Université de Rennes 1

Introduction à la géométrie algébrique : Les ensembles algébriques

Alice Bouillet

01 Juin 2017 — 18 Juillet 2017

Table des matières

Introduction

La géométrie algébrique est un domaine des mathématiques qui, historiquement, s'est d'abord intéressé à des objets géométriques (courbes, surfaces...) composés des points dont les coordonnées vérifiaient des équations ne faisant intervenir que des sommes et des produits. La simplicité de cette définition fait qu'elle embrasse un grand nombre d'objets et qu'elle permet de développer une théorie riche.

Les premiers travaux de cette nature remontent aux mathématiques arabes avec Omar Khayyam.
La Géométrie de Descartes, inaugurant l'étude des courbes algébriques par les méthodes de la géométrie analytique, marque la deuxième grande étape dans la genèse de cette discipline.

À proprement parler, il faut attendre le début du vingtième siècle pour que la géométrie algébrique devienne un domaine à part entière. Cela fut initié, d'une part, par les travaux de David Hilbert, puis fut développé, d'autre part, par l'école italienne de la fin du XIX^{eme} siècle. Ce fut principalement André Weil qui introduisit, vers la fin des années 1930, un formalisme permettant de démontrer rigoureusement leurs résultats.

Après 1930, les écoles américaine (Zariski, Mumford...), allemande (Noether, Brauer), russe (Kolmogorov...) et française (Weil, Chevalley...) développèrent sous une forme plus algébrique l'étude des variétés sur un corps commutatif quelconque en utilisant essentiellement la théorie des anneaux.

Dans les années 1950, elle fut totalement transformée par les travaux de l'école française sous l'impulsion de Pierre Samuel, d'Henri Cartan, de Jean-Pierre Serre et d'Alexandre Grothendieck.

Ce document a pour but d'expliquer le lien entre la géométrie et l'algèbre à travers la correspondance des ensembles algébriques de K^n et les idéaux de $K[X_1, ..., X_n]$.
Tous nos anneaux sont supposés commutatifs.

Ce rapport se décompose en plusieurs parties. Nous devons tout d'abords introduire du vocabulaire algébriste dont nous allons avoir besoin tout au long de ce sujet, et ainsi se remémorer/découvrir quelques propriétés importantes.
Nous entamons ensuite un des théorèmes fondamental en algèbre commutative, le Nullstellensatz, qui nous permettra de créer un véritable dictionnaire algèbre $\longleftrightarrow$ géométrie.
Nous verrons ensuite le sujet d'une manière topologique, mais avec une topologie particulière, propre à ce domaine d'algèbre commutative, et allons étudier quelques propriétés intéressantes de cette topologie.
Pour terminer, nous allons parler de la dimension d'un ensemble algébrique.

1 Définitions, premières propriétés

1.1 Un peu d'algèbre

Définition 1.1.1. *Soit A un anneau commutatif. A est dit* ***noethérien*** *si tous ses idéaux sont de type fini.*

Lemme 1.1.1. *Soit A un anneau. Soit $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq I_{n+1} \subseteq ...$ une suite croissante d'idéaux. Alors, $I = \cup_{n\in\mathbb{N}} I_n$ est un idéal.*

Démonstration. $0 \in I$ trivial.
Soient $a, b \in I$. $\exists j, i \in \mathbb{N}$ tels que $a \in I_i$ et $b \in I_j$. Supposons $j \geq i$. On a donc $a \in I_j$ et donc $a - b \in I_j \subseteq I$.
Soient $a \in A$ et $b \in I$. $\exists j \in \mathbb{N}$ tel que $b \in I_j$. Comme I_j idéal, on a $ab \in I_j \subseteq I$. □

Théorème 1.1.1. *Un anneau A est noethérien si et seulement si, dans A, toute suite croissante d'idéaux est stationnaire.*

Démonstration. "$\Rightarrow$" Soit A un anneau tel que tous ses idéaux sont de type fini. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. i.e :
$I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq I_{n+1} \subseteq ...$ Soit I$= \bigcup\limits_{n\in\mathbb{N}} I_n$. Comme A est noethérien, I est de type fini. Il existe donc $(a_1, ..., a_n) \in A^n$ tel que $I =< a_1, ..., a_n >$. D'où :
$\forall i \in \{1, ..., n\}, a_i \in \bigcup\limits_{n\in\mathbb{N}} I_n$. $\forall i \in \{1, ..., n\} \exists j \in \mathbb{N} : a_i \in I_j$
Comme la suite $(I_n)_{n\in\mathbb{N}}$ est croissante, $\exists n_j \in \mathbb{N}$ tel que $a_1, ..., a_n \in I_{n_j}$. D'où $< a_1, ..., a_n > \subseteq I_{n_j}$
Donc $I_{n_j} = I = \bigcup\limits_{n\in\mathbb{N}} I_n$. La suite est donc stationnaire.
"$\Rightarrow$" Soit $I \subseteq A$ un idéal de A. Montrons que I est de type fini.
Si $I = (0)$, on a fini.
Sinon, $\exists a_0 \in A$ tel que $a_0 \in I$. On obtient donc :

$$(0) \subsetneq < a_0 > \subseteq I.$$

Si $I =< a_0 >$, on a terminé. Sinon $\exists a_1 \in I$ tel que $a_1 \neq a_0$. On obtient donc :

$$(0) \subsetneq < a_0 > \subsetneq < a_0, a_1 > \subseteq I.$$

Ce processus doit s'arrêter car sinon, on aurait une suite croissante d'idéaux non stationnaire. □

Théorème 1.1.2 (De base de Hilbert)**.** *Soit A un anneau noethérien. Alors $A[X]$ est noethérien.*

Démonstration. Soit A un anneau noethérien. Soit I un idéal de A[X]. Montrons que I est de type fini.
$\forall i \geq 0$, on pose :

$$I_i = \{c \in A \mid \exists f \in I : f = cX^i + g\}$$

(où g est un polynôme de degré $< i$).
Montrons que les I_i sont des idéaux.
$0 \in I_i$ trivial.
Soient $a, b \in I_i$. $\exists f, g, g_1, g_2 \in I$ tels que $f = aX^i + g_1$ et $g = bX^i + g_2$. Soit h=f+g. $h \in I$ car I idéal et $h = (a+b)X^i + g_1 + g_2$ et $g_1 + g_2$ est un polynôme de degré $< i$. Donc $a + b \in I_i$.
Soit $a \in I_i$ et $b \in A$. $\exists f, g \in I$ tel que $f = aX^i + g$. On sait que $bf \in I$ car I idéal de $A[X]$ et $b \in A[X]$. On a $bf = baX^i + bg$ avec bg de degré $< i$ car $\deg(b) = 0$. Donc $\forall i \geqslant 0, I_i$ est un idéal de A.
Soit $c \in I_i$. $\exists f \in I$ tel que $f = cX^i + g$. On a $Xf \in I$ par la propriété d'absorption. Donc, $\exists h \in I$ tel que $h = cX^{i+1} + Xg$. Donc $c \in I_{i+1}$. Donc,$(I_n)_{n \in \mathbb{N}}$ est une suite croissante d'idéaux de A, elle est donc stationnaire. Donc, $\exists d \geq 0$ tel que $I_i = I_d$ si $i \geq d$.
Soit $n_i \in \mathbb{N}$. $\forall i \leqslant d$, soit $c_{i,j}, 1 \leqslant j \leqslant n_i$ les générateurs des I_i, ie : $I_i =< c_{i,1}, ..., c_{i,n_i} >$
$\forall i, j$, soit $f_{i,j} = c_{i,j}X^i + g_{i,j} \in I$, les polynômes correspondants aux $c_{i,j}$.
Alors, $I =< f_{i,j} >$.
En effet, sinon : $\exists f \in I \setminus \sum\limits_{i,j} A[X]f_{i,j}$ de degré minimal. Soit $n = deg(f)$. On a $f = cX^n + g$.

— Si $n \geq d$, alors $c \in I_n = I_d$ (suite stationnaire). Donc, $\exists (\lambda_j)_j \in A^{n_d}$ tel que $c = \sum\limits_j \lambda_j c_{d,j}$.
  Alors, $f - X^{n-d} \sum\limits_j \lambda_j f_{d,j} \in I \setminus \sum\limits_{i,j} A[X]f_{i,j}$ (car sinon f serait dans l'idéal engendré par les $f_{i,j}$) est de degré strictement inférieur à n, ce qui est absurde.

— Si $n < d$, alors $c \in I_n$ et donc $\exists (\lambda_j)_j \in A^{n_n}$ tel que $c = \sum\limits_j \lambda_j c_{n,j}$.
  Ainsi $f - \sum\limits_j \lambda_j f_{n,j} \in I \setminus \sum\limits_{i,j} A[X]f_{i,j}$ est également de degré inférieur strictement à n, ce qui est impossible.

□

Corollaire 1.1.1. *$K[X_1, ..., X_n]$ est noethérien.*

Démonstration. Les idéaux de K sont $0 = (0)$ et $K = (1)$. Donc K est noethérien, on obtient donc par récurrence que, $\forall n \in \mathbb{N}$, $K[X_1, ..., X_n]$ est noethérien. □

1.2 Lien avec les ensembles algébriques

Définition 1.2.1. *(Ensemble algébrique)*
Soit K un corps. Soit n $\geq$1 un entier. Soit $(P_i)_{i \in I}$ une collection d'éléments de

$K[X_1, ..., X_n]$. On définit $V((P_i)_{i\in I})$ un ***ensemble algébrique*** *de la manière suivante :*
$V((P_i)_{i\in I}) = \{X = (x_1, ..., x_n) \in K^n, \forall i \in I, P_i(x_1, ..., x_n) = 0\}$

Exemple 1.2.1.

