Le théorème des zéros de Hilbert

Jules Besson, Eloan Rapion, sous la tutelle de Mercedes Haiech

8 décembre 2020

École Normale Supérieure de Rennes

Introduction au problème

Introduction à la géométrie algébrique

Topologie de Zariski

Le Nullstellensatz

Application à la géométrie algébrique

Pour aller plus loin : vers la géométrie algébrique moderne

Introduction au problème

David Hilbert (1862-1943)

Oscar Zariski (1899-1986)

Un théorème pilier de la géométrie algébrique

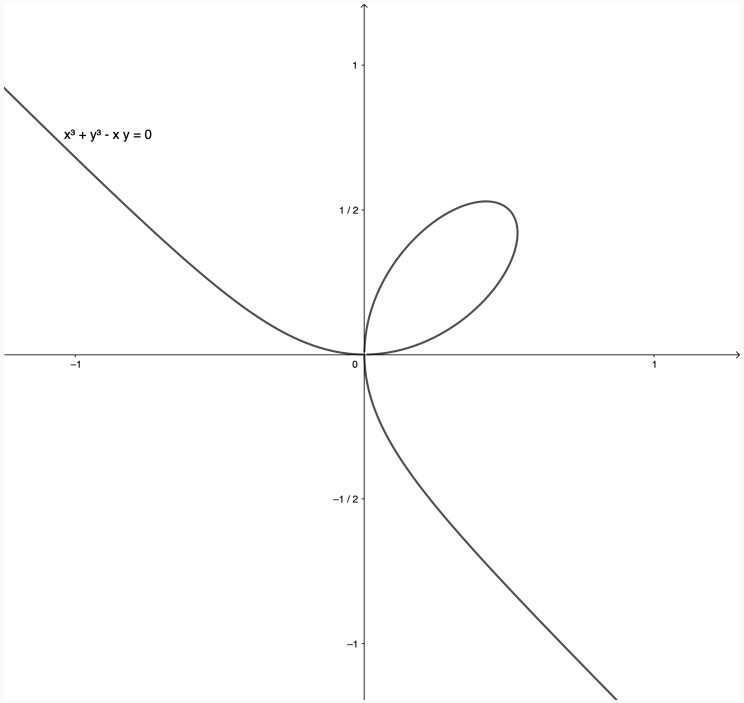
Le Nulstellensatz de Hilbert est un théorème fondamental en géométrie algébrique.

But de la géométrie algébrique : Étudier des ensembles de $\mathbb{K}^n$ décrits par une équation polynômiale.

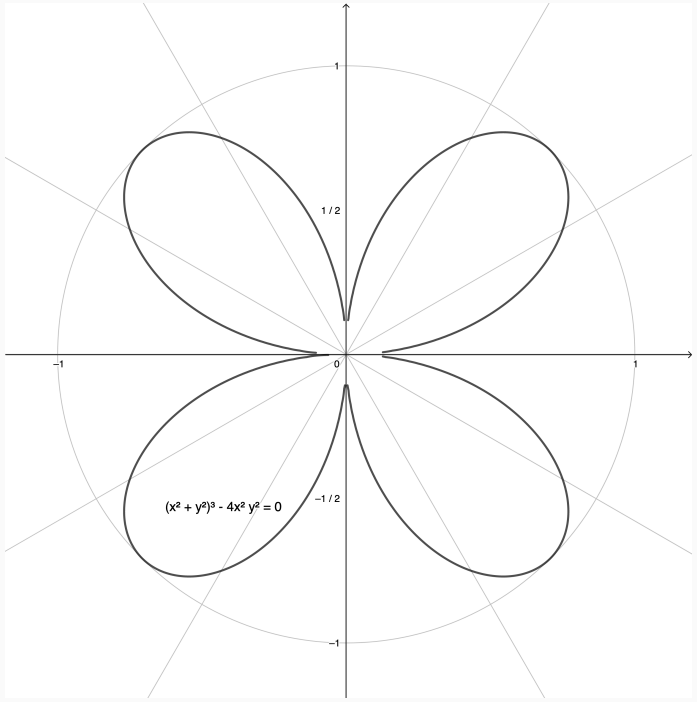
Un théorème pilier de la géométrie algébrique

Le Nulstellensatz de Hilbert est un théorème fondamental en géométrie algébrique.

