# Une preuve du Nullstellensatz par Zariski

Jules Besson, Éloan Rapion

**Résumé**

Ce document a pour but de présenter la preuve du *Nullstellensatz* de Hilbert par Oscar Zariski. C'est un théorème fondamental en Algèbre, qui a des utilisations en géométrie algébrique.

Il a été réalisé sous la tutelle de Mercedes Haiech, doctorante à l'université de Rennes.

## Table des matières



# 1 Une introduction au problème

Les éléments d'algèbre sont issus du cours de Daniel Perrin [1], ainsi que de nos connaissances, et les éléments de géométrie algébrique proviennent du livre de Daniel Perrin [2].

## 1.1 Lemme de Zorn

On sera ammené à utiliser le lemme de Zorn, que l'on ne démontrera pas. C'est une conséquence de l'axiome du choix. Dans tout le document, les anneaux seront considérés comme commutatifs.

**Définition (Élément maximal):**
Soit $(E, \prec)$ un ensemble ordonné, $a \in E$ est un élément maximal si :

$$\forall b \in E,\ a \not\prec b$$

**Définition (Majorant):**
Soit $(E, \prec)$ un ensemble ordonné, $a \in E$ est un majorant si :

$$\forall b \in E,\ b \prec a$$

**Définition (Partie totalement ordonnée):**
Soit $(E, \prec)$ un ensemble ordonné, $S \subset E$ est une partie totalement ordonée si $\forall a, b \in S$, on a $a \prec b$ ou $b \prec a$.

**Définition (Ensemble inductif):**
Soit $E$ un ensemble ordonné. Il est dit *inductif* si toute partie totalement ordonnée admet un majorant.

**Lemme de Zorn:**
Tout ensemble inductif admet un élément maximal.

## 1.2 Résultats sur les idéaux

**Définition (Idéal propre, premier, maximal):**
Soit $A$ un anneau, $I$ un idéal de $A$.

- L'idéal $I$ est *propre* s'il est distinct de $A$.
- L'idéal $I$ est *premier* si $I$ est propre et pour tout $x, y \in A$, si $xy \in I$, alors $x \in I$ ou $y \in I$.
- L'idéal $I$ est *maximal* si $I$ est maximal pour l'inclusion parmi les idéaux propres de $A$.

**Propriété:**
Soit $A$ un anneau commutatif, $I$ un idéal de $A$. Alors l'anneau quotient $A/I$ est intègre si et seulement si $I$ est premier, et $A/I$ est un corps si et seulement si $I$ est maximal.

***Preuve:*** Soit $A$ un anneau, $I$ un idéal de $A$. Le fait que $A/I$ soit non nul équivaut au fait que $I$ soit propre. De plus comme $A$ est commutatif, $A/I$ est commutatif. On pose $\pi$ le morphisme canonique de $A$ dans $A/I$.

Supposons $I$ premier. Soit $a$ et $b$ dans $A/I$ tels que $ab = 0$, soit $x$ et $y$ des antécédants respectifs par $\pi$ (qui est surjectif). Alors $xy \in I$, et comme $I$ est premier, $x \in I$ ou $y \in I$. Par conséquent en appliquant $\pi$ : $a = 0$ ou $b = 0$, donc $A/I$ est intègre.

Réciproquement, si $A/I$ est intègre et $x, y \in A$ sont tels que $xy \in I$, il suffit d'appliquer $\pi$ et l'intégrité de $A/I$ donne le résultat attendu.

Comme $\pi$ est surjectif, il met en bijection les idéaux de $A$ contenant $I$ et les idéaux de $A/I$. Ainsi $I$ est maximal si et seulement si $A/I$ a pour seuls idéaux $A/I$ et $(0)$, donc si et seulement si $A/I$ est un corps. □

**Définition (Corps résiduel):**
Soit $A$ un anneau et $M$ un idéal maximal de $A$, alors le corps $A/M$ est appelé *corps résiduel* de $M$.

**Définition (Famille filtrante croissante):**
Soit $(S_x)_{x\in X}$ une famille d'ensembles indexée par $X$. Elle est dite *filtrante croissante* si pour tout $x$, $y$ dans $X$, il existe $z$ dans $X$ tel que $S_x$ et $S_y$ soient inclus dans $S_z$.

**Propriété:**
Soit $(I_x)_{x\in X}$ une famille filtrante croissante d'idéaux d'un anneau $A$. Alors $\bigcup_{x\in X} I_x$ est un idéal de $A$.

***Preuve:*** Il suffit de vérifier la stabilité par la somme. Soit $a, b \in \bigcup_{x\in X} I_x$, il existe $x, y \in X$ tels que $a \in I_x$, $b \in I_y$, or il existe $z \in X$ tel que $I_x, I_y \subset I_z$, donc $a + b \in I_z \subset \bigcup_{x\in X} I_x$. Donc $\bigcup_{x\in X} I_x$ est un idéal. □

**Remarque:** Cette propriété est valable pour les structures d'ensembles usuelles en algèbre et ne se limite pas aux idéaux (monoïdes, groupes, anneaux, corps...).

**Théorème (Krull):**
Soit $A$ un anneau commutatif, et $I$ un idéal propre de cet anneau, alors il existe $M$, un idéal maximal contenant $I$.

***Preuve:*** Considérons $\mathscr{J} \coloneqq \{J \text{ idéal propre de } A \mid I \subset J\}$ muni de l'inclusion pour relation d'ordre. Considérons $(J_x)_{x\in X}$ une partie totalement ordonnée de $\mathscr{J}$. Elle est filtrante croissante car pour $I_x$, $I_y$ dans cette famille, soit $I_x \subset I_y$, soit $I_y \subset I_x$. Donc $\bigcup_{x\in X} I_x$ est un idéal, il est également propre, car sinon $1 \in \bigcup_{x\in X} I_x$, donc il existe $x \in X$ tel que $1 \in I_x$, or $I_x$ est propre, c'est donc exclu, donc $\bigcup_{x\in X} I_x$ est un majorant de cette famille, donc $\mathscr{J}$ est inductif. D'après le lemme de Zorn, il admet un élément maximal $M$ et c'est un idéal maximal car il est propre, et s'il existe $N$ un idéal propre tel que $M \subsetneq N$, alors cela contredit l'hypothèse de maximalité de $M$ car $N \in \mathscr{J}$. □

**Définition (Radical):**
Soit $A$ un anneau et $S \subset A$, on appelle *radical* de $S$ l'ensemble

$$\sqrt{S} \coloneqq \{a \in A \mid \exists n \in \mathbb{N}^*, a^n \in S\}$$

**Propriété:**
Soit $I$ un idéal d'un anneau $A$. Alors $\sqrt{I}$ est un idéal de $A$.

***Preuve:*** Déjà $0 \in S \subset \sqrt{S}$. Ensuite soit $x, y \in \sqrt{S}$, avec $n, m \in \mathbb{N}$ tels que $x^n \in S$ et $y^m \in S$. Alors la formule du binôme de Newton donne $(x - y)^{n+m} =$

$\sum_{k=0}^{n+m}(-1)^{n+m-k}\binom{n+m}{k}x^k y^{n+m-k}$. Pour tout indice $k$, on a $k \geqslant n$ ou $n+m-k \geqslant m$. Ainsi chaque terme se factorise par un élément de $S$. Par conséquent $(x-y)^{n+m} \in S$, donc $x-y \in \sqrt{S}$. Enfin si $a \in A$, on a $(ax)^n = a^n x^n \in S$, donc $ax \in \sqrt{S}$. □

Exemple: Soit $\mathbb{K}$ un corps et $p \in \mathbb{K}[X]$, le radical d'un idéal $p\mathbb{K}[X]$ est $q\mathbb{K}[X]$ avec $q$ le produit des polynômes irréductibles que divisent $p$. En effet, si $n$ est la plus grande valuation de $p$, alors $p$ divise $q^n$, donc $q \in \sqrt{p\mathbb{K}[X]}$. Réciproquement, si $r \in \sqrt{p\mathbb{K}[X]}$, alors il existe $m$ tel que $p$ divise $r^m$, donc par théorème de Gauss, chaque diviseur irréductible de $p$ divise $r$, et donc $q$ divise $r$.

**Définition (Idéal radiciel):**
Un *idéal radiciel* est un idéal d'un anneau qui est son propre radical.

**Propriété:**
Le radical d'un idéal d'un anneau est radiciel.

***Preuve:*** Soit $I$ un idéal d'un anneau $A$. Soit $x \in A$ et $n \in \mathbb{N}$ tels que $x^n \in \sqrt{I}$. Alors on dispose de $m \in \mathbb{N}$ tel que $(x^n)^m \in I$. Ainsi $x^{nm} \in I$, d'où $\sqrt{\sqrt{I}} \subset \sqrt{I}$. L'inclusion réciproque est immédiate. □

## 1.3 Anneaux noethériens

**Définition-Proposition (Anneau noethérien):**
Soit $A$ un anneau, il est dit *noethérien* s'il vérifie une des trois assertions équivalentes suivantes :

(*i*) Tout idéal de $A$ est de type fini (engendré par une partie finie).

(*ii*) Toute suite croissante d'idéaux est stationnaire.

(*iii*) Tout ensemble non vide d'idéaux admet un élément maximal.

***Preuve:*** Montrons le résultat par une chaîne d'implications :

— Supposons (*i*) vraie, et considérons $(I_n)_{n\in\mathbb{N}}$ une suite d'idéaux croissante pour l'inclusion. On note $J \coloneqq \bigcup_{n\in\mathbb{N}} I_n$ Il est engendré par $(x_1, \ldots, x_n)$. On note ensuite $k = \min\{k \in \mathbb{N} \mid x_1, \ldots, x_n \in I_k\}$. Alors $J \subset I_k \subset J$, et pour tout $i \geqslant k$, $J = I_k \subset I_i \subset J$, donc la suite est stationnaire, donc (*ii*) est vérifiée.

— Supposons (*iii*) fausse, alors il existe un ensemble d'idéaux sans élément maximal. On se choisit alors un premier idéal $I_0$ de cet ensemble, puis pour tout $n \in \mathbb{N}$, on choisit $I_{n+1}$ tel que $I_n \subsetneq I_{n+1}$, c'est possible car l'ensemble n'admet pas d'élément maximal. Ainsi on a construit une suite croissante non stationnaire donc (*ii*) est fausse.

— Supposons (*iii*) vraie, et considérons $I$ un idéal de $A$, on note $\mathscr{J} \coloneqq \{J \subset I, \text{idéal de type fini}\}$. Cet ensemble d'idéaux est non vide car $\{0\} \in \mathscr{J}$, donc grâce à (iii), on exhibe alors un élément maximal $J$ de $\mathscr{J}$. $J \subset I$, et il est de type fini. Si $J \neq I$, on choisit $x \in I \setminus J$, et l'idéal $\langle J, x\rangle$ est de type fini, inclus dans $I$ ce qui contredit la maximalité de $J$, donc $J = I$, donc $I$ est de type fini, d'où (*i*). □

**Théorème (Hilbert):**
Si $A$ est un anneau noethérien, l'anneau des polynômes en une variable $A[X]$ est noethérien.

***Preuve:*** Pour $I$ un idéal de $A[X]$ et $k \in \mathbb{N}$, on pose $d_k(I)$ l'ensemble des coefficients dominants des polynômes de degré $k$ de $I$, en ajoutant 0. Comme $I$ est un idéal, on vérifie qu'il en est de même pour $d_k(I)$. On vérifie également que $d_k(I)$ est croissante en fonction de $k$ (à l'aide de la multiplication par $X$), et de $I$, pour l'inclusion.

Supposons à présent $A$ noethérien, et montrons que $A[X]$ suit la deuxième définition. Soit $(I_n)$ une suite croissante d'idéaux de $A[X]$. Comme $A$ est noethérien et que $(d_i(I_j))_{i,j\in\mathbb{N}^2}$ est une suite croissante d'idéaux de $A$, d'après $(iii)$, il existe $(l,m) \in \mathbb{N}^2$ tels que $d_l(I_m)$ soit maximal. De plus, d'après $(ii)$, on a pour tout $k \leqslant l$, il existe $n_k$ tel que $d_k(I_{n_k})$ soit majorant de $(d_k(I_n))_{n\in\mathbb{N}}$. On pose alors $N$ le maximum entre $m$ et les $n_k$.

Montrons que pour tout $k$, les suites $(d_k(I_n))_n$ sont stationnaires à partir de $N$. On pose $n \geqslant N$. Si $k \geqslant l$, on a $d_l(I_m) \subset d_k(I_m) \subset d_k(I_N) \subset d_k(I_n)$ par croissance de $d$, et il y a égalité par maximalité de $d_l(I_m)$. En particulier $d_k(I_n) \subset d_k(I_N)$. Si $k < l$, on a $d_k(I_{n_k}) \subset d_k(I_N) \subset d_k(I_n)$ par croissance de $d$, et il y a égalité par définition de $n_k$.