1. *Si les P_i sont de degré 1, on retrouve les sous-variétés linéaires affines de K^n. C'est-à-dire les droites, les plans,... Si P est de degré 2, c'est une conique : (Intersection d'un plan avec un cône de révolution : cercle, ellipse, parabole, hyperbole).*
2. *$n = 2$, et $K = \mathbb{R}$. $V(P) = \{(x, y) \in \mathbb{R}^2, P(x, y) = 0\}$. Ce sont les courbes planes.*
3. *Dans l'espace K^3, une équation $P(x, y, z) = 0$ définit une surface.*
4. *$SL_n(K) = \{A \in M_n(K) \mid det(A) = 1\}$: En effet*
   $det([M_{i,j}]) = \sum_{\sigma\in G_n} \varepsilon(\sigma) \prod_{i=1}^{n} M_{i,\sigma(i)}$
5. *$O_n(K) = \{A \in M_n(K) \mid {}^tAA = I_d\}$*
6. *Un point de K^n est un ensemble algébrique :*
   $\{a_1, ..., a_n\} = V(X_1 - a_1, ..., X_n - a_n)$.

Définition 1.2.2. *On appelle* ***hypersurface*** *de K^n tout ensemble algébrique défini par un polynôme non constant.*

Proposition 1.2.1. *$V((P_i)_{i\in I}) = V(< P_i >_{i\in I})$*

Démonstration. Soit $x \in K^n$ tel que $x \in V((P_i)_{i\in I})$. $\forall i \in I, P_i(x) = 0$. Soit $Q \in< Pi >_{i\in I}$. On peut écrire $Q = \sum_{i\in I} Q_i P_i$ avec les Q_i presque tous nuls.
$Q(x) = \sum_{i\in I} Q_i(x)P_i(x) = 0$. Donc, $x \in V(< P_i >_{i\in I})$.
Soit $x \in V(< P_i >_{i\in I})$. $\forall Q \in< P_i >_{i\in I}$, $Q(x) = 0$.
Comme $(P_i)_{i\in I} \subseteq < P_i >_{i\in I}$, on a $x \in V((P_i)_{i\in I})$. □

Proposition 1.2.2. *$V(< P_i >_{i\in I}) = V(< P_j >_{1\leqslant j\leqslant m})$ pour un certain $m \in \mathbb{N}$.*

Démonstration. Comme $K[X_1, ..., X_n]$ est noethérien, $< P_i >_{i\in I} := \{$idéal engendré par les $P_i\}$, est de type fini. Donc $< P_i >_{i\in I}=< P_j >_{1\leqslant j\leqslant n}$. □

2 Théorème des zéros de Hilbert (Nullstellensatz)

2.1 Correspondance des ensembles algébriques avec les idéaux de $K[X_1, ..., X_n]$

A tout idéal I de $K[X_1, ..., X_n]$, on associe un ensemble algébrique :

$$I \mapsto V(I) := X$$

A toute partie de K^n, on associe :

$$X \mapsto \mathscr{I}(X) = \{P \in K[X_1, ..., X_n] \mid \forall x \in X, P(x) = 0\}.$$

Proposition 2.1.1. *Soit $X \subseteq K^n$.*
$\mathscr{I}(X) = \{P \in K[X_1, ..., X_n] \mid \forall x \in X, P(x) = 0\}$ est un idéal de $K[X_1, ..., X_n]$.

Démonstration. Soit $X \subseteq K^n$. $\forall x \in X, 0(x)$ (polynôme nul) $= 0$. Donc $0 \in \mathscr{I}(X)$.
Soient P,Q $\in \mathscr{I}(X)$. Soit $x \in X$ $(P-Q)(x) = P(x) - Q(x) = 0$. Donc $P - Q \in \mathscr{I}(X)$.
Soit $P \in K[X_1, ..., X_n], Q \in \mathscr{I}(X)$. Soit $x \in X$. $PQ(x) = P(x)Q(x) = 0$.
Donc, PQ $\in \mathscr{I}(X)$. □

Proposition 2.1.2. *Soit S une partie de $K[X_1, ..., X_n]$. On a $S \subseteq \mathscr{I}(V(S))$.*

Démonstration. Soit $P \in S$. Soit $x \in V(S)$. On a $P(x) = 0$.
Donc $P \in \mathscr{I}(V(S))$. □

Proposition 2.1.3. *Soit X une partie de K^n. On a $X \subseteq V(\mathscr{I}(X))$.*

Démonstration. Soit $x \in X$. Soit $P \in \mathscr{I}(X)$. $P(x) = 0$. Donc $x \in V(\mathscr{I}(X))$. □

⚠ Ces inclusions peuvent être strictes !

2.2 Lien avec les radicaux

Définition 2.2.1. *Soit I un idéal de $K[X_1, ..., X_n]$. On définit le **radical** de I de la manière suivante :*
$\sqrt{I} = \{P \in K[X_1, ..., X_n] \mid \exists m \in \mathbb{N}^*, P^m \in I\}$.

Proposition 2.2.1. *$\sqrt{I}$ est un idéal de $K[X_1, ..., X_n]$.*

Démonstration. $0 \in \sqrt{I}$ car $0^1 \in I$.
Soient $P, Q \in \sqrt{I}$. $\exists m, n \in \mathbb{N}$ tels que $P^n \in I$ et $Q^m \in I$.
$(P-Q)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} P^k Q^{n+m-k}(-1)^{n+m-k}$.
Si $k \geq n$, $P^k = P^{n+k-n} = (P^n)^{k-n} \in I$ (Car $P^n \in I$).
Donc $\sum_{k=n}^{n+m} \binom{n+m}{k} P^k Q^{n+m-k}(-1)^{n+m-k} \in I$.
Si $k \leqslant n$, $Q^{n+m-k} = (Q^m)^{n-k} \in I$ (car $Q^m \in I$).
Donc $\sum_{k=0}^{n} \binom{n+m}{k} P^k Q^{n+m-k}(-1)^{n+m-k} \in I$.
On obtient donc $(P-Q)^{n+m} \in I$.
Soit $P \in K[X_1, ..., X_n]$ et $Q \in I$.$\exists n \in \mathbb{N}$ tel que $Q^n \in I$.
Alors $(PQ)^n = P^n Q^n \in I$. □

Exemple 2.2.1. $\sqrt{< X^2, Y >} = < X, Y >$

Démonstration. "$\subseteq$" Soit $P \in < X, Y >$. $\exists Q_1, Q_2 \in K[X, Y]$ tels que
$P = Q_1 X + Q_2 Y$.
$P^2 = (Q_1 X + Q_2 Y)^2$
$P^2 = Q_1^2 X^2 + Q_2^2 Y^2 + 2 Q_1 Q_2 X Y$
$P^2 = Q_1^2 X^2 + Y(Q_2^2 Y + 2 X Q_1 Q_2)$
$P^2 \in < X^2, Y >$.
Donc, $P \in \sqrt{< X^2, Y >}$.
"$\supseteq$" Soit $P \in \sqrt{< X^2, Y >}$. $\exists n \in \mathbb{N}$ tel que $P \in < X^2, Y >$. Donc, $\exists Q_1, Q_2 \in K[X, Y]$ tels que
$P^n = Q_1 X^2 + Q_2 Y$
X est un polynôme non nul de $K[X, Y]$, on peut donc effectuer la division euclidienne de P par X dans $K[X, Y]$. On obtient l'existence et l'unicité de deux polynômes P_1 et R_1 tels que :
$P = P_1 X + R_1$ avec $\deg_X(R_1) < 1$ i.e : $R_1 \in K[Y]$. De même, Y est un polynôme non nul de $K[Y]$, on peut donc effectuer la division euclidienne de R_1 par Y dans $K[Y]$. On obtient l'existence et l'unicité de deux polynômes P_2 et R_2 tels que :
$P = P_1 X + R_1 = P_1 X + P_2 Y + R_2$ avec $\deg_Y(R_2) < 1$ i.e $R_2 \in K$.
Mais on a $P^n = Q_1 X^2 + Q_2 Y$ donc $P^n(0,0) = 0$. Comme K est intègre, on obtient $P(0,0) = R_2 = 0$. Donc, $P \in < X, Y >$. □

Définition 2.2.2. *Soit I un idéal d'un anneau A. On dit que I est* ***radical*** *si $I = \sqrt{I}$.*

Proposition 2.2.2. $I \subseteq \sqrt{I} \subseteq \mathscr{I}(V(I))$

Démonstration. Soit $P \in I$. On a $P^1 \in I$. Donc $I \subseteq \sqrt{I}$.
Soit $P \in \sqrt{I}$. $\exists n \in \mathbb{N}$ tel que $P^n \in I$. Soit $x \in V(I)$. On a $P^n(x) = 0$. Donc $P(x) = 0$ car K est un corps, il est donc intègre. Donc $P \in \mathscr{I}(V(I))$. □

Proposition 2.2.3. *Si I est un idéal premier, on a $\sqrt{I} = I$.*

Démonstration. On a déjà $I \subseteq \sqrt{I}$. Montrons l'inclusion inverse.
Soit $P \in \sqrt{I}$. $\exists n \in \mathbb{N}$ tel que $P^n \in I$. Comme I est premier, on a $P^n = P^{n-1} * P \in I \Rightarrow P \in I$ ou $P^{n-1} \in I$. Si $P \notin I, P^{n-1} \in I$. En réitérant ce procédé, on obtient $P \in I$. □

Question : Si $I = \sqrt{I}$, a-t'on $\mathscr{I}(V(I)) = I$?
$\hookrightarrow$ ***NON***

Exemple 2.2.2. *$K = \mathbb{R}$, $I =< X^2 + 1 >$. $V(I) = \{x \in \mathbb{R}, x^2 + 1 = 0\} = \emptyset$*
$\mathscr{I}(\emptyset) = \mathbb{R}[X]$ mais $I \neq \mathbb{R}[X]$.
Et on a bien $I = \sqrt{I}$ car :
$\mathbb{R}[X]/I \cong \mathbb{C}$, qui est un corps, donc intègre, donc I est premier, il est donc radical.