But de la géométrie algébrique : Étudier des ensembles de $\mathbb{K}^n$ décrits par une équation polynômiale.



$$X^3 + Y^3 - XY = 0$$



$$(X^2 + Y^2)^3 - 4X^2Y^2 = 0$$

Motivation

Soit S un ensemble de polynômes.

$\Longrightarrow$ Une question naturelle :

Quels sont les polynômes s'annulant sur les mêmes points que les polynômes de S ?

Motivation

Soit S un ensemble de polynômes.

$\Longrightarrow$ Une question naturelle :

Quels sont les polynômes s'annulant sur les mêmes points que les polynômes de S ?

Dans $\mathbb{C}[X]$ la réponse est évidente : il faut que le polynôme soit multiple des composantes irréductibles communes à nos polynômes de base.

Que se passe-t-il avec plusieurs variables ?

Introduction à la géométrie algébrique

Pour introduire proprement le théorème, on se fixe un corps $\mathbb{K}$ algébriquement clos.

On posera $\mathscr{K}_n$ l'anneau des polynômes à n indéterminées $\mathbb{K}[X_1, \ldots X_n]$.

Pour introduire proprement le théorème, on se fixe un corps $\mathbb{K}$ algébriquement clos.

On posera $\mathscr{K}_n$ l'anneau des polynômes à n indéterminées $\mathbb{K}[X_1, \dots X_n]$.

Définition (Radical):
Soit A un anneau et I un idéal de A, on appelle *radical* de I l'ensemble

$$\sqrt{I} := \{a \in A \mid \exists n \in \mathbb{N}^*,\ a^n \in I\}$$

Remarque: Comme un corps est nécessairement intègre, on remarque que S, $\langle S \rangle$ et $\sqrt{\langle S \rangle}$ ont les même points d'annulation.

Ensemble algébrique, Idéal d'ensemble

Définition (Ensemble algébrique affine):
Soit S une partie de $\mathscr{K}_n$, on appelle *ensemble algébrique affine* de S, l'ensemble

$$V(S) := \{\alpha \in \mathbb{K}^n \mid \forall p \in S,\, p(\alpha) = 0\}$$

C'est l'ensemble des points d'annulation de tous les polynômes de S.

Définition-Proposition (Idéal d'ensemble):
Soit T une partie de $\mathbb{K}^n$, on appel *idéal* de T l'ensemble

$$\mathscr{I}(T) := \{p \in \mathscr{K}_n \mid \forall \alpha \in T,\, p(\alpha) = 0\}$$

C'est un idéal radiciel.

Avec ces deux définitions, on formule plus simplement l'ensemble recherché : $\mathscr{I}(V(S))$

Algèbre affine

Définition-Proposition (Algèbre affine):
Pour W un ensemble algébrique affine de $\mathbb{K}^n$, *l'algèbre affine* de W est l'ensemble de fonctions

$$\Gamma(W) \coloneqq \left\{ \ p : W \to \mathbb{K} \ , \ p \text{ polynômiale} \right\}$$

C'est une $\mathbb{K}$-algèbre de type fini isomorphe à $\mathscr{K}_n / \mathscr{I}(W)$.

Les algèbres affines sont une sorte de dual des ensembles algébriques affines. Autrement dit, travailler sur $\Gamma(W)$ revient à travailler sur W.

Topologie de Zariski

Définition

Les ensembles algébriques affines induisent une topologie sur $\mathbb{K}^n$.