Déduisons-en que la suite des $I_n$ est stationnaire à partir de $N$. Soit $n \geqslant N$. On a $I_N \subset I_n$. Par l'absurde, supposons qu'il existe $p$ dans $I_n \setminus I_N$. Soit $k$ le degré de $p$, choisissons $p$ tel que $k$ soit minimal. Comme $d_k(I_N) = d_k(I_n)$, il existe $q \in I_N$ tel que $q$ est de degré $k$ de même coefficient dominant. Alors $p - q$ est dans $I_n \setminus I_N$, mais de degré strictement inférieur à $k$, ce qui est absurde. Ainsi $A[X]$ est noethérien. □

**Corollaire:**
Si $A$ est un anneau noethérien, l'anneau des polynômes à $n$ indéterminées est noethérien.

***Preuve:*** La preuve consiste à utiliser le théorème de Hilbert ci-dessus, et la définition récursive de $\mathscr{K}_n$ : $\mathscr{K}_{n+1} = \mathscr{K}_n[X_{n+1}]$. □

**Remarque:** Tout corps est noethérien car il n'a que deux idéaux ($\langle 0\rangle$ et lui-même). Par conséquent les anneaux de polynômes à un nombre fini d'interminées sur un corps sont noethériens.

## 1.4 Corps algébriquement clos

Le Nullstellensatz ne s'appliquera qu'avec l'hypothèse selon laquelle le corps considéré est algébriquement clos.

**Définition (Corps algébriquement clos):**
Un corps $\mathbb{K}$ est dit *algébriquement clos* si tout polynôme non constant de $\mathbb{K}[X]$ admet une racine dans $\mathbb{K}$.

Exemple:
- Par théorème de d'Alembert-Gauss, $\mathbb{C}$ est algébriquement clos. Par contre $\mathbb{R}$ ne l'est pas car $X^2 + 1$ n'a pas de racine.
- Aucun corps fini n'est algébriquement clos : en effet, soit $n$ le cardinal d'un corps fini. Un polynôme unitaire de degré 2 admet une racine si et seulement s'il est produit de deux polynômes unitaires de degré 1. Il y a $n$ polynômes unitaires de degré 1, donc $\binom{n}{2} + n$ soit $n\dfrac{n+1}{2}$ polynômes unitaires de degré 2 admettant une racine. Or il y a $n^2$ polynômes unitaires de degré 2, et comme $n \geq 2$, on a $n > \dfrac{n+1}{2}$ et donc il existe des polynômes sans racine.

## 1.5 Extensions de corps

Pour toute la suite, on note $\mathbb{K}$ un corps, et $\mathscr{K}_n := \mathbb{K}[X_1, \ldots, X_n]$ l'anneau des polynômes à $n$ indéterminées.

**Définition (Morphisme de corps):**
Soit $\mathbb{K}, \mathbb{L}$ deux corps, un morphisme de corps $j$ est la donnée d'une application de $\mathbb{K}$ vers $\mathbb{L}$ vérifiant les propriétés suivantes :

- $j$ est un morphisme du groupe $(\mathbb{K}, +)$ vers $(\mathbb{L}, +)$.
- $j$ induit un morphisme du groupe $(\mathbb{K}^*, \times)$ vers le groupe $(\mathbb{L}^*, \times)$.

**Propriété:**
Un morphisme de corps est injectif.

***Preuve:*** Soit $j$ un morphisme du corps $\mathbb{K}$ vers le corps $\mathbb{L}$. C'est aussi un morphisme d'anneaux, donc son noyau est un idéal, or les idéaux d'un corps sont $\{0\}$ et lui même, et l'image de $j$ n'est pas réduite à $\{0\}$, donc $\ker j = \{0\}$, donc $j$ est injectif. □

**Définition (Extension de corps):**
Une *extension* du corps $\mathbb{K}$ la donnée d'un corps $L$ et d'un morphisme non trivial $j$ de $\mathbb{K}$ dans $L$.

**Remarque:** Etant donné un morphisme d'extension $j$ de $K$ dans $L$, on peut identifier $K$ à un sous-corps de $L$ par injectivité de $j$. Dans la suite on ne précisera plus le morphisme d'extension et on raisonnera par inclusion, en gardant à l'esprit que ces extensions se font à isomorphisme de corps près.

**Définition (Algèbre engendrée, extension engendrée):**
Soit $L$ une extension de $\mathbb{K}$ et $B \subset L$.

— On appelle $\mathbb{K}$-algèbre *engendrée* par $B$ et on note $\mathbb{K}[B]$ le sous-anneau de $L$ engendré par $\mathbb{K}$ et $B$. C'est une $\mathbb{K}$-algèbre.

— On appelle extension de $\mathbb{K}$ *engendrée* par $B$ et on note $\mathbb{K}(B)$ le sous-corps de $L$ engendré par $\mathbb{K}$ et $B$. C'est une extension de $\mathbb{K}$.

**Définition (Extension de type fini):**
Une extension $L$ du corps $\mathbb{K}$ est de type fini s'il existe $B \subset L$ fini tel que $L = \mathbb{K}[B]$.

**Propriété:**
Une extension $L$ du corps $\mathbb{K}$ est de type fini si et seulement si elle est isomorphe à un quotient de $\mathscr{K}_n$ pour un entier $n$ par un de ses idéaux.

***Preuve:*** Soit $L$ une extension de $\mathbb{K}$ de type fini. Soit $(\alpha_1, \ldots, \alpha_n) \in L^n$ tel que $L = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$. On pose alors $\phi : \mathscr{K}_n \to L$ le morphisme de $\mathbb{K}$-algèbre qui à chaque $X_i$ associe $\alpha_i$. Ce morphisme est surjectif, donc par premier théorème d'isomorphisme $L \simeq {}^{\mathscr{K}_n}\!/_{\ker \phi}$.

Réciproquement, s'il existe un idéal $\mathscr{I}$ de $\mathscr{K}_n$ tel que $L \simeq {}^{\mathscr{K}_n}\!/_{\mathscr{I}}$, alors on dispose d'un morphisme surjectif $\phi : \mathscr{K}_n \to L$. Alors on a $L = \mathbb{K}[\phi(X_1), \ldots, \phi(X_n)]$ car les $X_i$ engendrent la $K$-algèbre $\mathscr{K}_n$. □

**Définition (Algébricité et transcendance):**
Soit $L$ une extension de $\mathbb{K}$ et $x \in L$, alors $x$ est dit *algébrique* sur $\mathbb{K}$ s'il existe un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ admettant $x$ comme racine, dans le cas contraire, $x$ est dit *transcendant* sur $\mathbb{K}$.

Une partie d'une extension de corps est dite *algébrique* sur $\mathbb{K}$ si tous ses éléments le sont.

**Théorème (Steinitz):**
Soit $\mathbb{K}$ un corps, alors il existe une extension algébrique de $K$ algébriquement close.

***Preuve:*** Considérons l'ensemble $\mathscr{L}$ des extension de corps de $K$, algébriques sur $K$. Montrons qu'il est inductif pour l'inclusion, afin d'appliquer le lemme de Zorn. Soit $X$ un ensemble, et $(L_x)_{x\in X}$ une famille d'éléments de $\mathscr{L}$ indexée par $X$, totalement ordonnée, montrons alors que $L \coloneqq \bigcup_{x\in X} L_x$ est un majorant de cette famille, pour cela montrons l'appartenance à $\mathscr{L}$. On a évidemment $\mathbb{K} \subset L$, et $L$ est un corps, car la famille est filtrante-croissante. Il est également algébrique sur $K$, car tout élément de $L$ appartient à un élément de $\mathscr{L}$ qui est algébrique, donc tout élément de $L$ est algébrique. Donc $L$ est un majorant de la famille, alors $\mathscr{L}$ est inductif. Par le lemme de Zorn, on exhibe un élément maximal $\mathbb{L}$ de cet ensemble. Supposons qu'il ne soit pas algébriquement clos, alors il existe un polynôme $p$ non constant à coefficients dans $\mathbb{L}$ sans racine dans ce même corps. On peut le choisir irréductible, alors l'idéal $\langle p\rangle$ est maximal, donc $\mathbb{L}[X]/\langle p\rangle$ est une extension algébrique de $K$, incluant $\mathbb{L}$, non incluse dans $\mathbb{L}$ car $p$ admet une racine dedans. Cela contredit la maximalité de $\mathbb{L}$, donc il est algébriquement clos. □

**Définition (Clôture algébrique):**
Soit $L$ une extension de corps de $\mathbb{K}$, $L$ est une clôture algébrique de $\mathbb{K}$ si elle est algébrique sur $\mathbb{K}$ et algébriquement close.

Les notions suivantes sont analogues à celles des espaces vectoriels, on cherche à algébriser ces definitions, par exemple les polynômes sont les équivalents des formes linéaires.

**Définition (Liberté algébrique):**
Soit $L$ une extension de $\mathbb{K}$, $B \subset L$, $B$ est dite *algébriquement libre* si pour toute partie finie $\{b_1, \dots b_n\} \subset B$, pour tout $p \in \mathscr{K}_n$ tel que $p(b_1, \dots, b_n) = 0$, on ait $p = 0$. Dans le cas contraire, elle est dite *algébriquement liée*.

**Définition (Génération algébrique):**
Soit $L$ une extension de $\mathbb{K}$, $B \subset L$, $B$ est dite *algébriquement génératrice* si $L$ est algébrique sur $\mathbb{K}(B)$.

**Remarque:** Dire que $B$ est génératrice revient à dire que pour tout $l \in L$, il existe une partie libre $C$ de $B$ telle que $C \cup \{l\}$ soit algébriquement liée.

**Définition (Base de transcendance):**
Soit $L$ une extension de corps, $B \subset L$, $B$ est une *base de transcendance* si elle est algébriquement libre et génératrice.

**Définition-Proposition (Degré de transcendance):**
Soit $L$ une extension de corps, il existe au moins une base de transcendance, et toutes les bases de transcendance ont le même cardinal appelé *degré de transcendance*, noté $\partial_{\mathbb{K}}(L)$.

***Preuve:*** À l'instar des bases pour les espaces vectoriels, on va utiliser le lemme de Zorn pour l'existence. Considérons $\mathscr{B} \coloneqq \{B \text{ partie libre de } L\}$ avec l'inclusion pour relation d'ordre, il est non vide car l'ensemble vide est dedans. Considérons une partie totalement ordonnée $(B_x)_{x\in X} \in \mathscr{B}^X$, montrons que $\bigcup\limits_{x\in X} B_x$ est un majorant. L'inclusion est évidente, montrons donc qu'il est libre. Soit $\{b_1,\dots,b_n\} \subset \bigcup\limits_{x\in X} B_x$ et $p \in \mathscr{K}_n$ tels que $p\,(b_1,\dots,b_n) = 0$, or pour tout entier $i$ tel que $1 \leqslant i \leqslant n$, il existe $x_i \in X$ tel que $b_i \in B_{x_i}$. En considérant le plus grand de ces ensembles pour l'inclusion que l'on notera $C$, on a $\{b_1,\dots,b_n\} \subset C$, or $C$ libre donc $p = 0$, donc $\bigcup\limits_{x\in X} B_x \in \mathscr{B}$, c'est donc un majorant, donc $\mathscr{B}$ est inductif. D'après le lemme de Zorn, on peut exhiber un élément maximal $B$. Montrons alors qu'il est générateur. Supposons qu'il ne le soit pas, alors on peut exhiber un élément $l$ transcendant dans $L$ par rapport à $\mathbb{K}(B)$, montrons alors que $B \cup \{l\}$ est encore libre. Soit $\{l, b_1,\dots,b_n\} \subset B$, $p \in \mathscr{K}_{n+1}$ tel que $p\,(b_1,\dots,b_n,l\} = 0$, alors d'après la définition récursive de $\mathscr{K}_{n+1}$, il existe une suite presque nulle de polynômes $(q_k)_{k\in\mathbb{N}} \in \mathscr{K}_n^{\mathbb{N}}$ telle que $p(X_1,\dots,X_{n+1}) = \sum\limits_{k\in\mathbb{N}} q_k(X_1,\dots,X_n)X_{n+1}^k$, alors $\sum\limits_{k\in\mathbb{N}} q_k(b_1,\dots,b_n)l^k = 0$ donc $l$ est racine d'un polynôme de $\mathbb{K}(B)$, donc $l$ est algébrique, c'est exclu. Donc $B \cup \{l\}$ est libre, or cela contredit la maximalité de $B$, donc $B$ est générateur.

Montrons maintenant l'égalité des cardinaux de deux bases algébriques.

Passons d'abord par le cas fini, et supposons que pour deux bases $B$ et $C$, $card(B) < card(C)$, on exhibe $c \in C$, et l'on construit une injection $\varphi : B \to C \setminus \{c\}$ , à l'aide de cela on construit un morphisme injectif de corps assuré par l'injectivité et la liberté des bases :

$$\begin{array}{rccc} \psi : & \mathbb{K}(B) & \longrightarrow & \mathbb{K}(C\setminus\{c\}) \\ & b & \longmapsto & \varphi(b) \end{array}$$

On en déduit un morphisme $\Psi : \mathbb{K}(B)[X] \to \mathbb{K}(C\setminus\{c\})[X]$. Comme $c \in L$, il existe $p \in (\mathbb{K}(B))[X]$ non nul tel que $p(c) = 0$, on pose alors $q \coloneqq \Psi(p) \in (\mathbb{K}(C \setminus \{c\}))[X]$ et $q(c) = 0$, ce qui est exclu car $C$ est libre, donc $card(B) \geqslant card(C)$, et par symétrie du raisonnement $card(B) = card(C)$.