La correspondance ensemble algébrique $\leftrightarrow$ idéal n'est donc pas bijective. D'ailleurs, des idéaux différents peuvent donner le même ensemble algébrique, comme par exemple dans $K[X]$,
$< x > \neq < x^2 >$ mais $V(< x >) = V(< x^2 >) = \{0\}$.

Nous allons maintenant introduire un théorème fondamentale en algèbre commutative : le Nullstellensatz.
Si $K = \overline{K}$. On se place dans $K[X]$. Comme K est un corps, $K[X]$ est principal et donc tout idéal I s'écrit sous la forme $I =< f >$ pour un certain f dans $K[X]$. Comme K est algébriquement clos, tout polynôme non nul non constant admet au moins une racine. Donc, si $V(I) = \emptyset$, on a forcément f constant non nul. On a donc $\frac{1}{f} \in K$ donc $\frac{1}{f} * f = 1 \in I$ donc $I = K[X]$.
Réciproquement, si $I = K[X]$, $V(I) = \{x \in K \mid P(x) = 0 \ \forall P \in K[X]\}$. On voit trivialement que, sous ces conditions, on a forcément $V(I) = \emptyset$ car par exemple il n'y a pas de racine commune au polynôme X et X-1.

Le Nullstellensatz version faible nous dit que cette propriété reste vraie avec les polynômes de plusieurs variables ! Le Nullstellensatz version forte va nous donner des hypothèses nécessaires et suffisantes pour que l'on ai une bijection ensemble algébrique $\leftrightarrow$ idéal.

2.3 Le Nullstellensatz, version faible

Théorème 2.3.1. *(Nullstellensatz, version faible) Si $K = \overline{K}$ un corps non dénombrable, soit $I \subseteq K[X_1, ..., X_n]$ un idéal **propre**. Alors $V(I) \neq \emptyset$.*

Pour démontrer ce théorème, nous avons besoin de quelques résultats préliminaires.

Théorème 2.3.2. *Les idéaux maximaux de $K[X_1, ..., X_n]$ sont les idéaux de la forme :*

$$I_{\alpha_1,...,\alpha_n} = (X_1 - \alpha_1, ..., X_n - \alpha_n).$$

Pour un certain $(\alpha_1, ..., \alpha_n) \in K^n$.

Démonstration. "$\Leftarrow$" Montrons que les idéaux $I_{\alpha_1,...,\alpha_n}$ sont bien maximaux. Pour cela, nous allons montrer que $I_{\alpha_1,...,\alpha_n}$ est le noyau de cette application :

$$\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n} : K[X_1, ..., X_n] \to K$$
$$X_1 \mapsto \alpha_1$$
$$...$$
$$X_n \mapsto \alpha_n$$

$\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n}$ est le prolongement de l'application $id : K \to K$, par propriété universelle des polynômes. Elle est donc surjective car id l'est. Effectuons le raisonnement par récurrence sur n :
(Initialisation) : Si n=1. Montrons que $(X_1 - \alpha_1)$ est le noyau de l'application :

$$\varphi_{X_1\mapsto\alpha_1} : K[X_1] \to K$$
$$X_1 \mapsto \alpha_1$$

Soit $P \in (X_1 - \alpha_1)$. $\exists Q \in K[X_1]$ tel que $P = Q(X_1 - \alpha_1)$. On a donc $\varphi_{X_1\mapsto\alpha_1}(P) = \varphi_{X_1\mapsto\alpha_1}(Q)\varphi_{X_1\mapsto\alpha_1}(X_1 - \alpha_1) = 0$. Donc, $P \in Ker(\varphi_{X_1\mapsto\alpha_1})$.
Soit $P \in Ker(\varphi_{X_1\mapsto\alpha_1})$. Comme $X_1 - \alpha_1$ est non nul dans $K[X_1]$, on peut effectuer la division euclidienne de P par $X_1 - \alpha_1$. On obtient donc l'existence et l'unicité de deux polynômes P_1 et $P_2 \in K[X_1]$ tels que $P = P_1(X_1 - \alpha_1) + P_2$ avec $\deg_{X_1}(P_2) < 1$, i.e $P_2 \in K$.
On applique $\varphi_{X_1\mapsto\alpha_1}$ à cette égalité pour obtenir :
$\varphi_{X_1\mapsto\alpha_1}(P) = 0 = \varphi_{X_1\mapsto\alpha_1}(P_2) = P_2$ car $P_2 \in K$. On obtient bien
$P \in (X_1 - \alpha_1)$. Donc $Ker(\varphi_{X_1\mapsto\alpha_1}) = (X_1 - \alpha_1)$.
(Hérédité) : Supposons pour n fixé que $I_{\alpha_1,...,\alpha_n}$ est le noyau de l'application $\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n}$. Soit $\varphi_{X_{n+1}\mapsto\alpha_{n+1}} : K[X_1, ..., X_{n+1}] \to K$ le prolongement de l'application $\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n}$ par propriété universelle des polynômes. L'application $\varphi_{X_{n+1}\mapsto\alpha_{n+1}}$ est surjective car $\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n}$ l'est. Cherchons $Ker(\varphi_{X_{n+1}\mapsto\alpha_{n+1}})$. Soit $P \in Ker(\varphi_{X_{n+1}\mapsto\alpha_{n+1}})$. Comme $X_{n+1} - \alpha_{n+1}$ est non nul dans $K[X_1, ..., X_{n+1}]$, on peut effectuer la division euclidienne de P par $X_{n+1} - \alpha_{n+1}$. On obtient l'existence et l'unicité de deux polynômes, P_1 et P_2 dans $K[X_1, ..., X_{n+1}]$ tels que

$$P = P_1(X_{n+1} - \alpha_{n+1}) + P_2$$

avec $\deg_{X_{n+1}}(P_2) < 1$, donc $P_2 \in K[X_1, ..., X_n]$. On a ainsi :
$\varphi_{X_{n+1}\mapsto\alpha_{n+1}}(P) = \varphi_{X_{n+1}\mapsto\alpha_{n+1}}(P_1(X_{n+1} - \alpha_{n+1}) + P_2) =$
$\varphi_{X_{n+1}\mapsto\alpha_{n+1}}(P_2) = \phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n}(P_2) = 0$
(Car $P \in Ker(\varphi_{X_{n+1}\mapsto\alpha_{n+1}})$). D'après l'hypothèse de récurrence, on a $P_2 \in I_{\alpha_1,...,\alpha_n}$. Donc, $P \in I_{\alpha_1,...,\alpha_{n+1}}$. L'inclusion réciproque est triviale.
Donc, $\forall n \in \mathbb{N}, I_{\alpha_1,...,\alpha_n} = Ker(\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n})$.
D'après le premier théorème d'isomorphisme de Noether, on obtient :

$$\frac{K[X_1, ..., X_n]}{I_{\alpha_1,...,\alpha_n}} \cong K$$

Comme K est un corps, on en déduit que $I_{\alpha_1,...,\alpha_n}$ est maximal.