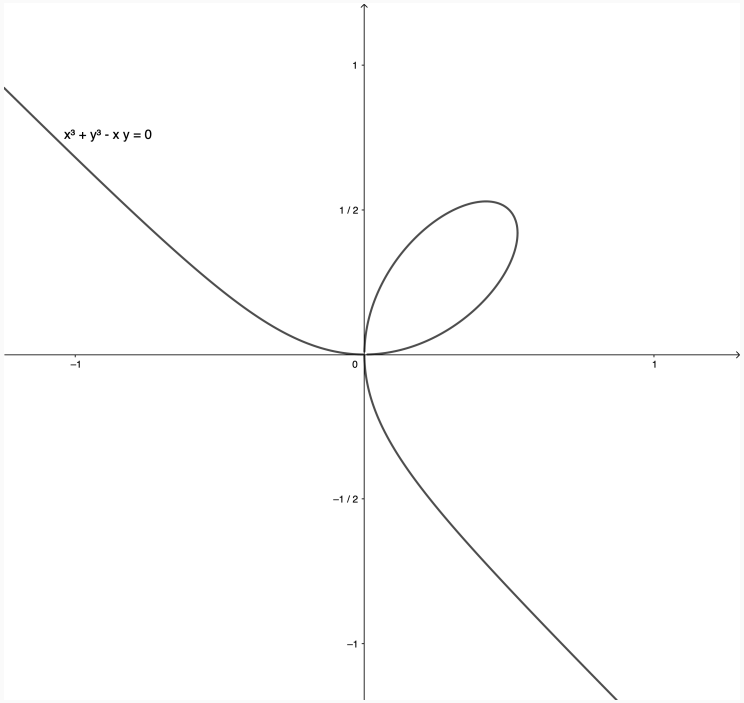
Propriété (Stabilité par intersection quelconque):

$$\bigcap_{x \in X} V(I_x) = V\left(\sum_{x \in X} I_x\right)$$

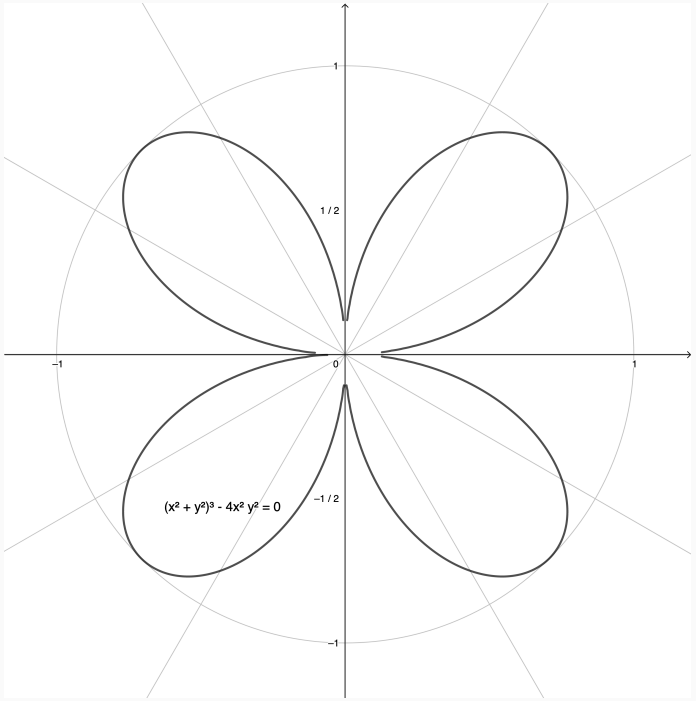
Propriété (Stabilité par union finie):