Considérons maintenant le cas où $B$ est infini. Au vu du point précédent, $C$ l'est aussi. Construisons à l'aide de l'axiome du choix une fonction $f : B \to \mathscr{P}_f(C)$ qui à un point $b$ associe une partie finie $D$ de $C$ pour laquelle il soit algébrique sur $\mathbb{K}(D)$, alors en notant $A \lesssim B$ s'il existe une injection de A dans B, on a :

$$B = \bigcup_{D\in\mathscr{P}_f(C)} f^{-1}(D) \lesssim \bigsqcup_{D\in\mathscr{P}_f(C)} D \times \mathbb{N} = \mathscr{P}_f(C) \times \mathbb{N} \simeq \mathscr{P}_f(C) \simeq C$$

donc $card(B) \leqslant card(C)$ et vis-versa, donc $card(B) = card(C)$. □

## 1.6 Définitions de géométrie algébrique

Dans cette section, $\mathbb{K}$ est un corps algébriquement clos, $\mathscr{K}_n \coloneqq \mathbb{K}[X_1,\dots,X_n]$ est l'anneau des polynômes à $n$ indéterminées.

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

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

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

Exemple: Voici le graphe de deux ensembles algébriques affines pour des polynômes dans $\mathbb{K}[X, Y]$ :

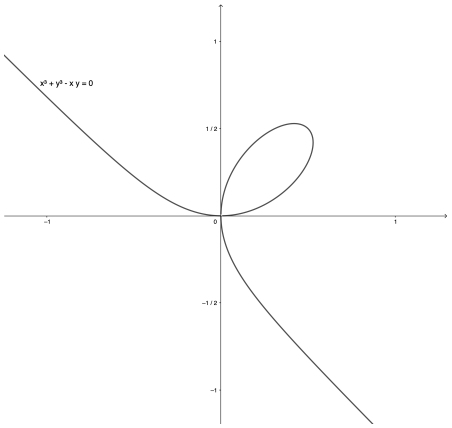


Figure 1 – $X^3 + Y^3 - XY = 0$

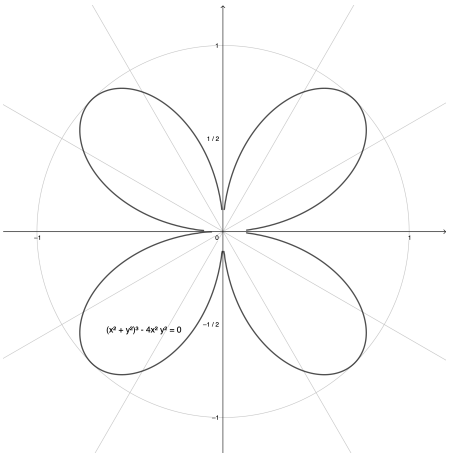


Figure 2 – $(X^2 + Y^2)^3 - 4X^2Y^2 = 0$

**Remarque:** L'application $V : \mathscr{K}_n \to \mathbb{K}^n$ est décroissante.

**Définition-Proposition (Idéal d'ensemble):**
Soit $S \subset \mathbb{K}^n$, l'idéal de $S$ est l'ensemble

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

C'est un idéal radiciel.

**Remarque:** L'application $\mathscr{I} : \mathbb{K}^n \to \mathscr{K}_n$ est décroissante.

***Preuve:*** $\mathscr{I}(S)$ est un idéal car il est le noyau du morphisme d'anneaux $r$ qui au polynôme abstrait $p \in \mathscr{K}_n$ associe la fonction polynômiale associée de $S$ dans $\mathbb{K}$. Soit $p \in \mathscr{K}_n$ et $m$ un entier naturel tel que $p^m \in \mathscr{I}(S)$. On évalue en un point $x$ de $\mathscr{K}_n$ : $p^m(x) = 0$, et comme $\mathbb{K}$ est intègre, $p(x) = 0$. Ainsi $p^m \in \mathscr{I}(S)$, donc $\mathscr{I}(S)$ est radiciel. □

**Propriété:**
Soit $W$ un ensemble algébrique affine, alors $W = V(\mathscr{I}(W))$

***Preuve:*** L'inclusion $W \subset V(\mathscr{I}(W))$ est évidente, maintenant il existe $I$ un idéal tel que $W = V(I)$, or $I \subset \mathscr{I}(W)$, donc par décroissance de $V$, $V(\mathscr{I}(W)) \subset W$. □

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

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

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

***Preuve:*** Il suffit de considérer encore une fois $r$ de la preuve précédente, alors $\operatorname{Im} r \simeq \mathscr{K}_n / \ker r$, soit $\Gamma(S) \simeq \mathscr{K}_n / \mathscr{I}(S)$. C'est une $\mathbb{K}$-algèbre car c'est un espace de fonction dont l'espace d'arrivée est $\mathbb{K}$, et de type fini car quotient de $\mathscr{K}_n$. □

# 2 Preuve du Nullstellensatz

Le théorème de Hilbert est essentiel en géométrie algébrique, car on utilise la topologie de Zariski qui est caractérisée par les ensembles algébriques $V(I)$, avec $I$ un idéal de $\mathscr{K}_n$, qui constituent la famille des fermés. Si l'on observe les idéaux de ces ensembles, on peut obtenir des informations sur l'irréductibilité de certains ensembles. Cela permet par exemple de développer des résutats par densité dans $\mathscr{M}_n(\mathbb{K})$ : une identité vraie sur les matrices inversibles est valable pour toutes (voir 3.3).

Dans toute la suite, $\mathbb{K}$ est un corps algébriquement clos, $\mathscr{K}_n \coloneqq \mathbb{K}[X_1, \dots, X_n]$ est l'anneau des polynômes à $n$ indéterminées.

Le déroulement de la preuve suit le papier publié par Oscar Zariski [3], et le Lemme de Zariski version non-dénombrable est issu du livre de Daniel Perrin [2]

## 2.1 Énoncés du théorème des zéros de Hilbert

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

Ce théorème (démontré par la suite) nous donne de grandes informations également sur l'idéal $I$. En effet, il est naturel de se demander quels autres polynômes s'annulent sur les mêmes points que ceux de l'idéal $I$. Il permet en quelque sorte de calculer la "clôture polynômiale" de l'idéal $I$. Pour le démontrer, on passe par une formulation à l'apparence plus faible, mais équivalente.

**Le Nullstellensatz faible:**
$\mathscr{H}_2$ : Soit $I$ un idéal de $\mathscr{K}_n$ tel que $V(I)$ soit vide, alors $I$ est l'idéal engendré par l'unité.

**Remarque:** Si $\mathbb{K}$ n'est pas algébriquement clos, le Nullstellensatz est toujours faux, même en version faible. En effet, il existe alors un polynôme $p$ non constant à une indéterminée qui n'admet pas de racine. On considère que $p \in \mathscr{K}_n$ en assimilant l'indéterminée de $p$ à le première indéterminée de $\mathscr{K}_n$. Alors $V(\langle p \rangle)$ est vide, pourtant $\langle p \rangle$ est distinct de $\mathscr{K}_n$.

**Lemme:**
Le Nullstellensatz de Hilbert et le Nullstellensatz faible sont équivalents.

***Preuve:*** (De Rabinovitch) Procédons par double implication.

On suppose $\mathscr{H}_1$. Soit $I$ un idéal de $\mathscr{K}_n$ tel que $V(I) = \varnothing$, alors $\mathscr{I}(V(I)) = \mathscr{K}_n$, donc $\sqrt{I} = \mathscr{K}_n$, i.e. $I = \mathscr{K}_n = \langle 1 \rangle$, d'où $\mathscr{H}_2$.

On suppose $\mathscr{H}_2$. Comme $\mathbb{K}$ est intègre, il est évident que $\sqrt{I} \subset \mathscr{I}(V(I))$. Soit $I$ un idéal de $\mathscr{K}_n$. Considérons $X_{n+1}$ une indéterminée supplémentaire pour travailler dans $\mathscr{K}_{n+1}$, et $p$ un polynôme de $\mathscr{K}_n$ s'annulant sur $V(I)$. On pose alors le polynôme $q \coloneqq 1 + X_{n+1}p$, et l'idéal de $\mathscr{K}_{n+1}$ $J \coloneqq \langle I, q\rangle$. On a alors $V(J) = \varnothing$, car $V(J) \subset V(I)$, donc un élément de $V(J)$ annule $p$, donc n'annule pas $q$. On peut donc utiliser l'hypothèse de $\mathscr{H}_2$, soit il existe $\sum_{i=1}^{k} a_i t_i + bq \in J$ tel que $\sum_{i=1}^{k} a_i t_i + bq = 1$ (la somme avec les élément $t_i$ de $I$ est explicitée car les $a_i$ ne sont plus dans $\mathscr{K}_n$, mais $\mathscr{K}_{n+1}$. On remplace alors l'indéterminée $X_{n+1}$ par $-\frac{1}{p}$, alors $q\left(\frac{1}{p}\right) = 1 - \frac{1}{p}p = 0$, ce qui laisse une égalité dans le corps des fractions à $n$ indéterminées du type $\sum_{i=1}^{l} \frac{c_i h_i}{p^{\alpha_i}} = 1$ avec $c_i \in \mathscr{K}_n$, $h_i \in I$ et $\alpha_i \in \mathbb{N}$. On pose alors $m = \max\{\alpha_i, 1 \leqslant i \leqslant l\}$ et on a en multipliant par $p^m$ une égalité du type $\sum_{i=1}^{l} c_i p^{m-\alpha_i} h_i = p^m$, donc $p^m \in I$, donc $\mathscr{I}(V(I)) \subset \sqrt{I}$. Ainsi on a $\mathscr{H}_1$. □

## 2.2 Lemme de Zariski

Dans son article, Zariski démontre le Nullstellensatz à partir du lemme qui porte désormais son nom.

> **Lemme de Zariski version non dénombrable:**
> Supposons $\mathbb{K}$ non dénombrable et algébriquement clos, soit $L$ une extension de corps de $\mathbb{K}$, de dimension au plus dénombrable, alors $L = \mathbb{K}$.

***Preuve:*** La clef est de montrer que $L$ est algébrique, car s'il l'est, pour tout $a \in L$, il existe $p \in \mathbb{K}[X]$ irréductible tel que $p(a) = 0$. Comme $\mathbb{K}$ est algébriquement clos, $p$ est scindé dans $\mathbb{K}[X]$, donc par théorème de Gauss, $X - a$ divise un $X - b$ avec $b \in \mathbb{K}$. en évaluant en $a$, on a $a = b$, donc $a \in \mathbb{K}$.

Supposons $L$ non algébrique, alors il admet un élément transcendant, donc on peut construire un sous corps isomorphe à $\mathbb{K}(X)$ inclus dans $L$. Considérons (à isomorphisme près) la famille des $(\frac{1}{X-c})_{c\in\mathbb{K}}$, cette famille est 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. □

**Remarque:** Ici la non dénombrabilité de $\mathbb{K}$ est problématique, par exemple pour le corps $\mathbb{Q}$ dont l'étude des algébriques et des transcendants est fort utile, Zariski dans son papier utilise une version différente : l'hypothèse de cardinalité du corps de base a disparu, mais l'algèbre doit être de type fini.

> **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:*** On montre le résultat par récurrence sur le nombre minimal de générateur d'une algèbre $\mathscr{R}$ de type fini. Si ce nombre est 1, soit $\xi$ un générateur de $\mathscr{R}$. Alors $\frac{1}{\xi}$ est un polynôme en $\xi$ à coefficients dans $\mathbb{K}$. Appelons $f$ ce polynôme : $\xi$ est racine de $Xf - 1$.

Supposons la propriété vraie au rang $n-1$ (pour $n \geqslant 2$). Supposons l'algèbre $\mathscr{R}$ engendrée par $\xi_1$, ..., $\xi_n$. D'après l'hypothèse de récurence, $\mathscr{R}$ est une extension algébrique de $\mathbb{K}(\xi_1)$. Montrons à présent que $\xi_1$ est algébrique sur $\mathbb{K}$.

Chaque élément $\omega$ de $\mathbb{K}(\xi_1)$ s'écrit sous la forme $st^{-1}$ avec $s$ et $t$ dans $\mathbb{K}[\xi_1]$ et $t$ non nul. On appellera $t$ un dénominateur de $\omega$. Chacun des $\xi_i$ (pour $i$ entre 2 et $n$) est racine d'un polynôme $f_i$ à coefficients dans $\mathbb{K}(\xi_1)$. Quitte à les multiplier par le produit de dénominateurs de chaque coefficient, on peut les supposer à coefficients dans $\mathbb{K}[\xi_1]$. On note $b_i$ leur coefficient dominant et $m_i$ leur degré.

Soit $\omega \in R$. Alors $\omega$ s'écrit sous le forme d'une somme presque nulle $\sum_{j \in \mathbb{N}^{n-1}} \lambda_j \xi^j$, avec les $\lambda_j$ des coefficients dans $\mathbb{K}[\xi_1]$, et $\xi^j$ signifiant le produit des $\xi_i$ à la puissance correspondante dans le multi-indice. On pose alors $\rho$ un entier tel que pour tous les $j$ correspondant à un terme non nul et tous les $i$, on ait $j_i \leqslant m_i + \rho - 1$. On pose alors $\omega' = \omega(b_2 \dots b_n)^\rho$.

On peut écrire $\omega'$ comme une combinaison linéaire à coefficients dans $\mathbb{K}[\xi_1]$ des $\xi^j$ avec $j$ parcourant le produit cartésien $\prod_{i=2}^{n} [\![0, m_i - 1]\!]$. En effet, si on a un terme non nul dans la décomposition de $\omega$ avec un $i$ tel que $j_i \geqslant m_i$, alors $(b_2 \dots b_n)^\rho \xi_i^{j_i} = (b_2 \dots b_n)^\rho b_i^{\rho-1} \xi_i^{j_i - m_i} (b_i \xi_i^{m_i} - f_i(\xi_i))$ ce qui diminue $j_i$ de 1, et par choix de $\rho$ on peut répéter ainsi jusqu'à ce que tous les $j_i$ soient inférieurs à $m_i - 1$.