"$\Rightarrow$" : Montrons que tout idéal maximal de $K[X_1, ..., X_n]$ est de cette forme.
Soit I un idéal maximal de $K[X_1, ..., X_n]$. Montrons que $\exists(\alpha_1, ..., \alpha_n) \in K^n$ tel que $I = I_{\alpha_1,...,\alpha_n}$.
$\forall j \in \{1, ..., n\}$, on considère l'application :

$$\varphi_j : K[X_j] \overset{i}{\hookrightarrow} K[X_1, ..., X_n] \overset{\pi}{\to} \frac{K[X_1, ..., X_n]}{I}$$

$K[X_j]$ est principal car K est un corps, donc $Ker(\varphi_j) = (P)$ pour un certain $P \in K[X_j]$. Montrons que P est irréductible dans $K[X_j]$. Comme I est maximal, $\dfrac{K[X_1, ..., X_n]}{I}$ est un corps, il est donc intègre. Ainsi, $im(\varphi_j)$ est un sous-anneau intègre de $\dfrac{K[X_1, ..., X_n]}{I}$. Donc $Ker(\varphi_j)$ est premier. Donc P est premier.
Donc, **(Si P $\neq$ 0)***,P est irréductible.
Comme K est algébriquement clos, P est donc de la forme :
$(X_j - \alpha_j)$ avec $\alpha_j \in K$.
Donc, si I est maximal dans $K[X_1, ..., X_n]$, $\forall j \in 1, ..., n, \exists\alpha_j \in K$ tel que $X_j - \alpha_j \in I$. Donc $\forall j \in 1, ..., n, \exists\alpha_j \in K$ tel que $(X_j - \alpha_j) \subseteq I$. Donc si I maximal, $\exists(\alpha_1, ..., \alpha_n) \in K^n$ tel que $(X_1 - \alpha_1, ..., X_n - \alpha_n) \subseteq I$. Ces deux idéaux étant maximaux, on a l'égalité.
* : Montrons que $P \neq 0$. Supposons par l'absurde qu'il existe un morphisme injectif $\varphi : K[X_j] \to k := K[X_1, ..., X_n]/I$. C'est donc un morphisme injectif, de l'anneau intègre $K[X]$ vers le corps k. Par propriété universelle du corps des fraction, φ se prolonge en un morphisme qui reste injectif $\tilde{\varphi} : K(X) \to k$ (la définition est donnée par $\tilde{\varphi}(P/Q) = \dfrac{\varphi(P)}{\varphi(Q)}$ dès que cela fait sens). Montrons que c'est impossible.
Tout d'abord, K est un sous anneau de $K(X)$ et k, comme on peut le voir en remarquant que $I \cap K$ est réduit à 0. Ces deux anneaux sont donc muni d'une structure de K espace vectoriel, la multiplication scalaire provenant

de la multiplication dans chacun de ces anneaux. De plus, si $x \in K \subset K(\mathrm{X})$, alors $\tilde{\varphi}(x) = \varphi(x) = x \in k$

Ceci permet de voir que $\tilde{\varphi}$ est une application K-linéaire, qui est injective par propriété universelle.

Ainsi, l'image d'une famille libre de $K(\mathrm{X})$ par $\tilde{\varphi}$ est libre dans k (toujours pour les structures de K-espace vectoriel). On va montrer que la famille F des $\left(\dfrac{1}{X-c}\right)_{c\in K}$, est libre dans $K(\mathrm{X})$. On considère donc une expression $\displaystyle\sum_{finie} \lambda_c \frac{1}{X-c} = 0, \lambda_c \in K$ et on veut montrer que chaque λ_c est nul. Ceci est vrai par unicité du développement en éléments simple de 0 (par exemple, on peut aussi considérer la dérivabilité pour un argument plus élémentaire).

La famille image $\tilde{\varphi}(\mathrm{F})$ est donc une famille libre de k, de cardinal indénombrable (car K n'est pas dénombrable). Or, en tant que K espace vectoriel, k est engendré par les classes (modulo I) de la forme $X_1^{\alpha_1}...X_n^{\alpha_n}$, en nombre dénombrable. La dimension de k comme K espace vectoriel est donc au plus dénombrable. La théorie de la dimension (qui marche, en dimension infinie, grâce à l'axiome du choix) fournit une contradiction, car alors toute famille libre de k est de cardinal au plus dénombrable.

□

On a donc montré que les idéaux maximaux de $K[X_1, ..., X_n]$ sont les idéaux de la forme :

$$I_{\alpha_1,...,\alpha_n} = (X_1 - \alpha_1, ..., X_n - \alpha_n).$$

Prouvons maintenant le Nullstellensatz version faible.

Démonstration. (Nullstellensatz, version faible)

Soit $I \subseteq K[X_1, ..., X_n]$ un idéal propre.

$V(I) = \{X = (\alpha_1, ..., \alpha_n) \in K^n, \forall P \in I, P(\alpha_1, ..., \alpha_n) = 0\}$

$V(I) = \{X = (\alpha_1, ..., \alpha_n) \in K^n, \forall P \in I, \phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n}(P) = 0\}$

$V(I) = \{X = (\alpha_1, ..., \alpha_n) \in K^n \mid I \subseteq Ker(\phi_{X_1\mapsto\alpha_1,...,X_n\mapsto\alpha_n})\}$

$V(I) = \{X = (\alpha_1, ..., \alpha_n) \in K^n \mid I \subseteq (X_1 - \alpha_1, ..., X_n - \alpha_n)\}$

D'après le théorème de Krull, il existe I_{max} un idéal maximal de $K[X_1, ..., X_n]$ tel que $I \subseteq I_{max}$.

Comme tous les I_{max} sont de la forme $(X_1 - \alpha_1, ..., X_n - \alpha_n)$, on a $V(I) \neq \emptyset$.

□

2.4 Le Nullstellensatz, version forte

Théorème 2.4.1. *(Nullstellensatz, version forte) Si K est algébriquement clos et $I \subseteq K[X_1, ..., X_n]$ est un idéal, alors :*

$$\mathscr{I}(V(I)) = \sqrt{I}$$

Pour montrer ce résultat, nous allons avoir besoin du lemme suivant :

Lemme 2.4.1. *Soit K un corps et $I =< f_1, ..., f_s >\subseteq K[X_1, ..., X_n]$. Alors $f \in \sqrt{I}$ si et seulement si $1 \in J :=< f_1, ..., f_s, 1 - Yf >\subseteq K[X_1, ..., X_n, Y]$.*

Démonstration. "$\Rightarrow$" On suppose $f \in \sqrt{I}$. $\exists m \in \mathbb{N}$ tel que $f^m \in I$.
On a : $1 = Y^m f^m + (1 - Y^m f^m)$.
$1 = Y^m f^m + (1 - Yf)(1 + Yf + ... + Y^{m-1} f^{m-1})$
Or, comme $I \subseteq J$, on a $f^m \in J$, d'où $Y^m f^m \in J$ car J idéal de $K[X_1, ..., X_n, Y]$.
Donc, $1 \in J$.
"$\Leftarrow$". Soit $f \in K[X_1, \cdots, X_n]$. On suppose $1 \in J$
On peut donc écrire : $1 = \sum_{i=1}^{s} p_i f_i + q(1 - Yf)$ avec les $(p_i)_{i\in(1,..,s)}$ et $q \in K[X_1, ..., X_n, Y]$.
En évaluant en $Y = \frac{1}{f}$, on a :
$1 = \sum_{i=1}^{s} p_i(X_1, ..., X_n, \frac{1}{f}) f_i$
On multiplie par f^m pour m assez grand (m=max($\deg_{X_i}(dnominateurs)$)) et on obtient :
$f^m = \sum_{i=1}^{s} \tilde{p}_i f_i \in I$ car les $\tilde{p}_i \in K[X_1, ..., X_n]$. □

Démonstration du Nullstellensatz. Soit $I \subseteq K[X_1, ..., X_n]$ un idéal. Montrons que $\mathscr{I}(V(I)) = \sqrt{I}$.

On a déjà vu $\mathscr{I}(V(I)) \supseteq \sqrt{I}$. Montrons que $\mathscr{I}(V(I)) \subseteq \sqrt{I}$.

Soient $f_1, ..., f_s$ tels que $I =< f_1, ..., f_s >$ et soit $f \in \mathscr{I}(V(I))$.
On considère, via l'injection canonique, que les f_i sont dans $K[X_1, ..., X_n, Y]$.
Soit $J =< f_1, ..., f_s, 1 - Yf >$. Montrons que $V(J) = \emptyset$.
Raisonnons par l'absurde. Si $(x_1, ..., x_n, y) \in V(J)$, on a :
$f_i(x_1, ..., x_n, y) = 0$ car $(x_1, ..., x_n, y) \in V(J)$. On a alors $(x_1, ..., x_n, y) \in V(I)$.
Donc $f(x_1, ..., x_n, y) = 0$ car $f \in \mathscr{I}(V(I))$.
$\Rightarrow (1 - Yf)(x_1, ..., x_n, y) = 1 \neq 0$ ce qui est absurde par hypothèse.
Donc $V(J) = \emptyset$.
Donc, d'après le Nullstellenstz version faible, $J = K[X_1, ..., X_n]$. Donc $1 \in J$.
Donc, d'après le lemme, $f \in \sqrt{I}$. □

Ce théorème très puissant nous permet donc de créer un nouveau dictionnaire algèbre-géométrie.

2.5 Conséquences et applications du Nullstellensatz

Proposition 2.5.1. *Soit V un ensemble algébrique de K^n. Alors, $\mathscr{I}(V)$ est un idéal radical.*

Démonstration. On a déjà montré que $\mathscr{I}(V)$ est un idéal. Montrons qu'il est radical. Il suffit de montrer que $\sqrt{\mathscr{I}(V)} \subseteq \mathscr{I}(V)$.
Soit $P \in \sqrt{\mathscr{I}(V)}$. $\exists n \in \mathbb{N}$ tel que $P^n \in \mathscr{I}(V)$. Soit $x \in V$. On a $P^n(x) = 0$. Comme K est intègre, on a $P(x) = 0$. Donc $P \in \mathscr{I}(V)$. □

Corollaire 2.5.1. *(Du Nullstelensatz) Soit K un corps algébriquement clos. On a une bijection **décroissante***
$\mathscr{I}$: {*Ensembles algébriques de* K^n } $\longrightarrow$ {*Idéaux radicaux de* $K[X_1, \cdots, X_n]$}

$$X \longmapsto \mathscr{I}(X)$$

V : {*Idéaux radicaux de* $K[X_1, \cdots, X_n]$} $\longrightarrow$ {*Ensembles algébriques de* K^n}

$$I \longmapsto V(I)$$

Démonstration.