$$\bigcup_{x \in X} V(I_x) = V\left(\prod_{x \in X} I_x\right)$$

Irréductiblité

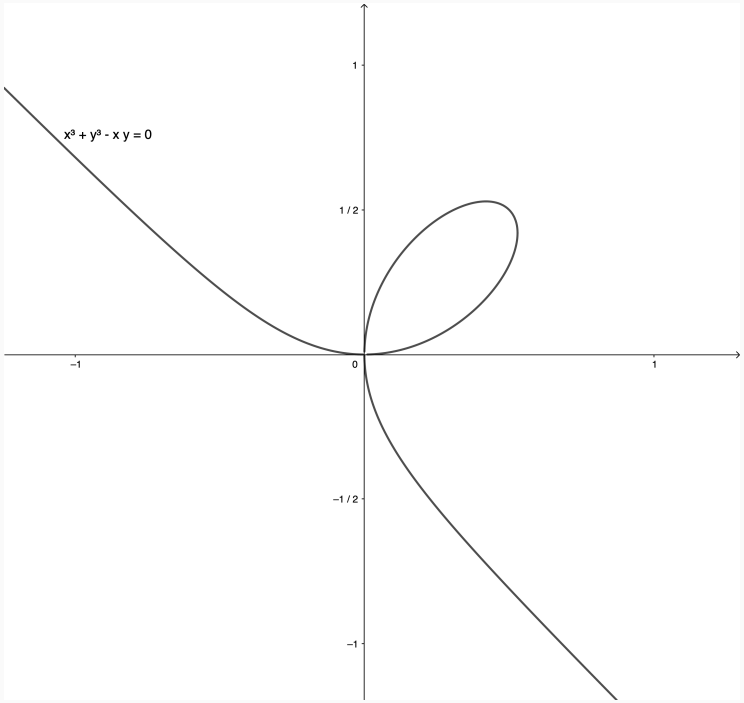


$$X^3 + Y^3 - XY = 0$$

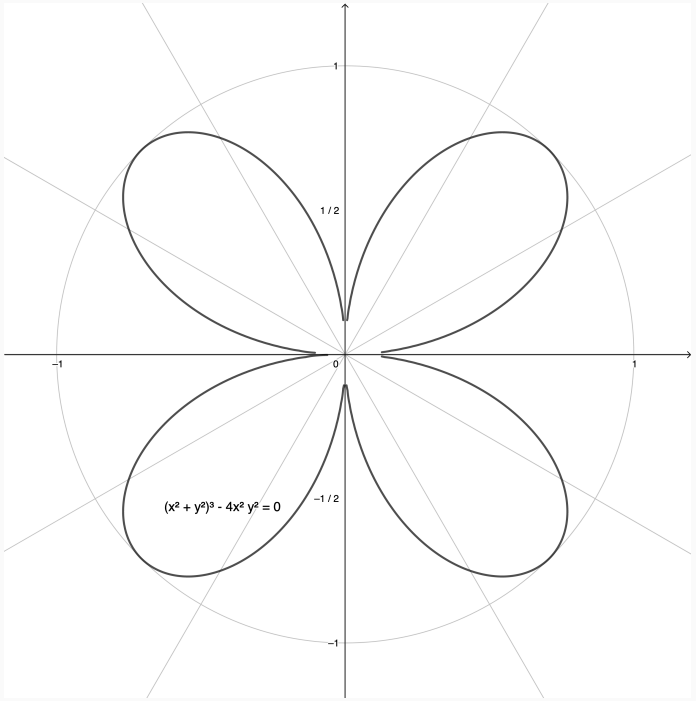


$$(X^2 + Y^2)^3 - 4X^2Y^2 = 0$$

Irréductiblité



$$X^3 + Y^3 - XY = 0$$



$$(X^2 + Y^2)^3 - 4X^2Y^2 = 0$$

Les fermés de la topologie de Zariski sont "petits".

Irréductiblité

Définition-Proposition (Espace topologique irréductible):
Soit $(X, \mathscr{T})$ un espace topologique non vide, il est dit *irréductible* s'il vérifie l'une des trois assertions équivalentes suivantes :

(i) Soit F, G deux fermés de X tels que $X = F \cup G$, alors $X = F$ ou $X = G$.

(ii) Soit U, V deux ouverts de X tels que $U \cap V = \varnothing$, alors $U = \varnothing$ ou $V = \varnothing$.

(iii) Tout ouvert non vide de X est dense.

On peut écrire un ensemble algébrique affine de manière unique comme union de fermés irréductibles sans inclusion de l'un dans un autre.

Caractérisation algébrique de l'irréductibilité

Théorème:
Soit W un ensemble algébrique affine muni de sa topologie de Zariski, alors

$$W \text{ est irréductible} \iff \mathscr{I}(W) \text{ est premier} \iff \Gamma(W) \text{ est intègre}$$

On en déduit que $\mathbb{K}^n$ est irréductible.

