible à l'adresse http://name.math.univ-rennes1.fr/antoine.chambert-loir/publications/teach/algcom.pdf, 2001.

[CL04] _____, « Algèbre corporelle », Polycopié de l'École Polytechnique, disponible à l'adresse http://name.math.univ-rennes1.fr/antoine.chambert-loir/publications/teach/algebre.pdf, 2004.

[Gob01] R. GOBLOT – *Algèbre commutative*, seconde éd., Dunod, 2001.

[Goz97] Y. GOZARD – *Théorie de Galois*, Ellipses, 1997.

---

9 décembre 2004

STEF GRAILLAT, Université de Perpignan, 52, avenue Paul Alduy, F-66860 Perpignan Cedex

E-mail : graillat@univ-perp.fr • *Url :* http://gala.univ-perp.fr/~graillat