Montrons que si $X_1 \subseteq X_2$, alors $\mathscr{I}(X_2) \subseteq \mathscr{I}(X_1)$.
Soient $X_1 \subseteq X_2 \subseteq K^n$ deux ensembles algébriques de K^n. Soit $P \in \mathscr{I}(X_2)$. Soit $x \in X_1$. On a $x \in X_2$ donc $P(x) = 0$ donc $P \in \mathscr{I}(X_1)$.

Montrons que si $I_1 \subseteq I_2$, alors $V(I_2) \subseteq V(I_2)$. Soient $I_1 \subseteq I_2$ deux idéaux radicaux de $K[X_1, ..., X_n]$. Soit $x \in V(I_2)$. Soit $P \in I_1$. Alors, $P \in I_2$ donc $P(x) = 0$. Ainsi, $x \in V(I_1)$.

Soit I un idéal radical. Grâce au Nullstellensatz, on sait que

$$\mathscr{I}(V(I)) = \sqrt{I} = I.$$

Montrons maintenant que, pour tout ensemble algébrique X, on a

$$V(\mathscr{I}(X)) = X.$$

Soit $x \in X$. Soit $P \in \mathscr{I}(X)$. Par définition, $P(x) = 0$ donc $x \in V(\mathscr{I}(X))$. Réciproquement, comme X est un ensemble algébrique de K^n, il se définit de la manière suivante : $X = V(< f_1, ..., f_s >)$ pour des certains $f_1, ..., f_s \in K[X_1, ..., X_n]$. Par définition de $\mathscr{I}(X)$, on a $f_1, ..., f_s \in \mathscr{I}(X)$. Comme $\mathscr{I}(X)$ est un idéal, on a $< f_1, ..., f_s > \subseteq \mathscr{I}(X)$. Maintenant, comme $I \mapsto V(I)$ est décroissante, on a $V(\mathscr{I}(X)) \subseteq V(< f_1, ..., f_s >) = X$. □

3 Notion d'irréductibilité, topologie

3.1 Irréductibilité

Définition 3.1.1. *Un espace topologique X est dit **irréductible** s'il est non vide et s'il n'est pas la réunion de deux fermés stricts (i.e $\neq X$).*

Exemple 3.1.1. *Les espaces séparés irréductibles sont réduits à un point.*

Démonstration. Soit $(X, \mathscr{T}_X)$ un espace topologique séparé irréductible. Supposons que X ne soit pas réduit à un point. Donc, $\exists a, b \in X$ tels que $a \neq b$. Comme $a \neq b$ et que X est séparé, $\exists U, V$ deux ouverts de $\mathscr{T}_X$ tels que $a \in U, b \in V$ et $U \cap V = \emptyset$. Alors,

$$U^c \cup V^c = X$$

et X est l'union de deux fermés. Donc $U^c = X$ ou $V^c = X$. i.e $U = \emptyset$ ou $V = \emptyset$. Ceci est impossible car $a \in U$ et $b \in V$. Donc X est réduit à un point. Réciproquement, soit $\{x\}$ un singleton d'un espace topologique séparé X. On suppose $\{x\} = U \cup V$ avec U,V fermés. On a donc $x \in U$ ou $x \in V$ i.e $\{x\} = U$ ou $\{x\} = V$. Donc $\{x\}$ est bien irréductible. □

Proposition 3.1.1. *Soit X un espace topologique non vide. On a équivalence :*

1. *X est irréductible.*
2. *Si U, V sont deux ouverts de X avec $U \cap V = \emptyset$, on a $U = \emptyset$ ou $V = \emptyset$.*
3. *Tout ouvert non vide de X est dense.*

Démonstration.

1. $\Leftrightarrow$ 2. Supposons $\exists U, V$ deux ouverts de X tels que $U \cap V = \emptyset$. On a donc $(U \cap V)^c = \emptyset^c$
   $U^c \cup V^c = X$ Comme U^c et V^c sont fermés, on a $U^c = X$ ou $V^c = X$ i.e $U = \emptyset$ ou $V = \emptyset$.
   L'autre sens se fait par passage au complémentaire.
2. $\Rightarrow$ 3. Soit U un ouvert non vide de X. Montrons que $\overline{U} = X$. i.e Montrons que $\overline{U}^c = \emptyset$.
   Comme $\overline{U}$ est fermé, $\overline{U}^c$ est ouvert. On a $U \cap \overline{U}^c = \emptyset$ car si $x \in \overline{U}^c, x \notin \overline{U}$ donc $x \notin U$. On obtient donc, grâce à l'hypothèse 2), que $U = \emptyset$ ou $\overline{U}^c = \emptyset$. U étant supposé non vide, on obtient bien $\overline{U}^c = \emptyset$.
3. $\Rightarrow$ 2. Soient U,V deux ouverts de X tels que $U \cap V = \emptyset$. Supposons par l'absurde $U \neq \emptyset$ et $V \neq \emptyset$. On a donc $\overline{U} = X$ et $\overline{V} = X$
   Soit $x \in U$. Comme $\overline{V} = X$, on a $x \in \overline{V}$. Donc, pour tout ouvert W dans le voisinage de x, on a $W \cap V \neq \emptyset$. Or, U est un ouvert qui contient x, donc $U \cap V \neq \emptyset$, ce qui est impossible par hypothèse.

□

Proposition 3.1.2. *Soit X un espace topologique irréductible et $U \subseteq X$ un ouvert non vide de X. Alors, U est irréductible.*

Démonstration. Soient F, G fermés de U tels que $U = F \cup G$. On a $\overline{U} = \overline{F \cup G}$ i.e $X = \overline{F} \cup \overline{G}$ est une décomposition en deux fermés de X, on a donc $X = \overline{F}$ ou $X = \overline{G}$. Cela nous donne donc $X \cap U = \overline{F} \cap U$ ou $X \cap U = \overline{G} \cap U$. i.e $U = F$ ou $U = G$ car F et G sont des fermés de U. Donc U est irréductible. □

Dans le cas des ensembles algébriques affines, on a une caractérisation très simple des irréductibles en terme de l'idéal $\mathscr{I}(V)$. (cf suite du cours).

Exemple 3.1.2. *Dans* $\mathbb{R}[X, Y]$, $V(< XY >) = \{(x, y) \in \mathbb{R}^2 \mid xy = 0\}$ *n'est pas irréductible car il se décompose en ces deux fermés :* $\{(x, y) \in \mathbb{R}^2 \mid x = 0\}$ *et* $\{(x, y) \in \mathbb{R}^2 \mid y = 0\}$.

3.2 La topologie de Zariski

Définition 3.2.1. *Soit K un corps algébriquement clos. On définit la topologie de Zariski sur K^n comme étant la topologie dont les fermés sont les ensembles algébriques de K^n.*

Proposition 3.2.1. *La topologie de Zariski est une topologie sur K^n.*

Démonstration.
— $K^n = V(\{0\})$; $\emptyset = V(K[X_1, ..., X_n])$

— Montrons qu'une union finie de ensembles algébriques est un ensemble algébrique. Montrons pour cela que l'union de deux ensembles algébriques est un ensemble algébrique.
Soient I_1, I_2 deux idéaux de $K[X_1, ..., X_n]$.
Montrons que $V(I_1) \cup V(I_2) = V(I_1 I_2)$.
Soit $x \in V(I_1 I_2)$. On suppose $x \notin V(I_1)$. Soit $P \in I_2$. Comme $x \notin V(I_1)$, $\exists Q \in I_1$ tel que $Q(x) \neq 0$. On a $PQ(x) = P(x)Q(x) = 0$ car $PQ \in I_1 I_2$. Comme K est intègre, on en déduit $P(x) = 0$. Donc $x \in V(I_2)$.
Réciproquement, on a $I_1 I_2 \subseteq I_1$, donc $V(I_1) \subseteq V(I_1 I_2)$. De même $V(I_2) \subseteq V(I_1 I_2)$. On a donc $V(I_1) \cup V(I_2) \subseteq V(I_1 I_2)$, d'où l'égalité.

— Montrons qu'une intersection quelconque de ensembles algébriques est un ensemble algébrique. Soit $V(I_i)_{i \in I}$ une famille de ensembles algébriques. Montrons que $\bigcap\limits_{i \in I} V(I_i) = V(\bigcup\limits_{i \in I} I_i)$.
Soit $x \in \bigcap\limits_{i \in I} V(I_i)$. i.e $\forall i \in I, \forall P \in I_i, P(x) = 0$. Soit $P \in \bigcup\limits_{i \in I} I_i$. $\exists i \in I$ tel que $P \in I_i$. On a donc $P(x) = 0$. Donc $x \in V(\bigcup\limits_{i \in I} I_i)$.
Soit $x \in V(\bigcup\limits_{i \in I} I_i)$. $\forall P \in \bigcup\limits_{i \in I} I_i, P(x) = 0$. Soit $i \in I$. Soit $P \in I_i$. On a $P \in \bigcup\limits_{i \in I} I_i$. Donc P(x)=0. Donc $x \in V(P_i)$. Comme l'indice i est quelconque, on a $x \in \bigcap\limits_{i \in I} V(I_i)$, d'où l'égalité.