Prolongement des identités algébriques

Propriété:
Soit W un ensemble algébrique affine différent de $\mathbb{K}^n$ et $p \in \mathscr{K}_n$, alors si p est nul en dehors de W, c'est le polynôme nul.

Ce résultat est une généralisation des raisonnements par densité sur $\mathbb{R}$ ou $\mathbb{C}$ avec les matrices par exemple :
Toute identité polynômiale vraie sur les matrices inversibles est vraie sur toutes les matrices.

Le Nullstellensatz

Le Nullstellensatz

Le Nullstellensatz de Hilbert:
$\mathscr{H}_1$: Soit I est un idéal de $\mathscr{K}_n$, alors $\mathscr{I}(V(I)) = \sqrt{I}$.

En d'autres termes, les polynômes qui s'annulent sur les mêmes points que les zéros commun de l'idéal sont ceux qui à une certaine puissance appartiennent à cet idéal.

Le Nullstellensatz

Le Nullstellensatz de Hilbert:
$\mathscr{H}_1$: Soit I est un idéal de $\mathscr{K}_n$, alors $\mathscr{I}(V(I)) = \sqrt{I}$.

En d'autres termes, les polynômes qui s'annulent sur les mêmes points que les zéros commun de l'idéal sont ceux qui à une certaine puissance appartiennent à cet idéal.

Le Nullstellensatz faible:
$\mathscr{H}_2$: Soit I un idéal de $\mathscr{K}_n$ tel que $V(I)$ soit vide, alors $I = \mathscr{K}_n$.

Remarque: Il est évident que la version de Hilbert implique la version faible (d'où son nom) mais les deux sont équivalentes.

On remarque également l'importance de la clôture algébrique pour $\mathscr{H}_2$: par ex pour $\mathbb{R}[X]$ avec $\langle X^2 + 1 \rangle$.

Équivalence des deux versions

Preuve: $\mathbb{K}$ est intègre donc $\sqrt{I} \subset \mathscr{I}(V(I))$.

Équivalence des deux versions

Preuve: $\mathbb{K}$ est intègre donc $\sqrt{I} \subset \mathscr{I}(V(I))$.

$p \in \mathscr{I}(V(I))$

Dans $\mathscr{K}_{n+1}$: $\quad q := 1 + X_{n+1}p, \quad J := \langle I, q \rangle$.

$V(J) \subset V(I)$ et si $t \in V(I) : p(t) = 0$, alors $q(t) = 1 \neq 0$ donc $V(J) = \varnothing$

Équivalence des deux versions

Preuve: $\mathbb{K}$ est intègre donc $\sqrt{I} \subset \mathscr{I}(V(I))$.

$p \in \mathscr{I}(V(I))$

Dans $\mathscr{K}_{n+1}$: $\quad q := 1 + X_{n+1}p, \quad J := \langle I, q \rangle$.

$V(J) \subset V(I)$ et si $t \in V(I) : p(t) = 0$, alors $q(t) = 1 \neq 0$ donc $V(J) = \varnothing$

$\mathscr{H}_2 : \exists \sum_{i=1}^{k} a_i t_i + bq \in J$ (avec $a_i, b \in \mathscr{K}_{n+1}$ et $t_i \in I$) tel que $\sum_{i=1}^{k} a_i t_i + bq = 1$.

On évalue X_{n+1} en $-\frac{1}{p}$: $q = 1 - \frac{1}{p}p = 0$

$\sum_{i=1}^{l} \frac{c_i h_i}{p^{\alpha_i}} = 1$ avec $c_i \in \mathscr{K}_n$, $h_i \in I$

$m = \max\{\alpha_i, 1 \leqslant i \leqslant l\}$

$p^m = \sum_{i=1}^{l} c_i p^{m-\alpha_i} h_i \in I$, donc $\mathscr{I}(V(I)) \subset \sqrt{I}$. $\square$

Lemme de Zariski

Pour montrer $\mathscr{H}_2$, on utilise un lemme :

Lemme de Zariski version finie:
Si une algèbre de type fini sur $\mathbb{K}$ est un corps, alors c'est une extension algébrique de $\mathbb{K}$.