Soit $\nu$ le degré de l'extension $\mathscr{R}$ comme $\mathbb{K}(\xi_1)$-espace vectoriel. Par théorème de la base incomplète, il admet une base 1, $\omega_2$, ..., $\omega_\nu$. Pour chaque $j$ dans $\prod_{i=2}^{n} [\![0, m_i - 1]\!]$, le coefficient de 1 de la décomposition de $\xi^j$ dans cette base admet un dénominateur. On pose $b_1$ le produit sur tous les $j$ de ces dénominateurs. Ainsi pour tout $j$, la décomposition de $\xi^j$ a un coefficent de 1 dans $\mathbb{K}[\xi_1]$.

Finalement, on pose $b$ le produit de $b_1$ et des $b_i$ définis précédemment. On a $b \in \mathbb{K}[\xi_1]$. Soit alors $\zeta \in \mathbb{K}[\xi_1]$. On définit $\rho$ comme précédamment, à partir de $\omega = \frac{1}{\zeta}$. On pose $\rho'$ le maximum entre 1 et $\rho$ (il conserve la propriété définissant $\rho$). Alors on pose $e = \frac{b^{\rho'}}{\zeta}$, et on a $e \in \mathbb{K}(\xi_1)$ donc $e$ est égal à son coefficient de 1 dans la base 1, $\omega_2$, ..., $\omega_\nu$. Alors :

$$\begin{aligned} e &= b_1 \sum_j \lambda_j \xi^j \\ &= \sum_j \lambda_j b_1 \xi^j \\ &= \sum_j \lambda_j (a_{1j} + a_{2j}\omega_2 + \dots + a_{\nu j}\omega_\nu) \\ &= \sum_j \lambda_j a_{1j} + \left(\textstyle\sum_j \lambda_j a_{2j}\right) \omega_2 + \dots + \left(\textstyle\sum_j \lambda_j a_{\nu j}\right) \omega_\nu \\ &= \sum_j \lambda_j a_{1j} \end{aligned}$$

Par définition de $\rho'$ et de $b_1$, on a $\lambda_j a_{1j}$ dans $\mathbb{K}[\xi_1]$ pour tout $j$ dans la somme, et donc $e \in \mathbb{K}[\xi_1]$. Ainsi $b^{\rho'}$ est multiple de $\xi$ dans $e \in \mathbb{K}[\xi_1]$.

Finalement, supposons $\xi_1$ transcendant sur $\mathbb{K}$. Alors $\mathbb{K}[\xi_1]$ est isomorphe à un anneau de polynômes. Comme tous élément divise une puissance de $b$, en particulier c'est le cas de tout polynôme irréductible, donc par théorème de Gauss, tout polynôme irréductible divise $b$. c'est absurde car il y a une infinité de polynôme irréductible. Ainsi $\xi_1$ est algébrique sur $\mathbb{K}$. On pose $(x_k)_k$ une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\xi_1]$.

Montrons que chacun des $\xi_i$ ($1 \leqslant i \leqslant n$) est algébrique sur $\mathbb{K}$. On en choisit un et on pose $(y_l)_l$ une base du $\mathbb{K}[\xi_1]$-espace vectoriel $\mathbb{K}[\xi_1][\xi_i]$. Alors $(x_k y_l)_{k,l}$ est une base

du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\xi_1, \xi_i]$. Il est donc de dimension finie, donc $\xi_i$ est algébrique sur $\mathbb{K}$. □

Avec les résultats que l'on a, nous sommes maintenant en mesure de prouver le Nullstellensatz faible, et par conséquent le Nullstellensatz de Hilbert :

***Preuve:*** Montrons que l'assertion $\mathscr{H}_2$ est vérifiée. Soit $I \neq \langle 1 \rangle$ un idéal de $\mathscr{K}_n$, il admet un idéal maximal le contenant $M$. On pose le corps résiduel $R := {}^{\mathscr{K}_n}\!/_M = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$. D'après le lemme de Zariski, on sait que les $\alpha_i$, $1 \leqslant i \leqslant n$ sont algébriques sur $\mathbb{K}$. Comme $\mathbb{K}$ est algébriquement clos, chaque $\alpha_i$ est dans $\mathbb{K}$. Le point $(\alpha_1, \ldots, \alpha_n)$ est alors un zéro de $M$, et donc de $I$. Par contraposée, $\mathscr{H}_2$ est vraie. □

## 2.3 Application

Le Nullstellensatz a les corollaires suivant en géométrie algébrique :

**Corollaire:**
Si $\mathbb{K}$ est algébriquement clos, la fonction $\mathscr{I}$ est une bijection décroissante entre les ensembles algébriques affines de $\mathbb{K}^n$ et les idéaux radiciels de $\mathscr{K}_n$, de bijection réciproque décroissante $V$.

***Preuve:*** Soit $I$ un idéal radiciel. Alors $\mathscr{I}(V(I)) = \sqrt{I}$ d'après le Nullstellensatz, et $\sqrt{I} = I$ car $I$ est radiciel. Ainsi $I = \mathscr{I}(V(I))$. Réciproquement, on a déjà montré $W = V(\mathscr{I}(W))$ pour tout ensemble algébrique affine $W$. Enfin, la décroissance de $\mathscr{I}$ et $V$ on déjà été évoquées précédemment. □

**Corollaire:**
Si $S \subset \mathbb{K}^n$, $V(\mathscr{I}(S)) = \overline{S}$. Si $S \subset \mathscr{K}_n$, $\mathscr{I}(V(S)) = \sqrt{\langle S \rangle}$.

***Preuve:*** Par croissance de $V \circ \mathscr{I}$ et comme $\overline{S}$ en est un point fixe par la corollaire précédant, on a $V(\mathscr{I}(S)) \subset \overline{S}$. De plus $S \subset V(\mathscr{I}(S))$, et $V(\mathscr{I}(S))$ est fermé, d'où l'inclusion réciproque. L'autre proposition se traite de la même manière, la fonction $\sqrt{\langle \cdot \rangle}$ ayant des propriété similaires à l'adhérence. □

**Corollaire:**
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 $I = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Le corps résiduel de $I$ est alors isomorphe à $\mathbb{K}$.

***Preuve:*** Soit $(a_1, \ldots, a_n) \in \mathbb{K}^n$, montrons $\mathscr{K}_n / \langle X_1 - a_1, \ldots, X_n - a_n \rangle \simeq \mathbb{K}$. On pose :

$$\begin{array}{rccc} f: & \mathscr{K}_n & \to & \mathbb{K} \\ & P & \mapsto & P(a_1, \ldots, a_n) \end{array}$$

Soit $P \in \ker(f)$. Montrons par récurrence descendante que pour tout $0 \leq i \leq n$, $P \in \langle X_1 - a_1, \ldots, X_n - a_n \rangle + \mathbb{K}[X_1, \ldots, X_i]$. On initialise avec $i = n$, $P = 0 + P$. Supposons que pour $1 \leq i \leq n$, on ait $P = I + Q$ avec $I \in \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ et $Q \in \mathbb{K}[X_1, \ldots, X_i]$. Alors dans $\mathbb{K}[X_1, \ldots, X_{i-1}][X_i]$, on peut faire la division euclidienne de $Q$ par $X_i - a_i$ (de coefficient dominant inversible) : $Q = (X_i - a_i)R + S$ avec $S \in \mathbb{K}[X_1, \ldots, X_{i-1}]$. Ainsi $P = I + (X_i - a_i)R + S$ avec $I + (X_i - a_i)R \in I$ et $S \in \mathbb{K}[X_1, \ldots, X_{i-1}]$, ce qui termine la récurrence.

En particulier, pour $i = 0$, on a $P = I + q$ avec $I \in \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ et $q \in \mathbb{K}$. On évalue en $(a_1, \ldots, a_n)$ : $0 = 0 + q$, d'où $q = 0$ et $P \in \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Ainsi $\ker(f) \subset \langle X_1 - a_1, \ldots, X_n - a_n \rangle$, et l'autre inclusion est immédiate. Enfin,

avec les polynômes constants, $f$ est surjective. Le premier théorème d'isomorphisme donne alors $\mathscr{K}_n/\langle X_1 - a_1, \ldots, X_n - a_n\rangle \simeq \mathbb{K}$. Comme $\mathbb{K}$ est un corps, l'idéal $\langle X_1 - a_1, \ldots, X_n - a_n\rangle$ est maximal.

Réciproquement, un idéal maximal est premier, donc radiciel. D'après le premier corollaire, un idéal radiciel $I$ est maximal si et seulement si $V(I)$ est minimal sans être vide, autrement dit si c'est un singleton (tous les singletons étant fermés). Par conséquent, un idéal est maximal si et seulement s'il est l'image par $\mathscr{I}$ d'un singleton $\{(a_1, \ldots, a_n)\}$. Or $\langle X_1 - a_1, \ldots, X_n - a_n\rangle \subset \mathscr{I}(\{(a_1, \ldots, a_n)\})$, et comme le premier idéal est maximal et le second propre, il y a égalité. □

Grace à ce corollaire, on peut identifier l'ensemble des idéaux maximaux de $\mathscr{K}_n$ à $\mathbb{K}^n$ (ce qui servira dans la dernière partie). De plus, si $W$ est un ensemble algébrique affine, par le morphisme surjectif de passage au quotient par $\mathscr{I}(W)$, on peut identifier les idéaux maximaux de $\mathscr{K}_n$ contenant $\mathscr{I}(W)$ et les idéaux maximaux de $\Gamma(W)$. Ainsi, par décroissance de $V$, les idéaux maximaux de $\Gamma(W)$ sont en bijection avec les points de $W$.

# 3 Bases de géométrie algébrique classique

Dans cette section, on s'inspire principalement du livre de Daniel Perrin [2]

## 3.1 Topologie de Zariski

L'application $V$ qui à un idéal associe son ensemble algébrique affine vérifie des propriétés similaires aux morphismes de monoïdes qui s'avèreront utiles pour définir une topologie sur $\mathbb{K}^n$.

**Propriété:**
Soit $S$ une partie de $\mathscr{K}_n$, alors l'ensemble algébrique de $S$ est le même que celui de son idéal engendré, i.e.

$$V(S) = V(\langle S\rangle)$$

***Preuve:*** On a $S \subset \langle S\rangle \subset \mathscr{I}(V(S))$, et $V(S) = V(\mathscr{I}(V(S)))$, donc par monotonie de $V$, $V(S) = V(\langle S\rangle)$. □

**Propriété (Stabilité par intersection quelconque):**
Soit $X$ un ensemble, et $(S_x)_{x\in X}$ une famille de parties de $\mathscr{K}_n$ indexée par $X$, alors :

$$\bigcap_{x\in X} V(S_x) = V\left(\bigcup_{x\in X} S_x\right)$$

Pour toute famille d'idéaux indexée par $X$, $(I_x)_{x\in X}$, on a donc :

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

***Preuve:*** Soit $y \in \mathbb{K}^n$, $y \in \bigcap_{x\in X} V(S_x) \iff \forall x \in X,\, y \in V(S_x)$ □

$$\begin{aligned} &\iff \forall x \in X,\, \forall p \in S_x,\, p(y) = 0 \\ &\iff \forall p \in \bigcup_{x\in X} S_x,\, p(y) = 0 \\ &\iff y \in V\left(\bigcup_{x\in X} S_x\right) \end{aligned}$$

**Propriété (Stabilité par union finie):**
Soit $X$ un ensemble fini, et $(I_x)_{x\in X}$ une famille d'idéaux de $\mathscr{K}_n$ indexée par $X$, alors :

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

***Preuve:*** La preuve se fait avec deux idéaux $I$ et $J$, après il suffit de raisonner par récurrence.

La première inclusion est directe car $IJ \subset I, J$, donc par décroissance de $V$, on a $V(I), V(J) \subset V(IJ)$, donc $V(I) \cup V(J) \subset V(IJ)$.

Soit $y \in V(IJ)$, supposons que $y \notin V(I)$, alors il existe $p \in I$ tel que $p(y) \neq 0$, or pour tout $q \in J$, $p(y)q(y) = 0$, donc pour tout $q \in J$, $q(y) = 0$ par intégrité du corps $\mathbb{K}$. Donc $y \in V(J)$, donc $V(IJ) \subset V(I) \cup V(J)$. □

**Définition (Topologie de Zariski):**
Les propositions ci dessus nous montrent que l'ensemble $\{V(I),\, I \text{ idéal de } \mathscr{K}_n\}$ forme l'ensemble des fermés pour une topologie sur $\mathbb{K}^n$, on l'appelle *topologie de Zariski*.

**Remarque:** Les fermés de cette topologie sont très petits, et permettront de montrer des résultats par densité, en effet, $\mathbb{K}^n$ muni de cette topologie est un ensemble irréductible, ce qui nous ammène à la partie suivante.

**Propriété:**
Les polynômes sont des applications continues de $\mathbb{K}^n$ dans $\mathbb{K}$, munis de leurs topologies de Zariski.