□

Exemple 3.2.1. *Sur K, les fermés sont : K et les sous-ensembles finis de K, car ce sont les ensembles constitués des racines d'un polynôme ou des racines communes de plusieurs polynômes en une indéterminée. Ainsi, si un ensemble algébrique est infini, il correspond forcément au polynôme nul, qui nous donne finalement tout K.*
Par exemple, $\{x_1, ..., x_n\} = V(\prod_{i=1}^{n}(X - x_i))$.

Définition 3.2.2. *Pour $X \subseteq K^n$, on introduit la topologie induite : les fermés sont les ensembles algébriques inclus dans X.*

⚠ Cette toplogie est très différente des topologies usuelles. Nous allons donc voir quelques propriétés de cette topologie pour pouvoir mieux la visualiser.

Définition 3.2.3. *Soit $(X, \mathscr{T}_X)$ un espace topologique. On dit que $(O_i)_{i\in I}$ est une* ***base de la topologie*** *$\mathscr{T}_X$ si tout ouvert de $\mathscr{T}_X$ est réunion d'éléments de $(O_i)_{i\in I}$.*

Proposition 3.2.2. *Soit $P \in K[X_1, ..., X_n]$ et V(P) l'hypersurface définie par P. L'ensemble D(P)=$K^n \setminus V(P)$ est un ouvert de Zariski. L'ensemble de ces ouverts forme une base de la topologie de Zariski.*

Définition 3.2.4. *Les ouverts de cette forme sont appelés les* ***ouverts standards****.*

Démonstration. Soit U un ouvert de Zariski. U^c est un fermé de Zariski. C'est donc un ensemble algébrique. Comme $K[X_1, ..., X_n]$ est noethérien, tout idéal est de type fini. On peut donc considérer un idéal de $K[X_1, ..., X_n]$ tel que $U^c = V(I) = V((P_1, ..., P_s)) = V(P_1) \cap ... \cap V(P_s)$ Pour des certains $P_1, ..., P_s \in K[X_1, ..., X_s]$. Donc $U = \bigcup_{i=1}^{s} V(P_i)^c$. □

Proposition 3.2.3. *Si K est infini, la topologie de Zariski n'est pas séparée.*

Démonstration. Pour montrer que cette topologie n'est pas séparée, il suffit de montrer que deux ouverts non vide s'interceptent toujours.
Supposons qu'il existe deux ouverts U, W non vides tels que $U \cap W = \emptyset$. On a alors $U^c \cup W^c = K^n$. U^c et W^c sont des fermés de Zariski, ce sont donc des ensembles algébriques. On a donc $U^c = V((P_j)_{1\leqslant j\leqslant n})$ et $W^c = V((P'_k)_{1\leqslant k\leqslant m})$. Mais, grâce à ce que l'on a vu précédemment, on peut écrire : $U^c = V((P_j)_{1\leqslant j\leqslant n}) = \{x \in K^n \mid \forall j \in \{1, ..., n\} P_j(x) = 0\}$ et $W^c = V((P'_k)_{1\leqslant k\leqslant m}) = \{x \in K^n \mid \forall k \in \{1, ..., m\} P'_k(x) = 0\}$.
Ainsi, $U^c \cup W^c = K^n$ est juste l'ensemble des points de K^n vérifiant $P_j(x) = P'_k(x) = 0$ $\forall j \in \{1, ..., n\}$ et $\forall k \in \{1, ..., m\}$. Pour que cet ensemble de solutions soit égal à K^n tout entier, comme K est infini, il faut donc que $< P_j >_{1\leqslant j\leqslant n} = < P'_k >_{1\leqslant k\leqslant m} = \{0\}$. i.e il faut que $U^c = W^c = K^n$. Ceci est impossible car on a supposé U et W non vides. □

Définition 3.2.5. *Un espace topologique est dit* ***noethérien*** *lorsque toute suite décroissante de fermés est stationnaire.*

Proposition 3.2.4. *K^n,(où $K = \overline{K}$) muni de la topologie de Zariski, est un espace topologique noethérien.*

Démonstration. On a déjà vu que si $X_1 \subseteq X_2$, alors $\mathscr{I}(X_2) \subseteq \mathscr{I}(X_1)$.
Donc, soit $X_1 \supseteq X_2 \supseteq \cdots \supseteq X_n \supseteq X_{n+1} \supseteq \cdots$ une suite décroissante de ensembles algébriques de K^n.
On obtient : $\mathscr{I}(X_1) \subseteq \mathscr{I}(X_2) \subseteq \cdots \subseteq \mathscr{I}(X_n) \subseteq \mathscr{I}(X_{n+1}) \subseteq \cdots$ qui est une suite croissante d'idéaux de $K[X_1, \cdots, X_n]$: elle est donc stationnaire. Il en est de même pour $(X_n)_{n\in\mathbb{N}}$ car :
$\forall n \in \mathbb{N}$, $V(\mathscr{I}(X_n)) = X_n$ $\square$

3.3 Lien entre irréductibilité et idéaux premier

Théorème 3.3.1. *Soit $X \subseteq K^n$ un ensemble algébrique. Alors :*
X irréductible $\Leftrightarrow$ $\mathscr{I}(X)$ est un idéal premier.

Démonstration. "$\Rightarrow$" On suppose que X est irréductible. Soit $PQ \in \mathscr{I}(X)$. Soient $X_1 = X \cap V(P)$ et $X_2 = X \cap V(Q)$. X_1 et X_2 sont des fermés de X avec la topologie induite.
On a $V(P) \cup V(Q) = V(PQ)$. Soit $x \in X$. Comme $PQ \in \mathscr{I}(X)$, on a $PQ(x) = 0$. Donc $x \in V(PQ)$. Donc $X \subseteq V(PQ)$. Or,
$X_1 \cup X_2 = (X \cap V(P)) \bigcup (X \cap V(Q)) = X \bigcap (V(P) \cup V(Q)) = X \cap V(PQ) = X$. Comme X irréductible, on a $X_1 = X$ ou $X_2 = X$. i.e $X \subseteq V(P)$ ou $X \subseteq V(Q)$. Donc $P \in \mathscr{I}(X)$ ou $Q \in \mathscr{I}(X)$.
"$\Leftarrow$" On suppose que $\mathscr{I}(X)$ est premier. Supposons $X = X_1 \cup X_2$ avec X_1, X_2 deux fermés de X. On suppose $X_1 \neq X$. Montrons que $\mathscr{I}(X_2) = \mathscr{I}(X)$.
Comme $X_2 \subseteq X$, on a $\mathscr{I}(X) \subseteq \mathscr{I}(X_2)$. Montrons l'inclusion inverse.
Comme $X_1 \neq X$, on a $\mathscr{I}(X) \subsetneq \mathscr{I}(X_1)$ (Car la fonction $\mathscr{I}$ est injective). Donc, soit $P \in \mathscr{I}(X_1)\diagdown_{\mathscr{I}(X)}$. Soit $Q \in \mathscr{I}(X_2)$. Soit $x \in X$. Comme $X = X_1 \cup X_2$, on a PQ(x)=P(x)Q(x)=0. Donc $PQ \in \mathscr{I}(X)$. Comme $\mathscr{I}(X)$ est premier, on a $P \in \mathscr{I}(X)$ ou $Q \in \mathscr{I}(X)$. Comme $P \notin \mathscr{I}(X)$, on obtient $Q \in \mathscr{I}(X)$. D'où $\mathscr{I}(X) = \mathscr{I}(X_2)$. On obtient donc $X = X_2$ et X est irréductible. $\square$

Corollaire 3.3.1. *Soit K un corps algébriquement clos.*
Les fonctions $X \mapsto \mathscr{I}(X)$ et $I \mapsto V(I)$ induisent une bijection entre les ensembles algébriques irréductibles de K^n et les idéaux premier (donc radicaux) de $K[X_1, ..., X_n]$.

Exemple 3.3.1. *Si K est infini, K^n est irréductible.*

Démonstration. Comme K^n est infini, tout polynôme nul sur K^n est nul. Donc $\mathscr{I}(K^n) = \{0\}$, qui est un idéal premier car $\dfrac{K[X_1, ..., X_n]}{\{0\}} \cong K[X_1, ..., X_n]$ qui est intègre car K l'est. $\square$

Remarque 3.3.1. *Si K est fini, la proposition est fausse car K^n est fini, il est donc réunion finie de ses points qui sont des fermés.*

Corollaire 3.3.2. *(Principe de prolongement des identités algébriques) On suppose K infini. Soit V un ensemble algébrique différent de K^n, et*
$P \in K[X_1, ..., X_n]$. On suppose que P est nul en dehors de V. Alors P est le polynôme nul.