Preuve du lemme de Zariski

Lemme de Zariski version non dénombrable:
Supposons $\mathbb{K}$ non dénombrable et algébriquement clos, soit L une extension de corps de $\mathbb{K}$, de type fini, alors $L = \mathbb{K}$.

Preuve: Supposons L non algébrique $\Longrightarrow$ élément transcendant e

Donc on peut construire un sous corps isomorphe à $\mathbb{K}(X)$ ($X \leftrightarrow e$) inclus dans L.

Preuve du lemme de Zariski

Lemme de Zariski version non dénombrable:
Supposons $\mathbb{K}$ non dénombrable et algébriquement clos, soit L une extension de corps de $\mathbb{K}$, de type fini, alors $L = \mathbb{K}$.

Preuve: Supposons L non algébrique $\Longrightarrow$ élément transcendant e

Donc on peut construire un sous corps isomorphe à $\mathbb{K}(X)$ ($X \leftrightarrow e$) inclus dans L.

$(\frac{1}{X-c})_{c\in\mathbb{K}}$, famille non dénombrable et libre car pour $\lambda_1, \ldots, \lambda_n, c_1, \ldots, c_n \in \mathbb{K}$, si $\sum_{i=1}^{n} \frac{\lambda_i}{X-c_i} = 0$, alors pour tout entier i tel que $1 \leqslant i \leqslant n$, on multiplie par $X - c_i$, et on évalue en c_i, alors on trouve $\lambda_i = 0$.

Preuve du lemme de Zariski

Lemme de Zariski version non dénombrable:
Supposons $\mathbb{K}$ non dénombrable et algébriquement clos, soit L une extension de corps de $\mathbb{K}$, de type fini, alors $L = \mathbb{K}$.

Preuve: Supposons L non algébrique $\Longrightarrow$ élément transcendant e

Donc on peut construire un sous corps isomorphe à $\mathbb{K}(X)$ ($X \leftrightarrow e$) inclus dans L.

$(\frac{1}{X-c})_{c\in\mathbb{K}}$, famille non dénombrable et libre car pour $\lambda_1, \ldots, \lambda_n, c_1, \ldots, c_n \in \mathbb{K}$, si $\sum_{i=1}^{n} \frac{\lambda_i}{X-c_i} = 0$, alors pour tout entier i tel que $1 \leqslant i \leqslant n$, on multiplie par $X - c_i$, et on évalue en c_i, alors on trouve $\lambda_i = 0$.

C'est exclu car sinon on pourrait constituer une base non dénombrable de L, alors par égalité des cardinaux des bases, c'est absurde. $\square$

Preuve de $\mathscr{H}_2$

Le Nullstellensatz faible:
$\mathscr{H}_2$: Soit I un idéal de $\mathscr{K}_n$ tel que $V(I)$ soit vide, alors $I = \mathscr{K}_n$.

Preuve: $I \neq \langle 1 \rangle$ un idéal de $\mathscr{K}_n$

Idéal maximal le contenant M, $R := {}^{\mathscr{K}_n}\!/_M = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$

Lemme de Zariski : les α_i sont algébriques sur $\mathbb{K}$

$\mathbb{K}$ est algébriquement clos : α_i est dans $\mathbb{K}$.

$(\alpha_1, \ldots, \alpha_n)$ est un zéro de M, donc de I.

Par contraposée, $\mathscr{H}_2$ est vraie car $V(I) \neq \varnothing$. □

Application à la géométrie algébrique

Application à la géométrie algébrique

On a un lien entre l'espace topologique $\mathbb{K}^n$ et l'anneau $\mathscr{K}_n$.

Application à la géométrie algébrique

On a un lien entre l'espace topologique $\mathbb{K}^n$ et l'anneau $\mathscr{K}_n$.

- Les fermés de $\mathbb{K}^n$ sont en bijections avec les idéaux radiciels de $\mathscr{K}_n$, via les bijections décroissantes $\mathscr{I}$ et V.

Application à la géométrie algébrique

On a un lien entre l'espace topologique $\mathbb{K}^n$ et l'anneau $\mathscr{K}_n$.