***Preuve:*** Soit $p \in \mathscr{K}_n$, on considère un fermé $\{x_1, \ldots, x_r\}$ de $\mathbb{K}$. On remarque que cela revient au même d'étudier le résultat pour un singleton car les fermés sont stables par union finie. On considère donc $x \in \mathbb{K}$, $p^{-1}(\{x\}) = \{y \in \mathbb{K}^n \mid p(y) = x\} = \{y \in \mathbb{K}^n \mid (p - x)(y) = 0\} = V(p)$, c'est donc un fermé. Donc $p$ est continu. □

**Remarque:** La topologie de Zariski est la moins fine telle que les polynômes soient continus en munissant $\mathbb{K}$ de la topologie cofinie.

## 3.2 Irréductibilité

**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.

**Remarque:** Dans les topologies irréductibles, on voit qu'à l'instar de la topologie de Zariski, les fermés sont très "petits" et les ouverts très "grands", ce n'est pas le cas des toplogies usuelles, comme les topologies métriques et plus généralement les espaces séparés.

***Preuve:*** Les deux premières assertions sont directement équivalentes par passage au complémentaire, il suffit alors de montrer $(ii) \Leftrightarrow (iii)$.

$(ii) \Rightarrow (iii)$ : Soit $U$ un ouvert non vide de $X$, alors pour tout ouvert non vide $V$, $U \cap V \neq \varnothing$ d'après $(ii)$, donc $U$ est dense.

$(iii) \Rightarrow (ii)$ : Soit $U, V$ deux ouverts tels que $U \cap V = \varnothing$, supposons $U \neq \varnothing$, alors $U$ est dense, donc si $V \neq \varnothing$, alors $U \cap V \neq \varnothing$, ce qui est exclu, donc $V = \varnothing$. □

**Théorème (Caractérisation algébrique de l'irréductibilité):**
Soit W un ensemble algébrique affine muni de sa topologie de Zariski, alors

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

**Remarque:** On pase ici d'une caractérisation géométrique à une propriété algébrique, c'est là l'essence de la géométrie algébrique.

***Preuve:*** La deuxième équivalence est directe, montrons donc la première, $(i) \Leftrightarrow (ii)$.

$(i) \Rightarrow (ii)$ : Soit $W$ un ensemble algébrique affine irréductible, et $p, q \in \mathscr{K}_n$ tels que $pq \in \mathscr{I}(W)$, alors on a $W = V(\mathscr{I}(W)) \subset V(p) \cup V(q)$. Donc $W = (V(p) \cap W) \cup (V(q) \cap W)$, donc $W$ irréductible est union de deux fermés, donc $W = V(p) \cap W \subset V(p)$ ou $W = V(q) \cap W \subset V(q)$, donc $p \in \mathscr{I}(W)$ ou $q \in \mathscr{I}(W)$.

$(ii) \Rightarrow (i)$ : Soit $W$ un ensemble algébrique affine tel que $\mathscr{I}(W)$ soit premier. Soit $V_1, V_2$ deux fermés de $W$ tels que $W = V_1 \cup V_2$, si $V_1 \neq W$, alors $\mathscr{I}(W) \subsetneq \mathscr{I}(V_1)$, donc on choisit $p_1 \in \mathscr{I}(V_1) \setminus \mathscr{I}(W)$. De même en supposant $V_2 \neq W$, on choisit $p_2 \in \mathscr{I}(V_2) \setminus \mathscr{I}(W)$. On a $P_1 p_2$ nul sur $W$, donc dans $\mathscr{I}(W)$, il y a donc une contradiction, donc $V_1 = W$ ou $V_2 = W$, d'où $(i)$. □

**Propriété:**
Si $\mathbb{K}$ est infini, l'espace $\mathscr{K}_n$ est irréductible.

***Preuve:*** Suposons $\mathbb{K}$ infini. Montrons $\mathscr{I}(\mathbb{K}^n) = \langle 0 \rangle$, par récurrence sur $n$.

Pour $n = 1$, tout polynôme non nul a un nombre fini de racine. Comme $\mathbb{K}$ est infini, on en déduit $\mathscr{I}(\mathbb{K}) = \langle 0 \rangle$.

Supposons le résultat vrai pour $\mathbb{K}^{n-1}$ avec $n$ un entier naturel non nul. Soit $p \in \mathscr{K}_n$ non constant, montrons qu'il existe un point de $\mathbb{K}^n$ où $p$ ne s'annule pas. Considérant $p$ comme un élément de $\mathbb{K}[X_1, \ldots, X_{n-1}][X_n]$, le coefficient dominant de $p$ est un polynôme non nul de $\mathbb{K}[X_1, \ldots, X_{n-1}]$. Par hypothèse de récurrence, il existe un point de $\mathbb{K}^{n-1}$ où il ne s'annule pas. On évalue les indéterminées $X_1, \ldots, X_{n-1}$ en ce point pour finalement obtenir un polynôme non constant en $X_n$. Avec le cas $n = 1$, on peut fixer la dernière coordonnée pour avoir un point de $\mathbb{K}^n$ où $p$ ne s'annule pas.

Ainsi pour tout entier naturel non nul $n$, on a $\mathscr{I}(\mathbb{K}^n) = \langle 0 \rangle$. Ainsi $\Gamma(\mathbb{K}^n) = \mathscr{K}_n$, qui est intègre car $\mathbb{K}$ est un corps, donc $\mathbb{K}^n$ est irréductible. □

Exemple: Montrons que si $\mathbb{K}$ est infini, l'ensemble algébrique affine $V(\langle X^2 - Y^3 \rangle)$ est irréductible. Pour cela, on considère le morphisme $\phi$ de $\mathbb{K}$-algèbre de $\mathbb{K}[X, Y]$ dans $\mathbb{K}[T]$ qui à $X$ associe $T^3$ et à $Y$ associe $T^2$. Alors $X^2 - Y^3$ est dans le noyau de $\phi$, par conséquent $\langle X^2 - Y^3 \rangle$ également.

Réciproquement, soit $p \in \ker(\phi)$. Considérant $p \in \mathbb{K}[Y][X]$, on effectue la division euclidienne de $p$ par $X^2 - Y^3$ : $p = (X^2 - Y^3)q + rX + s$ avec $q$ dans $\mathbb{K}[X, Y]$, $r$ et $s$ dans $\mathbb{K}[Y]$. Alors on applique $\phi$ : $r(T^2)T^3 + s(T^2) = 0$. Or $r(T^2)T^3$ est somme de termes de degrés impairs et $s(T^2)$ est somme de terme de degrés pairs. Ainsi ils sont nuls, et $p \in (\langle X^2 - Y^3 \rangle)$.

Par conséquent, $\ker(\phi) = \langle X^2 - Y^3 \rangle$, et par premier théorème d'isomorphisme,

$$\Gamma(V(\langle X^2 - Y^3 \rangle)) \simeq \mathbb{K}[X_1, \ldots, X_n]/\ker(\phi) = \mathrm{Im}(\phi)$$

Comme $\mathrm{Im}(\phi)$ est une sous-algèbre de $\mathbb{K}[T]$, $\Gamma(V(\langle X^2 - Y^3 \rangle))$ est intègre, donc $V(\langle X^2 - Y^3 \rangle)$ est irréductible.

Tous les ensembles algébriques affines ne sont pas irrécuctibles. Par exemple, $V(XY)$ n'est pas irréductible : c'est l'union des fermés $V(X)$ et $V(Y)$ (qui sont deux droites orthogonales). On a cependant le théorème suivant :

**Définition-Proposition (Composantes irréductibles):**
Soit $V$ un ensemble algébrique affine. Alors $V$ s'écrit de manière unique comme une union finie d'ensembles algébriques affines irréductibles tel qu'aucun n'est inclus dans un autre.

Les éléments de cette décomposition sont appelés *composantes irréductibles* de $V$.

***Preuve:*** Montrons l'existence. Par l'absurde, on suppose qu'il existe un ensemble algébrique affine qui ne se décompose pas ainsi. On considère l'ensemble des idéaux radiciels dont l'ensemble algébrique affine ne se décompose pas comme souhaité. Comme l'anneau des polynômes est noethérien, il y a un idéal maximal pour l'inclusion parmi eux. Il lui correspond un ensemble algébrique affine $E$ minimal pour l'inclusion, par décroissance de $V$. On considère cet ensemble, qui n'est par hypothèse pas irréductible, et s'écrit donc comme union d'ensembles algébriques qu'il inclut strictement. Par minimalité, ceux-ci sont union d'ensembles algébriques irréductibles, et alors $E$ est union de fermés irréductibles, ce qui est absurde.

Montrons l'unicité. Supposons que l'on ait un ensemble algébrique affine s'écrivant comme union d'irréductibles $E = \bigcup_{i=1}^{n} V_i = \bigcup_{j=1}^{m} W_i$. Alors pour tout $i$ : $V_i = V_i \cap V = \bigcup_{j=1}^{m} V_i \cap W_j$. Par irréductibilité de $V_i$, il existe alors un $j$ tel que $V_i = V_i \cap W_j$, c'est à dire $V_i \subset W_j$. Symétriquement, $W_j$ est inclus dans un $V_k$, et donc $V_i \subset V_k$, donc par hypothèse $V_i = V_k = W_j$. □

## 3.3 Prolongement des identités algébriques

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

***Preuve:*** C'est un raisonnement par densité, en effet, les polynômes sont des applications continues pour la topologie de Zariski. Si $W \neq \mathbb{K}^n$, alors $W^c \neq \varnothing$, donc il est dense, or une fonction continue nulle sur un ensemble dense est nulle partout, et $p$ s'annule sur $W^c$, donc $p = 0$. □

**Remarque:** Ce résultat est très utile en algèbre linéaire, où des identitées algébriques n'ont qu'à être vérifiées sur les matrices inversibles (quelque soit le corps tant qu'il

est infini), en effet le déterminant est un polynôme à valeurs dans $\mathscr{M}_n(\mathbb{K}) = \mathbb{K}^{n^2}$, et l'ensemble des matrices non inversibles n'est autre que $V(\det)$.

Exemple: Soit $\mathbb{K}$ un corps infini, montrons que pour toute matrice $A \in \mathscr{M}_n(\mathbb{K})$, ${}^t com(A)$ est un polynôme en $A$.

Soit $A \in GL_n(\mathbb{K})$, on a l'identité ${}^t com(A) = \det(A)A^{-1}$, or

$$\chi_A = \det(A) - p_1(A)X - \cdots - p_n(A)X^n$$

avec pour $1 \leqslant i \leqslant n$, $p_i \in \mathscr{K}_{n^2}$, donc

$$0 = \chi_A(A) = \det(A) - p_1(A)A - \cdots - p_n(A)A^n$$

i.e. :

$${}^t com(A) = (p_1(A)A + \cdots + p_n(A)A^n)A^{-1} = p_1(A) + \ldots p_n(A)A^{n-1}$$

Donc ${}^t com(A)$ est un polynôme en $A$ dont les coefficients sont des polynômes de $\mathscr{K}_{n^2}$, donc par prolongement des identités algébriques, pour toute matrice $A$ de $\mathscr{M}_n(\mathbb{K})$, ${}^t com(A)$ est un polynôme en $A$.

On peut également montrer ce résultat pour un corps fini $\mathbb{K}$, en le plongeant dans sa clôture algébrique ou dans le corps des fractions $\mathbb{K}(X)$ qui sont infinis car les $p_i(A)$ sont toujours les coefficients du polynômes caractéristiques donc ils restent dans $\mathbb{K}$.

# 4 Un pas vers les catégories

La théorie des catégorie est en quelque sorte l'étude des structures d'ensembles dans son sens le plus général, et généralise la notion de morphisme. Elle nous fournit un vocabulaire utile en géométrie algébrique moderne, le lien entre objets algébriques et géométriques pourra être désigné comme une équivalence de catégorie. On remarquera l'utilisation de classes dont on n'explicitera pas la définition.

Les définitions des catégories sont tirées du polycopié d'Antoine Ducros [4], et les résultats en géométrie algébrique proviennent toujours du livre de Daniel Perrin [1].

## 4.1 Courte introduction aux catégories

**Définition:**
Une catégorie $C$ est la donnée des éléments suivants :

- Une classe d'objets notée $\mathrm{Ob}\, C$.
- Pour tout couple $X, Y$ d'objets de $C$, un ensemble $\hom_C(X, Y)$ dont les éléments sont appelés morphismes de source $X$ et de but $Y$.
- Pour tout triplet $X, Y, Z$ d'objets de $C$ une application

$$\begin{array}{rcl} \hom_C(X,Y) \times \hom_C(Y,Z) & \to & \hom_C(X,Z) \\ f, g & \mapsto & g \circ f \end{array}$$

  induisant une loi de composition associative $\circ$ sur les morphismes, qui pour tout objet $X$ admet un élément neutre $\mathrm{Id}_X \in \hom_C(X, X)$.

Exemple: Voici des catégories bien connues :

— **Ens** dont les objets sont les ensembles et les morphismes les applications.

— **Gp** dont les objets sont les groupes et les morphismes les morphismes de groupes.
— **Ann** dont les objets sont les anneaux et les morphismes les morphismes d'anneaux.
— **A-mod** avec $A$ un anneau, dont les objets sont les $A$-modules et les morphismes les applications $A$-linéaires.
— **Top** dont les objets sont les espaces topologiques et les morphismes les applications continues.

**Remarque:** On peut également étendre les notion d'endomorphismes, d'isomorphismes et d'automorphismes, à la différence près que les notions d'injectivité et de surjectivité doivent être redéfinies.