Démonstration. Pour montrer ceci, il suffit de montrer que $V(P) = K^n$. Soit $x \in V^c$. On a P(x)=0. D'où :
$V^c \subseteq V(P) \subseteq K^n$ donc
$V^c \cup V \subseteq V(P) \cup V \subseteq K^n$ i.e
$K^n \subseteq V(P) \cup V \subseteq K^n$ donc $V(P) \cup V = K^n$. Comme K^n est irréductible et que V(P) et V sont des fermés, on a que $V(P) = K^n$ ou $V = K^n$. Par hypothèse, $V \neq K^n$ donc $V(P) = K^n$ et ainsi P est le polynôme nul. □

Théorème 3.3.2. *V et $\mathscr{I}$ réalisent une bijection entre les points de K^n et les idéaux maximaux de $K[X_1, ..., X_n]$.*

Démonstration. Soit $a = (a_1, ..., a_n)$ un point de K^n. On peut écrire $a = V(X_1 - a_1, ..., X_n - a_n)$ et on a vu auparavant que $(X_1 - a_1, ..., X_n - a_n)$ est un idéal maximal de $K[X_1, ..., X_n]$. Réciproquement soit $\mathbf{m}$ un idéal maximal de $K[X_1, ..., X_n]$, on a vu que $\exists (a_1, ..., a_n) \in K^n$ tel que $\mathbf{m} = (X_1 - a_1, ..., X_n - a_n) = \mathscr{I}((a_1, ..., a_n))$. □

3.4 Décomposition en irréductibles

Théorème 3.4.1. *Soit V un ensemble algébrique non vide. V se décompose de façon unique (à permutation près) en une réunion finie d'ensembles algébriques irréductibles, non contenues l'un dans l'autre. i.e :*
$V = V_1 \cup V_2 \cup ... \cup V_r$ avec les V_i ensembles algébriques irréductibles et $V_i \nsubseteq V_j$ quand $i \neq j$.

Démonstration.

— Existence : supposons qu'il existe un ensemble algébrique V non vide qui ne se décompose pas en une réunion finie d'irréductibles. Alors, V n'est pas irréductible sinon $V = V$ serait une décomposition. Donc, $\exists V_1$, V' des fermés de Zariski tels que $V = V_1 \cup V'$ avec $V_1 \subsetneq V$ et $V' \subsetneq V$. Si V_1 et V' possédaient une décomposition finie en irréductibles, on en déduirait une décomposition pour V, ce qui est impossible par hypothèse. Donc V_1 ou V' ne possède pas de décomposition en irréductible. Sans perte de généralité, supposons que V_1 ne possède pas de décomposition. Alors, pour la même raison que précédemment, V_1 ne peut pas être irréductible, et donc $\exists V_2$ et V" tels que $V_2 \subsetneq V_1$, V"$\subsetneq V_1$ et $V_1 = V_2 \cup$ V". Pour les mêmes raison, V_2 ou V" ne possède pas de décomposition en irréductible, car par hypothèse V_1 n'en possède pas. Sans perte de généralité, supposons que ce soit V_2. Comme précédemment, V_2 ne peut pas être irréductible donc nous avons donc l'existence de V_3, V''' des fermés de Zariski tels que $V_3 \subsetneq V_2$, et $V''' \subsetneq V_2$ tels que $V_2 = V_3 \cup V'''$. En réitérant ce procédé, nous obtenons une suite décroissante de ensembles algébriques

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq ... \supsetneq V_n \supsetneq ..$$

Ce qui contredit le caractère noethérien de la topologie de Zariski.

— Unicité : supposons qu'il existe un ensemble algébrique V possédant deux décompositions en irréductibles. i.e :
$V = V_1 \cup ... \cup V_s = W_1 \cup ... \cup W_r$ avec les V_i et les W_i irréductibles.
Soit $i \in \{1, ..., s\}$. On écrit $V_i = V \cap V_i = (W_1 \cup ... \cup W_r) \cap V_i = (W_1 \cap V_i) \cup ... \cup (W_r \cap V_i)$. Comme V_i est irréductible, $\exists j \in \{1, ...r\}$ tel que $W_j \cap V_i = V_i$ i.e $\exists j \in \{1, ..., r\}$ tel que $V_i \subseteq W_j$. De même, $\exists k \in \{1, ..., s\}$ tel que $W_j \subseteq V_k$. Donc $V_i \subseteq V_k$ et donc par hypothèse, on a i=k et donc $V_i = W_j$.

□

Définition 3.4.1. *Les V_i sont appelées les* ***composantes irréductibles*** *de V.*

Remarque 3.4.1. *Si W est un fermé irréductible de V, on a
$W \subseteq V = V_1 \cup ... \cup V_s$. Donc $\exists i \in \{1, ..., s\}$ tel que $W \subseteq V_i$. Ainsi, les composantes irréductibles d'un ensemble algébrique sont exactement les fermés irréductibles maximaux pour l'inclusion.*

Exemple 3.4.1. *Soit K un corps algébriquement clos. On a :*

— $V(X^2 - X) = \{x \in K \mid x^2 - x = 0\}$
$= \{x \in K \mid x = 0\} \cup \{x \in K \mid x - 1 = 0\}$
$= V(X) \cup V(X-1)$ *est la décomposition en irréductible de* $V(X^2 - X)$ *car* $< X >$ *et* $< X - 1 >$ *sont des idéaux premiers de* $K[X]$.

— *V(XZ,YZ)=* $\{(x, y, z) \in K^3 \mid x = y = 0\} \cup \{(x, y, z) \in K^3 \mid z = 0\} = \{(x, y, z) \in K^3 \mid x = 0 \text{ et } y = 0\} \cup V(Z)$.

Rappel 3.4.1. *Soit A un anneau :
A factoriel $\Rightarrow$ A[X] factoriel
A principal $\Rightarrow$ A factoriel. Ici, K est un corps donc c'est un anneau principal. Il est donc factoriel. Donc $K[X_1, ..., X_n]$ est factoriel.*

Théorème 3.4.2. *Soit $P \in K[X_1, ..., X_n]$, $P = P_1^{\alpha_1} ... P_s^{\alpha_s}$ sa décomposition en irréductibles. On a alors :
1) $\mathscr{I}(V(P)) = (P_1 ... P_s)$. En particulier si P est irréductible, on a $\mathscr{I}(V(P)) = (P)$.
2) La décomposition de V(P) en irréductibles est données par
V(P)=$V(P_1) \cup ... \cup V(P_s)$. En particulier si P est irréductible, V(P) l'est aussi.*

Démonstration. 1) D'après le Nullstellensatz version forte, on a que $\mathscr{I}(V(< P >)) = \sqrt{< P >}$. Montrons que $\sqrt{P} =< P_1 ... P_s >$.
Soit $Q \in < P_1 ... P_s >$. $\exists Q_1 \in K[X_1, ..., X_n]$ tel que $Q = Q_1 P_1 ... P_s$.
On a alors $Q^{\max\limits_{1 \leq i \leq s} \alpha_i} \in < P >$. Donc $Q \in \sqrt{< P >}$.
Soit $Q \in \sqrt{< P >}$. $\exists m \in \mathbb{N}$ tel que $Q^m \in < P >$. Donc $\exists Q_2 \in K[X_1, ..., X_n]$ tel que $Q^m = Q_2 P_1^{\alpha_1} ... P_s^{\alpha_s}$. $\forall i \in \{1, ..., s\}$, $P_i \mid Q^m$. Les P_i sont irréductible dans $K[X_1, ..., X_n]$, qui est factoriel. Ils sont donc premiers. Donc $\forall i \in \{1, ..., s\}$, $P_i \mid Q$. Toujours grâce à leur primalité, on en déduit que le produit $P_1 ... P_s \mid Q$. On a dont l'inclusion réciproque.
2) Provient directement du 1). □

4 Dimension d'un ensemble algébrique

Dans cette section, nous allons définir une notion de dimension sur nos ensembles algébriques. Cette notion n'échappe pas à la correspondance géométrie $\leftrightarrow$ algèbre. Elle sera dans un premier temps très intuitive, et nous allons ensuite donner des définitions équivalentes.

4.1 Définition utilisant les chaînes de fermés irréductibles

Le but de cette section est de donner une définition topologique de la dimension, qui s'identifie bien à notre intuition.
On travaille sur un corps K algébriquement clos.

Définition 4.1.1. *Soit X un ensemble. Une* ***chaîne*** *de parties de X est une suite*

$$X_0 \subsetneq X_1 \subsetneq ... \subsetneq X_n$$

avec les $X_i \subseteq X$. Une telle chaîne est dite ***de longueur n****.*

Définition 4.1.2. *Soit X un espace topologique. La* ***dimension*** *de X est la borne supérieur des longueurs des chaînes de parties* ***fermées irréductibles*** *de X. Si X est non vide, sa dimension est un entier positif, ou est égal à $+\infty$. On le note* $\dim(X)$.

Remarque 4.1.1. *i) Cette notion n'a pas d'intérêt si X est séparé. En effet : Si X est séparé,* $\dim(X) = 0$.

Démonstration. Les seuls fermés irréductibles d'un espace séparé sont ses points. On ne peut donc pas trouver une chaîne d'irréductibles distincts. □

ii) Par convention, on a $\dim(\emptyset) = -\infty$.

Exemple 4.1.1. *X=$\{(x, y) \in \mathbb{R}^2 \ |x = 0\}$, muni de la topologie de Zariski induite, est de dimension 1.*

Proposition 4.1.1. *Soit X un espace topologique et soit Y un sous-espace de X. Alors*
1) Si Y est irréductible, $\overline{Y}$ l'est aussi.
2) Si U est un ouvert de X, on a des bijections réciproques :
$\varphi : Y \mapsto \overline{Y}$
et $\phi : Z \mapsto Z \cap U$
entre les parties fermées irréductibles Y de U et les parties fermées irréductibles Z de X qui rencontrent U.