- Les fermés de $\mathbb{K}^n$ sont en bijections avec les idéaux radiciels de $\mathscr{K}_n$, via les bijections décroissantes $\mathscr{I}$ et V.
- Pour $S \subset \mathbb{K}^n$, $V \circ \mathscr{I}(S) = \overline{S}$.
- Pour $S \subset \mathscr{K}_n$, $\mathscr{I} \circ V(S) = \sqrt{\langle S \rangle}$.

Application à la géométrie algébrique

On a un lien entre l'espace topologique $\mathbb{K}^n$ et l'anneau $\mathscr{K}_n$.

- Les fermés de $\mathbb{K}^n$ sont en bijections avec les idéaux radiciels de $\mathscr{K}_n$, via les bijections décroissantes $\mathscr{I}$ et V.
- Pour $S \subset \mathbb{K}^n$, $V \circ \mathscr{I}(S) = \overline{S}$.
- Pour $S \subset \mathscr{K}_n$, $\mathscr{I} \circ V(S) = \sqrt{\langle S \rangle}$.
- Enfin les points de $\mathbb{K}^n$ sont en bijection avec les idéaux maximaux de $\mathscr{K}_n$.

Application à la géométrie algébrique

On a un lien entre l'espace topologique $\mathbb{K}^n$ et l'anneau $\mathscr{K}_n$.

- Les fermés de $\mathbb{K}^n$ sont en bijections avec les idéaux radiciels de $\mathscr{K}_n$, via les bijections décroissantes $\mathscr{I}$ et V.
- Pour $S \subset \mathbb{K}^n$, $V \circ \mathscr{I}(S) = \overline{S}$.
- Pour $S \subset \mathscr{K}_n$, $\mathscr{I} \circ V(S) = \sqrt{\langle S \rangle}$.
- Enfin les points de $\mathbb{K}^n$ sont en bijection avec les idéaux maximaux de $\mathscr{K}_n$.

Nullstellensatz faible version 2:
Un idéal I de $\mathscr{K}_n$ est maximal si et seulement s'il existe un point $(a_1, \ldots, a_n) \in \mathbb{K}^n$ tel que $I = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Alors $\mathscr{K}_n/I$ est alors isomorphe à $\mathbb{K}$.

Les points de W sont en bijection avec les idéaux maximaux de $\Gamma(W)$

Pour aller plus loin : vers la géométrie algébrique moderne

$\mathscr{K}_n$	$\mathbb{K}^n \simeq \mathsf{Spm}(\mathscr{K}_n)$	$\mathbb{K}$
$\Gamma(W)$	$W \simeq \mathsf{Spm}(\Gamma(W))$	$\mathbb{K}$

$\mathscr{K}_n$	$\mathbb{K}^n \simeq \mathsf{Spm}(\mathscr{K}_n)$	$\mathbb{K}$
$\Gamma(W)$	$W \simeq \mathsf{Spm}(\Gamma(W))$	$\mathbb{K}$
A		

Géométrie algébrique moderne

$\mathscr{K}_n$	$\mathbb{K}^n \simeq \mathsf{Spm}(\mathscr{K}_n)$	$\mathbb{K}$
$\Gamma(W)$	$W \simeq \mathsf{Spm}(\Gamma(W))$	$\mathbb{K}$
A	$\mathsf{Spec}(A)$	

Géométrie algébrique moderne

$\mathscr{K}_n$	$\mathbb{K}^n \simeq \mathsf{Spm}(\mathscr{K}_n)$	$\mathbb{K}$
$\Gamma(W)$	$W \simeq \mathsf{Spm}(\Gamma(W))$	$\mathbb{K}$
A	$\mathsf{Spec}(A)$	$\kappa(x) = \mathsf{Frac}\left(A/x\right)$

Bilbiographie

Daniel Perrin.
Géométrie algébrique : Une introduction.
InterÉditions - CNRS Éditions, 1995.

Oscar Zariski.
A new proof of hilbert's nullstellensatz.
Bulletin of the American Mathematical Society, 53(4) :362–368, 1947.

Daniel Perrin.
Cours d'algèbre, 1981.

Antoine Ducros.
Introduction à la théorie des schémas, 2014.