**Définition (Injectivité, surjectivité et bijectivité):**
Soit $C$ une catégorie, $X, Y$ des objets de $C$, et $f \in \hom_C(X, Y)$, alors :

- $f$ est injectif s'il existe $g \in \hom_C(Y, X)$ tel que $g \circ f = \mathrm{Id}_X$.
- $f$ est surjectif s'il existe $h \in \hom_C(Y, X)$ tel que $f \circ h = \mathrm{Id}_Y$
- $f$ est bijectif s'il est injectif et bijectif, dans ce cas $g = h$, et ce morphisme est unique, on le note $f^{-1}$

Après avoir introduit ce nouvel objet, on aimerait trouver des liens entre catégories, pour cela on introduit les foncteurs qui généralisent les opérateurs.

**Définition (Foncteur covariant, contravariant):**
Soit $C$ et $D$ deux catégories, un *foncteur* $F$ de $C$ vers $D$ est la donnée :

- pour tout objet $X$ de $C$, d'un élément $F(X) \in \mathrm{Ob}\, D$.
- pour tout morphisme $f \in \hom_C(X, Y)$, d'un morphisme
  — $F(f) : F(X) \longrightarrow F(Y)$ dans ce cas il est dit *covariant*
  — $F(f) : F(Y) \longrightarrow F(X)$ dans ce cas il est dit *contravariant*

Avec les propriétés suivantes :

- Pour $X$ objet de $C$, $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$.
- Pour $f \in \hom_C(X, Y)$, $g \in \hom_C(Y, Z)$, on a :
  — $F(g \circ f) = F(g) \circ F(f)$ si $F$ est *covariant.*
  — $F(g \circ f) = F(f) \circ F(g)$ si $F$ est *contravariant.*

**Remarque:** La notion de contravariance suit la même idée que la notion de dualité dans les espaces vectoriels par exemple.

On notera également que le foncteur préserve l'injectivité, la surjectivité, et le passage à l'inverse.

**Définition (Foncteur fidèle, plein, pleinement fidèle):**
Soient $C$ et $D$ deux catégories, et soit $F : C \to D$ un foncteur. On dit que F est *fidèle* (resp. *plein*, resp. *pleinement fidèle*) si pour tout couple $X, Y$ d'objets de C, l'application

$$\begin{array}{ccc} \hom_C(X, Y) & \longrightarrow & \hom_D(F(X), F(Y)) \\ f & \longmapsto & F(f) \end{array}$$

est injective (resp. surjective, resp. bijective).

Dans le cas de la contravariance, on intervertira $F(X)$ et $F(Y)$.

**Définition (Surjectivité essentielle):**
Soit $C$, $D$ deux catégories, et $F$ un foncteur de $C$ vers $D$, on dit que $F$ est *essentiellement surjectif* si pour tout objet $Y \in \mathrm{Ob}\, D$, il existe $X \in \mathrm{Ob}\, C$ tel que $F(X)$ soit isomorphe à $Y$.

**Définition (Équivalence de catégories):**
Soit $C$ et $D$ deux catégories, elles sont *équivalentes* s'il existe un foncteur pleinement fidèle et essentiellement surjectif de $C$ vers $D$.

Exemple: Considérons la catégorie $\mathbb{K}$-**Vect** dont les objets sont les $\mathbb{K}$-espaces vectoriels de dimension finie, et les morphismes les applications $\mathbb{K}$-linéaires, alors le foncteur qui à un espace vectoriel associe son dual, et à une application linéaire sa transposée est un foncteur contravariant pleinement fidèle et essentiellement surjectif.

**Remarque:** Travailler dans une catégorie $D$ équivalente à $C$ revient à travailler dans $C$ et offre un nouveau regard sur cette dernière. De plus si le foncteur en question est contravariant, on pourra considérer $D$ comme le "dual" de $C$.

Nous n'allons pas pousser dans ses retranchements la théorie des catégories car ce n'est pas l'objectif, mais voyons quel regard elle offre sur la géométrie algébrique.

## 4.2 Application de la théorie des catégories à la géométrie algébrique classique

**Définition (Application régulière):**
Soit $V \subset \mathbb{K}^n$ et $W \subset \mathbb{K}^m$ deux ensembles algébriques affines et $\varphi : V \to W$ . On note $\varphi_1, \ldots, \varphi_m$ ses composantes, alors $\varphi$ est *régulière* si chacune de ses composantes est polynômiale (i.e dans $\Gamma(V)$).
On note $\mathrm{Reg}(V, W)$ l'ensemble des applications régulières de $V$ dans $W$

**Propriété:**
La donnée des ensembles algébriques affines et des applications régulières forme une catégorie que l'on note **Alg**.

Exemple:
- Les éléments de $\Gamma(V)$, et en particulier les fonction coordonnées sont des morphismes de source $V$ et de but $\mathbb{K}$
- Soit $V \subset \mathbb{K}^n$, la projection $\varphi$ de $V$ sur $\mathbb{K}^p$ donnée par $\varphi(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_p})$ est un morphisme.
- Avec $W \coloneqq V(Y - X^2)$, $\varphi$ la projection par rapport à la première variable sur $\mathbb{K}$ est un isomorphisme de réciproque $x \mapsto (x, x^2)$.
- L'application $\begin{array}{rccc} \varphi : & \mathbb{K} & \longrightarrow & V(Y^2 - X^3) \\ & t & \longmapsto & (t^2, t^3) \end{array}$ est un morphisme bijectif au sens des applications, mais pas un isomorphisme car sa réciproque n'est pas régulière.

**Remarque:** Les applications régulières sont continues pour la topologie de Zariski, mais la réciproque n'est pas vraie (pour un corps $\mathbb{K}$ les applications bijectives de $\mathbb{K}$ dans lui même sont continues).

**Définition-Proposition (Foncteur $\Gamma$):**
On pose le foncteur contravariant $\Gamma$ de la catégorie des ensembles algébriques affines vers celle des algèbres affines de la manière suivante :

- Pour $V$ un ensemble algébrique affine, $\Gamma(V)$ garde la même signification que précédemment.
- Pour $\varphi$ régulière de source $V$, de but $W$, on pose $\Gamma(\varphi) = \varphi^*$, avec pour $p$ dans $\Gamma(V)$, $\varphi^*(p) = p \circ \varphi$.

**Remarque:** La notation $^*$ n'est pas anodine, encore une fois on fait un parallèle avec le foncteur contravariant de la dualité, on remarque que la transposition arbore une mécanique identique.

Il est simple de calculer $\varphi^*$ à partir de $\varphi$, si V $\subset \mathbb{K}^n$ et $W \subset \mathbb{K}^m$, on pose $\pi_i$ la $i$-ème fonction coordonnée sur $\Gamma(W)$, alors $\varphi^*(\pi_i) = \varphi_i$, or les $\varphi_i$ sont des restrictions à $V$ de polynômes $P_i(X_1, \ldots, X_n)$, comme $\Gamma(V) \simeq {}^{\mathscr{K}_n}\!/_{\mathscr{I}(V)}$, on peut définir le morphisme d'algèbres $\varphi^*$ par

$$\begin{array}{rccc} \varphi^* : & {}^{\mathscr{K}_n}\!/_{\mathscr{I}(W)} & \longrightarrow & {}^{\mathscr{K}_n}\!/_{\mathscr{I}(V)} \\ & \overline{Y_i} & \longmapsto & \overline{P_i}(X_1, \ldots, X_n) \end{array}$$

Exemple: Pour la paramétrisation $\varphi(t) = (t^2, t^3)$ de $V(Y^2 - X^3)$ vue précedemment, on a $\varphi^* : {}^{\mathbb{K}[X,Y]}\!/_{\langle Y^2 - X^3 \rangle} \to \mathbb{K}[T]$ définie par $\varphi^*(\overline{X}) = T^2$ et $\varphi^*(\overline{Y}) = T^3$.

Étudions maintenant les propriétés de ce foncteur.

**Propriété:**
Le foncteur $\Gamma$ est pleinement fidèle.

***Preuve:*** Soit $V \subset \mathbb{K}^n$ et $W \subset \mathbb{K}^m$, on note $\gamma$ la fonction induite par le foncteur $\Gamma$ de $\mathrm{Reg}(V, W)$ vers $\hom_{\mathbb{K}\textbf{-alg}}(\Gamma(W), \Gamma(V))$. Procédons en deux temps, d'abord l'injectivité puis la surjectivité de $\gamma$.

Soit $\varphi, \psi \in \mathrm{Reg}(V, W)$ telles que $\varphi^* = \psi^*$, alors pour chaque application coordonnée $\pi_i$, on a $\varphi_i = \varphi^*(\pi_i) = \psi^*(\pi_i) = \psi_i$. Donc $\varphi = \psi$, i.e. $\gamma$ est injective.

Soit $\theta \in \hom_{\mathbb{K}\textbf{-alg}}(\Gamma(W), \Gamma(V))$. On pose naturellement $\varphi_i = \theta(\pi_i) \in \Gamma(V)$, alors on définit clairement une application régulière $\varphi \in \mathrm{Reg}(V, \mathbb{K}^m)$. Il reste à montrer que son image est dans $W$. Pour cela prenons $p(Y_1, \ldots, Y_m) \in \mathscr{I}(W)$, et $x \in V$, alors

$$p(\varphi(x)) = p(\theta(\pi_1), \ldots, \theta(\pi_m))(x) = \theta(p(\pi_1, \ldots, \pi_m))(x)$$

On observe alors que $p(\pi_1, \ldots, \pi_m)$ est la fonction polynômiale dans $\Gamma(W)$ associée au polynôme $p(Y_1, \ldots, Y_m) \in \mathscr{I}(W)$, donc cet élément est nul, donc $\forall p \in I(W)$, $p(\varphi(x)) = 0$, donc $\varphi(x) \in W$. Donc $\varphi$ est bien à valeurs dans $W$, i.e. $\varphi^* = \theta$, donc $\gamma$ est surjective.

Avec ces deux résultats, on conclut que $\Gamma$ est pleinement fidèle. □

**Corollaire:**
Soit $\varphi : V \longrightarrow W$ une application régulière, alors $\varphi$ est un isomorphisme si et seulement si $\varphi^*$ en est un.

Autrement dit $V$ et $W$ sont isomorphes si et seulement si leurs algèbres associées le sont.

Exemple: Avec ce résultat, on peut montrer facilement que le paramétrage $\varphi(t) = (t^2, t^3)$ n'est pas un isomorphisme entre $\mathbb{K}$ et $V(Y^2 - X^3)$

En effet, si c'était le cas, alors $\varphi^*$ en serait un, or son image est le sous-anneau $\mathbb{K}[T^2, T^3] \subsetneq \mathbb{K}[T]$, donc c'est faux.

Dans la section précédente, on avu que la notion d'irréductibilité revêt un caractère important en géométrie algébrique, or le foncteur $\Gamma$ permet de caractériser plus facilement des ensembles irréductibles.

**Définition (Dominance):**
Soit $\varphi : V \longrightarrow W$ une application régulière, $\varphi$ est dite dominante si l'adhérence de son image pour la topologie de Zariski est égale à $W$ tout entier, i.e.

$$\overline{\varphi(V)} = W$$

**Remarque:** Cette contrainte n'est pas très forte car les fermés de la topologie de Zariski sont très petits.

**Propriété:**
Soit $\varphi : V \longrightarrow W$ une application régulière, alors :

(*i*) $\varphi$ est dominante $\iff \varphi^*$ est injectif.

(*ii*) Si $\varphi$ est dominante et $V$ irréductible, alors $W$ est irréductible.

***Preuve:*** Montrons les deux points.

(*i*) Supposons d'abord $\varphi$ dominante, si $p \in \ker \varphi^*$, alors $p \circ \varphi = 0$, i.e $p(\varphi(V)) = \{0\}$, or $p$ est continue pour la topologie de Zariski, donc $\overline{p(\varphi(V))} = p(\overline{\varphi(V)}) = p(W) = \{0\}$, donc $p = 0$, donc $\varphi^*$ est injective. Supposons maintenant $\varphi^*$ injective, on pose $U = \overline{\varphi(V)} \subset W$, c'est un fermé donc un ensemble algébrique affine. Si $U \neq W$, alors comme l'application $\mathscr{I}$ est injective sur les ensembles algébriques affine, il existe $p \in \Gamma(W)$ non nul tel que $p(U) = \{0\}$, or dans ce cas, on a également $\varphi^*(p) = p \circ \varphi = 0$, donc $p = 0$, c'est exclu, donc $U = W$, i.e. $\varphi$ est dominante.

(*ii*) Si $\varphi$ est dominante, et $V$ irréductible, alors $\varphi^*$ est injective, et $\Gamma(V)$ est intègre (voir section 3.2). Soit $p, q \in \Gamma(W)$ tels que $pq = 0$, alors $\varphi^*(pq) = 0$, donc $\varphi^*(p)\varphi^*(q) = 0$, or comme $\Gamma(V)$ est intègre, soit $\varphi^*(p) = 0$ soit $\varphi^*(q)$, i.e. $p = 0$ ou $q = 0$. Donc $\Gamma(W)$ est intègre, donc $W$ est irréductible. □

Pour finir, lorsque le corps de base est algébriquement clos, on a une équivalence de catégories.

**Théorème:**
Supposons $\mathbb{K}$ algébriquement clos, alors le foncteur $\Gamma$ induit une équivalence de catégories entre la catégorie des ensembles algébriques affines munie des applications régulières, et la catégorie des $\mathbb{K}$-algèbres réduites de type fini, munie des morphismes de $\mathbb{K}$-algèbres.

***NB:*** Une algèbre est dite réduite si elle n'admet pas d'élément nilpotent autre que 0, autrement dit $\{0\}$ est radiciel.

***Preuve:*** La pleine fidélité a déjà été prouvée, il ne reste que la surjectivité essentielle.

Soit $A$ une $\mathbb{K}$-algèbre réduite de type fini, elle est isomorphe à un certain quotient $\mathscr{K}_n/I$ (voir section 1.5). Comme $A$ est réduite, il en résulte que $I$ est radiciel. On pose $W = V(I)$, d'après le Nullstellensatz, on a $\mathscr{I}(W) = \sqrt{I} = I$, donc

$$A \simeq \mathscr{K}_n/\mathscr{I}(W) \simeq \Gamma(W)$$ □

# 5 Bases de géométrie algébrique moderne

On va a présent chercher à généraliser les notions de géométrie algébriques vues sur des anneaux de polynômes à tout anneau commutatif. Dans cette section, $A$ est un anneau commutatif.

## 5.1 Spectre d'un anneau

Avec les anneaux de polynôme, on pouvait faire de la géométrie sur l'espace $\mathbb{K}^n$. On va maintenant définir un espace topologique à partir de $A$, l'espace $\mathrm{Spec}(A)$.

**Définition (Spectre):**
On appelle *spectre* de $A$ et on note $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de $A$.

Exemple:
- Un anneau est intègre si et seulement si l'idéal nul est dans son spectre.
- Pour $\mathbb{Z}$, les idéaux premiers sont l'idéal nul et les idéaux engendrés par un nombre premier. On peut donc identifier $\mathrm{Spec}(\mathbb{Z})$ à l'union de $\{0\}$ et de l'ensemble des nombres premiers positifs.
- Pour $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps, les idéaux premiers sont ceux engendrés par un polynôme irréductibles, que l'on peut identifier à leur générateur unitaire, et l'idéal nul.
- En particulier, si $\mathbb{K}$ est algébriquement clos, les polynômes irréductibles sont ceux de degré 1, par conséquent on peut identifier $\mathrm{Spec}(\mathbb{K}[X])$ à $\mathbb{K}$ auquel on ajoute un point pour l'idéal nul.

Cette notion de spectre ne coïncide pas avec $\mathbb{K}^n$ dans le cas des anneaux de polynômes : en effet, on peut identifier $\mathbb{K}^n$ à l'ensemble des idéaux maximaux de l'anneau des polynômes (avec le troisième corollaire du Nullstellensatz), qui est une partie stricte de l'ensemble des idéaux premiers (par exemple l'idéal nul est premier mais pas maximal).

Comme le quotient d'un anneau par un idéal premier est intègre, on peut généraliser aux idéaux intègres la notion de corps résiduel :

**Définition (Corps résiduel):**
Soit $x \in \mathrm{Spec}(A)$. On appelle *corps résiduel* de $x$ et on note $\kappa(x)$ le corps $\mathrm{Frac}\, {}^{A}\!/_{x}$.

On notera $\iota_x$ la composée de l'injection canonique ${}^{A}\!/_{x} \to \mathrm{Frac}\, {}^{A}\!/_{x}$ et de la projection canonique $A \to {}^{A}\!/_{x}$.

Exemple: On conserve les identifications faites précédemment.
- Dans un anneau intègre, le corps résiduel de l'idéal nul est le corps des fractions.
- Pour $\mathbb{Z}$, le corps résiduel d'un nombre premier $p$ est $\mathbb{Z}/p\mathbb{Z}$, le corps résiduel de l'idéal nul est $\mathbb{Q}$.
- Pour $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps, le corps résiduel d'un polynôme unitaire irréductible est une $\mathbb{K}$-algèbre de dimension finie. Le corps résiduel de l'idéal nul est $\mathbb{K}(X)$.
- Pour $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps algébriquement clos, le corps résiduel d'un élément de $\mathbb{K}$ est $\mathbb{K}$. Par division euclidienne, si $x \in \mathbb{K}$, $\iota_x$ est l'évaluation en $x$.

Comme pour les anneaux de polynômes et $\mathbb{K}^n$, on souhaiterait pouvoir considérer $A$ comme un anneau de fonctions définies sur $\mathrm{Spec}(A)$ à valeurs dans un corps. Les évaluations seraient alors des morphismes d'anneaux de $A$ à valeur dans un corps. Les trois propriétés suivantes justifient partiellement ce point de vue.

**Propriété:**
Soit $\mathbb{K}$ un corps, $\phi : A \to \mathbb{K}$ un morphisme d'anneau. Alors $\ker(\phi) \in \mathrm{Spec}(A)$.

***Preuve:*** Déjà $\ker(\phi)$ un un idéal en tant que noyau d'un morphisme. Ensuite par théorème de factorisation, $A/\ker(\phi)$ s'injecte dans $\mathbb{K}$, qui est un corps. En particulier, c'est un anneau intègre, donc $A/\ker(\phi)$ également, donc $\ker(\phi)$ est premier. □

**Propriété:**
Soit $\mathbb{K}$ et $\mathbb{K}'$ deux corps, $p : \mathbb{K} \to \mathbb{K}'$ un morphisme de corps, $\phi : A \to \mathbb{K}$ un morphisme d'anneau. Alors $\ker(\phi) = \ker(p \circ \phi)$.

***Preuve:*** On a $\ker(p \circ \phi) = (p \circ \phi)^{-1}(\{0\}) = \phi^{-1}(p^{-1}(\{0\}))$. Comme $p$ est un morphisme de corps, il est injectif, donc $p^{-1}(\{0\}) = \{0\}$, d'où $\ker(\phi) = \ker(p \circ \phi)$. □

**Propriété:**
Soit $\mathbb{K}$ un corps, $\phi : A \to \mathbb{K}$ un morphisme d'anneau. Alors il existe un morphisme de corps $p : \kappa(\ker(\phi)) \to \mathbb{K}$ tel que $\phi = p \circ \iota_x$.

***Preuve:*** Par théorème de factorisation, on peut factoriser $\phi$ en la projection canonique et une injection $A/\ker(\phi) \to \mathbb{K}$. Ce morphisme d'anneau injectif peut se factoriser en l'injection canonique et un morphisme de corps $p : \kappa(\ker(\phi)) \to \mathbb{K}$. On a finalement factorisé $\phi$ en $p \circ \iota_x$. □

Avec ces trois propriétés, on obtient un autre point de vue sur $\mathrm{Spec}(A)$. En effet, on considère la classe des couples $(\mathbb{K}, \phi)$ avec $\mathbb{K}$ un corps et $\phi : A \to \mathbb{K}$ un morphisme. On quotiente cette classe par la relation d'équivalence engendrée par la relation binaire $\mathscr{R}$ définie par $(\mathbb{K}, \phi)\mathscr{R}(\mathbb{K}', \phi')$ est vraie s'il existe un morphisme $p : \mathbb{K} \to \mathbb{K}'$ tel que $\phi' = p \circ \phi$. On constate qu'alors, au vu des propriétés précédantes, le spectre de $A$ peut être vu comme l'ensemble des classes d'équivalences obtenues. Cependant, en l'absence d'une théorie des classes, la définition précédente n'est pas vraiment rigoureuse.

Cette considération nous incite à penser $A$ comme un anneau de fonctions définies sur $\mathrm{Spec}(A)$ à valeur dans un corps, et on note parfois $f(x)$ au lieu de $\iota_x(f)$ pour $f \in A$, $x \in \mathrm{Spec}(A)$. Cette analogie est parfois pertinente : Par exemple, un élément de $A$ est inversible si et seulement si il n'est dans aucun idéal premier (pour le sens direct, tout idéal premier est propre, pour le sens réciproque, pour tout idéal engendré par un élément non inversible, le théorème de Krull donne un idéal maximal donc premier le contenant). Ainsi, un élément $f$ de $A$ est inversible si et seulement si $f(x)$ est nul pour tout $x \in \mathrm{Spec}(A)$. Mais l'analogie avec un anneau de fonctions a des limites. Par exemple, $A$ peut contenir des éléments nilpotents non nuls, ce qui n'est pas le cas pour un anneau de fonctions à valeur dans un corps. Par ailleurs, $f(x)$ est nul pour tout $x$ dans $\mathrm{Spec}(A)$ si $f$ est nilpotent, même non nul. On montrera plus tard que l'ensemble des élément nilpotent est l'intersection des idéaux premiers ($\mathscr{I}(V(I)) = \sqrt{I}$, avec $I$ l'idéal nul), on en déduit qu'il y a équivalence entre $f(x)$ toujours nul et $f$ nilpotent.

## 5.2 Topologie de Zariski

On peut définir $V$ et $\mathscr{I}$ par analogie avec les définitions données avant :

**Définition:**
Soit $E$ une partie de $A$. On note $V(E)$ l'ensemble des éléments de $\mathrm{Spec}(A)$ qui incluent $E$.

Soit $F$ une partie de $\mathrm{Spec}(A)$. On note $\mathscr{I}(F)$ l'intersection des éléments de $F$.

Attention, dans le cas de $\mathscr{K}_n$, l'image de $V$ est plus grande qu'avec la définition d'avant (en identifiant $\mathscr{K}_n$ aux idéaux maximaux de $A$). Par contre $\mathscr{I}$ coïncide avec sa définition d'avant sur les idéaux maximaux. On prendra garde au fait qu'en particulier, $\mathscr{I} \circ V$ n'a à priori pas de raison d'être égale à $\mathscr{I} \circ V$ avec les anciennes définitions (on verra qu'en fait ce sera bien le cas).

**Propriété:**
Les fonctions $V$ et $\mathscr{I}$ sont décroissantes.

***Preuve:*** Si $E \subset F \subset A$, tout idéal qui inclut $F$ inclus aussi $E$.

Une intersection sur une famille plus grande donne un ensemble plus petit pour l'inclusion. □

**Propriété:**
Soit $E$ une partie de $A$. Alors $V(E) = V(\langle E \rangle)$.

***Preuve:*** Par décroissance de $V$, on a $V(\langle E \rangle) \subset V(E)$. Réciproquement, soit $x$ un idéal premier incluant $E$. Alors il inclut $\langle E \rangle$ par minimalité idéal engendré. □

On peut à présent définir la topologie de Zariski sur $\mathrm{Spec}(A)$

**Définition-Proposition (Topologie de Zariski):**
On appelle *topologie de Zariski* la topologie sur $\mathrm{Spec}\, A$ dont les fermés sont les $V(E)$ avec $E$ parcourant l'ensemble des parties de $A$.

***Preuve:*** Déjà $\emptyset = V(A)$ donc $\emptyset$ est fermé. Ensuite si $E$ et $E'$ sont deux parties de $A$, on a $V(E) \cup V(E') = V(E \cdot E')$, avec $E \cdot E' = \{ee' | e \in E, e' \in E'\}$. En effet, l'inclusion $V(E) \cup V(E') \subset V(E \cdot E')$ résulte de la stabilité d'un idéal pour produit par un élément de $A$. Réciproquement, si $x \in V(E \cdot E')$, supposons $x \notin V(E)$ et $x \notin V(E')$, alors on dispose de $e \in E \setminus x$ et $e' \in E' \setminus x$, mais comme $x$ est premier, $ee' \notin E \cdot E'$, ce qui est absurde.

Si on a $(E_i)_{i \in I}$ une famille de parties de $A$ (avec $I$ un ensemble), alors $\bigcap_{i \in I} V(E_i) = V\left(\bigcup_{i \in I} E_i\right)$. □

Exemple:
- Dans un anneau intègre, l'idéal nul est inclus dans tout idéal, donc son adhérence est l'espace entier. On dit que c'est un *point générique* de $\mathrm{Spec}(A)$. Si $A$ n'est pas un corps, on en déduit que $\mathrm{Spec}(A)$ n'est pas séparé.
- Dans $\mathrm{Spec}(\mathbb{Z})$, chaque nombre premier est fermé car engendre un idéal maximal. De plus, si $I$ est un idéal non nul, il est inclus dans les idéaux premiers engendrés par ses facteurs premiers, qui sont en nombre fini. Enfin, pour tout ensemble fini $P$ de nombres premiers, les idéaux engendrés par les éléments de $P$ sont les idéaux premiers qui contiennent l'idéal engendré par le produit des éléments de $P$. Par conséquent, les fermés de $\mathrm{Spec}(\mathbb{Z})$ sont les ensembles finis de nombres premiers et $\mathrm{Spec}(\mathbb{Z})$ entier.
- De la même manière, si $\mathbb{K}$ est un corps, les fermés de $\mathrm{Spec}(\mathbb{K}[X])$ sont $\mathrm{Spec}(\mathbb{K}[X])$ et les ensembles finis de polynômes irréductibles unitaire.

Dans le cas de $\mathscr{K}_n$, la topologie induite sur $\mathbb{K}^n$ est bien la topologie de Zariski qu'on avait définie avant.

On peut établir sur $V$ et $\mathscr{I}$ des propriétés analogues à celles de la géométrie algébrique classique.

**Propriété:**
Soit $F$ un fermé de Spec$(A)$. Alors $V(\mathscr{I}(F)) = F$.

***Preuve:*** Déjà $F \subset V(\mathscr{I}(F))$. Ensuite, par définition des fermés de Zariski, il existe une partie $E$ de $A$ telle que $F = V(E)$. Alors $E \subset \mathscr{I}(V(E))$, et par décroissance de $V$, $V(\mathscr{I}(V(E))) \subset V(E)$ ce qui est l'inclusion réciproque. □

**Propriété:**
Soit $I$ un idéal de $A$. Alors $\mathscr{I}(V(I)) = \sqrt{I}$.

***Preuve:*** Par définition, $\mathscr{I}(V(I))$ est l'intersection des idéaux premiers qui contiennent $I$. Soit $s \in A \setminus \sqrt{I}$. On peut montrer que l'ensemble des idéaux qui contiennent $I$ et aucune puissance de $s$ est un ensemble inductif. On applique le lemme de Zorn pour avoir un idéal $P$ maximal dans cet ensemble. C'est un idéal propre, montrons qu'il est premier en montrant que $xy \notin P$ pour $x, y \in A \setminus P$.

L'idéal $P+Ax$ contient alors strictement $P$, donc contient $s^n$ pour un entier naturel $n$. De même, $P + Ay$ contient $s^m$ pour un entier naturel $m$. Ainsi, en développant $s^{n+m} = s^n s^m$, on obtient la somme d'un élément de $P$ et du produit d'un élément $a$ de $A$ par $xy$. Comme, par définition de $P$, $s^{n+m}$ n'est pas dans $P$, $axy$ n'est pas dans $P$. Donc $xy$ n'est pas dans $P$.

Ainsi, il existe un idéal premier, $P$, qui contient $I$ et pas $s$. Par conséquent, $\mathscr{I}(V(I)) \subset \sqrt{I}$. L'inclusion réciproque résulte d'une simple vérification. □

On en déduit la propriété suivante :

**Corollaire:**
La fonction $V$ est un bijection de l'ensemble des idéaux radiciel de $A$ dans l'ensemble des fermés de Spec$(A)$, de réciproque $\mathscr{I}$.
De plus si $S \subset$ Spec$(A)$, $V(\mathscr{I}(S)) = \overline{S}$. Si $S \subset A$, $\mathscr{I}(V(S)) = \sqrt{\langle S \rangle}$.

On retrouve ainsi des résultats similaires à $\mathscr{K}_n$ (avec $\mathbb{K}$ un corps algébriquement clos) avec les idéaux maximaux. C'est pour cette raison que l'on peut faire de la géométrie algébrique sur $\mathscr{K}_n$ comme on l'a fait précédamment, en considérant uniquement des idéaux maximaux. On montrera dans la section suivante que c'est aussi le cas pour toute algèbre de type fini sur $\mathbb{K}$.

On finit cette section par une propriété topologique du spectre, la quasi-compacité. Pour établir cela, on a besoin d'une base d'ouverts particulière.

**Définition:**
Soit $a \in A$, on note $D(a)$ le complémentaire de $V(\{a\})$.

**Propriété:**
Les $D(a)$, avec $a$ parcourant $A$, forment une base d'ouverts de Spec$(A)$.

***Preuve:*** Soit $a \in A$. Alors $D(a)$ est ouvert comme complémentaire d'un fermé. Soit $O$ un ouvert de Spec$(A)$. Alors on dispose d'une partie $E$ de $A$ telle que $O$ est le complémentaire de $V(E)$. Alors $V(E) = \bigcap_{e \in E} V(\{e\})$, et en passant au complémentaire $O = \bigcup_{e \in E} D(e)$. □

**Théorème:**
L'espace Spec($A$) est quasi-compact.

***Preuve:*** Soit $\mathscr{O}$ un ensemble d'ouverts de Spec($A$). Chaque élément de $\mathscr{O}$ s'écrit comme union d'ouverts de la forme $D(a)$ ($a \in A$). On a donc un ensemble $E$ tel que si $e$ parcourt $E$, les $D(e)$ recouvrent Spec($A$) et tel que chaque $D(e)$ est inclut dans un ouvert de $\mathscr{O}$.

Alors pour chaque $x$ dans Spec($A$), il existe un $e$ dans $E$ tel que $e \notin x$. Par conséquent l'idéal engendré par $E$ n'est contenu dans aucun idéal premier, et donc par théorème de Krull, son idéal engendré est $A$ (sinon il serait inclus dans un idéal maximal, donc premier). Ainsi 1 est une somme (finie) de produits d'un élément de $A$ par un élément de $E$. Par conséquent 1, donc $A$, est engendré par un sous ensemble fini $F$ de $E$. Par conséquent 1, donc $A$, est engendrée par une partie finie $F$ de $E$, et donc pour tout $x$ dans Spec($A$), il existe un $f$ dans $F$ tel que $f \notin x$. Ainsi les $D(f)$ avec $f$ parcourant $F$ recouvrent Spec $A$.

Comme chaque $D(f)$ est inclus dans un ouvert de $\mathscr{O}$, Spec($A$) est recouvert par un nombre fini d'ouvert. Ainsi Spec($A$) est quasi-compact. □

En pratique, Spec($A$) est rarement compact car rarement séparé.

## 5.3 Algèbre de type finie sur un corps algébriquement clos

Soit $\mathbb{K}$ un corps algébriquement clos, $A$ une $\mathbb{K}$-algèbre de type finie. On dispose alors d'un entier $n$ et d'une famille de polynômes $P_1$,...,$P_n$ tels que $A \simeq \mathscr{K}_n/\langle P_1, \dots, P_n \rangle$. On pose Spm($A$) le *spectre maximal* de $A$, c'est-à-dire l'ensemble des idéaux maximaux de $A$. Le troisième corollaire du Nullstellensatz nous permet de l'identifier à l'ensemble algébrique affine de $P_1$,...,$P_n$ dans $\mathbb{K}^n$. On a Spm($A$) $\subset$ Spec($A$), et on va établir un lien plus fort entre les deux. Mais avant, posons $E$ un espace topologique quelconque, $C_E$ le plus petit ensemble de parties de $E$ contenant les ouverts et les fermés, et stable par union finie, intersection finie et passage au complémentaire. On peut décrire plus précisément ses éléments :

Soit $P$ une partie de $E$. Alors $P \in C_E$ si et seulement si il existe une famille d'ouverts $(U_i)_{i\in I}$ et une famille de fermés $(F_i)_{i\in I}$ indexées par un ensemble fini $I$ tels que $P = \bigcup_{i\in I} U_i \cap F_i$.

***Preuve:*** Soit $D$ l'ensemble des parties de Spec($A$) ayant la forme décrite. Si $U$ est un ouvert, on pose $I = \{0\}$, $U_0 = U$, $F_0 = \text{Spec}(A)$, alors $U \in \text{Spec}(A)$, donc $D$ contient les ouverts. Si $F$ est un fermé, on pose le même $I$, $U_0 = \text{Spec}(A)$ et $F_0 = F$, ainsi $D$ contient les fermés. Il est évidemment stable par union finie. Comme l'intersection finie distribue l'union, et qu'ouverts et fermés sont stables par intersection finie, $D$ est stable par intersection finie. Enfin, si $U$ est ouvert et $F$ est fermé, on a $\left(\bigcup_{i\in I} U_i \cap F_i\right)^c = \bigcap_{i\in I} U_i^c \cup F_i^c$, et $D$ étant stable par union et intersection finie, il est stable par complémentaire. De plus, il est clair que toute partie incluant ouverts et fermés et stable par union finie et intersection fini inclue $D$, donc par définition $C_E = D$. □

On a alors la proposition suivante :

**Propriété:**
La trace sur $\mathrm{Spm}(A)$ est une bijection de $C_{\mathrm{Spec}(A)}$ vers $C_{\mathrm{Spm}(A)}$, avec $\mathrm{Spec}(A)$ muni de la topologie de Zariski et $\mathrm{Spm}(A)$ de la topologie induite.

***Preuve:*** Déjà, remarquons que $C_{\mathrm{Spec}(A)}$ et $C_{\mathrm{Spm}(A)}$ sont des groupes pour la loi différence symétrique, de neutre $\emptyset$, et que la trace sur $\mathrm{Spm}(A)$ est un morphisme de groupe de $C_{\mathrm{Spec}(A)}$ vers $C_{\mathrm{Spm}(A)}$. De plus, par définition de la topologie induite, la trace sur $\mathrm{Spm}(A)$ est surjective de $C_{\mathrm{Spec}(A)}$ vers $C_{\mathrm{Spm}(A)}$. Il reste donc à établir que son noyau est réduit à l'ensemble vide.

En exploitant le lemme précédant, on pose $I$ fini, une famille d'ouverts $(U_i)_{i\in I}$ et une famille de fermés $(F_i)_{i\in I}$ tels que $\mathrm{Spm}(A) \cap \bigcup_{i\in I} U_i \cap F_i = \emptyset$. Soit $i \in I$, on pose $U = U_i$, $F = F_i$. Il existe un idéal $J$ de $A$ tel que $F = V(J)$, donc $F$ est l'ensemble des idéaux premiers de $A$ contenant $F$, et donc s'identifie à $\mathrm{Spec}(A/J)$. Alors $U \cap F$ peut être considéré comme un ouvert de $\mathrm{Spec}(A/J)$, et donc s'écrit $\bigcup_{a\in B} D(a)$ avec $B \subset A/J$. Soit $a \in B$. Comme $D(a)$ est l'ensemble des idéaux premiers de $A/J$ ne comprenant pas $a$, on peut l'identifier au spectre du localisé $\left(A/J\right)_a$. Par hypothèse, ce spectre n'a pas d'idéal maximal. Par conséquent, par théorème de Krull, $\left(A/J\right)_a$ est l'anneau nul, donc $a = 0$, donc $U \cap F$ est vide. □

**Corollaire:**
La trace sur $\mathrm{Spm}(A)$ met en bijection les ouverts de $\mathrm{Spec}(A)$ et ceux de $\mathrm{Spm}(A)$, ainsi que les fermés de $\mathrm{Spec}(A)$ et ceux de $\mathrm{Spm}(A)$. Dans le cas des fermés, l'adhérence dans $\mathrm{Spm}(A)$ en est la bijection réciproque.

***Preuve:*** Par définition de la topologie induite, les ouverts sont envoyés sur les ouverts et les fermés sur les fermés, de manière surjective. L'injectivité résulte de la propriété précédente. Dans le cas des fermés, l'adhérence $G$ de la trace d'un fermé $F$ est incluse dans ce fermé (par minimalité de l'adhérence). Mais alors la trace de $G$ est égale à la trace de $F$, donc par injectivité il y a égalité. □

Cette dernière proposition, combinée au fait que $V(\mathscr{I}(S)) = \overline{S}$, justifie le fait que pour les algèbres de type finie sur des corps algébriquement clos (en particulier pour les ensembles algébriques affines), on peut travailler sur Spm au lieu de Spec. Cela justifie ainsi l'approche de la géométrie algébrique classique, où les points de $\mathbb{K}^n$ ne s'identifient qu'aux idéaux maximaux.

## 5.4 Fonctorialité du spectre

**Propriété:**
Soit $B$ un anneau commutatif. Soit $\phi : A \to B$ un morphisme d'anneau. Alors on peut définir l'application image réciproque $\psi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$, qui est continue pour la topologie de Zariski. De plus si $x \in \mathrm{Spec}(B)$, $\kappa(\psi(x))$ se plonge dans $\kappa(x)$.

***Preuve:*** Déjà l'image réciproque d'un idéal premier par un morphisme d'anneau est un idéal premier.

Montrons le plongement. Comme le morphisme $\iota_x \circ \phi : A \to \kappa_x$ a valeur dans un corps, on peut le factoriser en $p \circ \iota_{\psi(x)}$, avec $p$ un morphisme de corps (donc injectif) de $\kappa_\psi(x)$ dans $\kappa_x$.

On peut en déduire que pour tout $x \in \mathrm{Spec}(B)$ et $a \in A$, $a \in \psi(x)$ équivaut à $\iota_{\psi(x)}(a) = 0$, ce qui équivaut à $p \circ \iota_{\psi(x)}(a) = 0$, ce qui équivaut à $\iota_x \circ \phi(a) = 0$, ce qui équivaut enfin à $\phi(a) \in x$.

On montre la continuité avec l'équivalence précédante : pour $E \subset A$,

$$\begin{aligned} \psi^{-1}(V(E)) &= \{\psi^{-1}(J),\, J \in \mathrm{Spec}(A) \mid E \subset I\} \\ &= \{I,\, I \in \mathrm{Spec}(B) \mid E \subset \psi(I)\} \\ &= \{I,\, I \in \mathrm{Spec}(B) \mid \phi(E) \subset I\} \;=\; V(\phi(E)) \end{aligned}$$

Ainsi l'image réciproque d'un fermé est un fermé. □

Ainsi Spec envoie un anneau sur un espace topologique, mais envoie aussi un morphisme d'anneau $\phi : A \to B$ sur une application continue $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. Cela se fait de manière contravariante vis-à-vis de la composition, c'est-à-dire que si $\phi$ et $\psi$ sont deux morphismes pouvant être composés, alors $\mathrm{Spec}(\phi \circ \psi) = \mathrm{Spec}(\psi) \circ \mathrm{Spec}(\phi)$. Enfin Spec envoie les fonctions identités sur les fonctions identités. Ainsi Spec est un foncteur contravariant de la catégorie des anneaux dans la catégorie des espaces topologiques.

# Références

[1] Daniel Perrin. *Géométrie algébrique :* Une introduction. InterÉditions - CNRS Éditions, 1995.

[2] Daniel Perrin. Cours d'algèbre, 1981.

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

[4] Antoine Ducros. Introduction à la théorie des schémas, 2014.