Démonstration. 1) On suppose $\overline{Y} = F \cup G$ avec F, G deux fermés. On a alors $Y \subseteq \overline{Y} = F \cup G$ donc $Y = (Y \cap F) \bigcup (Y \cap G)$ est une décomposition en deux fermés de Y. Comme Y est irréductible, on a $Y \cap F = Y$ ou $Y \cap G = Y$. i.e $Y \subseteq F$ ou $Y \subseteq G$. Comme $\overline{Y}$ est le plus petit fermé contenant Y et que F et G sont des fermés, on obtient que $\overline{Y} \subseteq F$ ou $\overline{Y} \subseteq G$ i.e $\overline{Y}$ est irréductible.
2) Soit U un ouvert de X. Soit Y un fermé irréductible de U. Montrons que $\phi(\varphi(Y)) = Y$.
$\phi(\varphi(Y)) = \phi(\overline{Y}) = \overline{Y} \cap U = Y$ car Y est un fermé de U.
Soit Z une partie irréductible de X telle que $Z \cap U \neq \emptyset$. Montrons que $\varphi(\phi(Z)) = Z$. $\varphi(\phi(Z)) = \varphi(Z \cap U) = \overline{Z \cap U} = Z$ car $Z \cap U$ est un ouvert non vide de Z, et Z est irréductible. Cet ouvert est donc dense dans Z. □

Proposition 4.1.2. *Soit X un espace topologique. Si Y est un sous-espace topologique de X, on a :*
1) $\dim(Y) \leqslant \dim(X)$.
2) Soit $(X_i)_{i \in I}$ une famille finie de parties fermées irréductibles de X telle que $X = \bigcup\limits_{i \in I} X_i$. On a alors $\dim(X) = \sup\limits_{i \in I}(\dim(X_i))$.

Démonstration. 1) Soit $F_0 \subsetneq F_1 \subsetneq ... \subsetneq F_n$ une chaîne de fermés irréductibles de Y. On en déduit $\overline{F_0} \subsetneq \overline{F_1} \subsetneq ... \subsetneq \overline{F_n}$ une chaîne de fermés, irréductible par la proposition précédente dans X. De plus, ils sont distincts car on a $\forall i \in I$, $F_i = \overline{F_i} \cap Y$. Donc, $\dim(Y) \leqslant \dim(X)$.
3) D'après 1), on a que $\forall i \in I$, $\dim(X_i) \leqslant \dim(X)$, donc
$\sup\limits_{i \in I}(\dim(X_i)) \leqslant \dim(X)$.
Réciproquement, soit $p = \sup\limits_{i \in I}(\dim(X_i))$.
Supposons par l'absurde que l'on ait une chaîne de X de longueur p+1. :
$F_0 \subsetneq F_1 \subsetneq ... \subsetneq F_{p+1}$. On a :
$F_{p+1} = X \cap F_{p+1}$
$F_{p+1} = (\bigcup\limits_{i \in I} X_i) \bigcap F_{p+1}$
$F_{p+1} = \bigcup\limits_{i \in I} (X_i \cap F_{p+1})$

Comme F_{p+1} est irréductible et que la ligne précédente est une décomposition de F_{p+1} en fermés, F_{p+1} est contenu dans l'un des X_i. Toute la chaîne écrite précédemment serait donc contenu dans cet X_i. Ceci est impossible car $\forall i \in I$, $\dim(X_i) \leqslant p$. □

Définition 4.1.3. *Un ensemble algébrique X est dit* ***équidimensionnel*** *si toutes ses composantes irréductibles ont même dimension.*

Définition 4.1.4. *Soit X un espace topologique. Soit Y un sous-espace topologique de X. Si X est de dimension finie, on définie la* ***codimention*** *de Y par :* $\dim(X) - \dim(Y)$.

4.2 Lien avec la dimension de Krull

Définition 4.2.1. *Soit A un anneau. La* ***dimension de Krull*** *de A est la borne supérieure de la longueur des chaînes*

$$p_0 \subsetneq ... \subsetneq p_n$$

d'idéaux premiers de A.
On la note $\dim_K(A)$.

Exemple 4.2.1. *1) Si A est intègre, alors* $\dim A = 0$ *si et seulement si A est un corps.*
2) Par convention, $\dim(0) = -\infty$.

Démonstration. 1) Soit A un anneau intègre. Si A est un corps, alors il ne possède que deux idéaux : (0) et A. L'idéal A n'est pas propre donc non premier, et l'idéal (0) est premier car A est intègre. La seule chaîne possible est donc $(0) \subsetneq A$. Donc $\dim(A) = 0$.
Si $\dim(A) = 0$, soit I un idéal de A, différent de A. D'après le théorème de Krull, il existe un idéal J maximal de A tel que $I \subseteq J$. Mais J est aussi premier, donc comme la dimension de A vaut 0, on a que $J = (0)$. D'où $I = (0)$ et donc A ne possède que deux idéaux, donc A est un corps. □

Définition 4.2.2. *Soit V un ensemble algébrique. Nous avons vu que nous pouvions lui associer un idéal :*
$I(V) = \{P \in k[X_1, ..., X_n] \mid \forall x \in V,\ P(x) = 0\}$.
Nous pouvons également lui associer un anneau :
$\Gamma(V) = \dfrac{k[X_1, ..., X_n]}{I(V)}$. $\Gamma(V)$ *est appelée l'algèbre affine de V.*

Définition 4.2.3. *Soit k un corps commutatif. On dit que A est une k algèbre si :*
1) A est un k-ev
2) Il existe une troisième loi, interne sur A, notée ×, telle que :
a)(A,+,×) est un anneau i.e × est distributive sur +
b) $\forall \lambda \in k$, $\forall (a, b) \in A^2, \lambda \cdot (a \times b) = (\lambda \cdot a) \times b$.

Exemple 4.2.2. *1) $\mathbb{R}$ est une $\mathbb{R}$-algèbre.*
2) Si V est un ensemble algébrique, $\Gamma(V)$ est une k-algèbre.

Proposition 4.2.1. *Soit V un ensemble algébrique. V est fini $\Leftrightarrow \Gamma(V)$ est un k-espace vectoriel de dimension finie.*

Démonstration. "$\Rightarrow$" Supposons V fini. $V = \{u_1, ..., u_r\}$ pour un certain entier r. Considérons le morphisme d'anneau :

$$\begin{array}{rcl} \phi : k[X_1, ..., X_n] & \longrightarrow & k^r \\ P & \mapsto & (P(u_1), \cdots, P(u_r)) \end{array}$$

On a $Ker(\phi) = I(V)$. ϕ induit donc (d'après le théorème de Noether) une injection de $\Gamma(V)$ dans k^r. $\Gamma(V)$ est donc de dimension finie.
"$\Leftarrow$" Supposons que $\Gamma(V)$ soit de dimension finie. On note $\overline{X_i}$ l'image de X_i dans $\Gamma(V)$ par le morphisme canonique. La famille $1, \overline{X_i}, ..., \overline{X_i^s}, ...$ est donc liée $\forall i \in \{1, \cdots, n\}$. Il existe donc une relation de la forme :

$$a_s \overline{X_i^s} + \cdots + a_0 = 0$$

Soit $u = (x_1, \cdots, x_n) \in V$. On a : $a_s x_i^s + \cdots + a_0 = 0$
Les coordonnées de u sont donc les racines du polynôme
$P = a_s X_i^s + \cdots + a_1 X_i + a_o$. Il y a donc un nombre fini de valeurs possibles pour u. V est ainsi fini. □

Lemme 4.2.1. *1) Soient A un anneau et $I \subseteq J \subsetneq A$ des idéaux de A. Alors, J est un idéal premier de A si et seulement si J/I est un idéal premier de A/I.*
2) Soit V un ensemble algébrique. Soit $\pi : k[X_1, ..., X_n] \to k[X_1, ..., X_n]/I(V)$ le morphisme canonique. π induit une bijection entre les idéaux premiers de $k[X_1, ..., X_n]$ qui contiennent I(V) et les idéaux premiers de $\Gamma(V)$.

Démonstration. 1) D'après le troisième théorème d'isomorphisme, J/I est un idéal de A/I, et on a $(A/I)/(J/I) \cong A/J$. Donc J est premier si et seulement si A/J est intègre si et seulement si $(A/I)/(J/I)$ est intègre si et seulement si J/I est premier dans A/I.
2) Comme π est surjective, on conclue avec le théorème de correspondance des idéaux et le 1) du lemme. □

Théorème 4.2.1. *Soit V un ensemble algébrique. On a*

$$\dim(V) = \dim_K(\Gamma(V)).$$

Démonstration. Soit $F_0 \subsetneq \cdots \subsetneq F_n$ une chaîne maximale de fermés irréductibles de V. On en déduit
$I(F_n) \subsetneq \cdots \subsetneq I(F_0)$ une chaîne d'idéaux premiers de $k[X_1, ..., X_n]$ (car $V \mapsto I(V)$ est une bijection décroissante). Comme $\forall i \in \{1, \cdots, n\}$, $F_i \subseteq V$,

on a $\forall i \in \{1, \cdots, n\}$, $I(V) \subseteq I(F_i)$. D'après le lemme, on en déduit
$\pi(I(F_n)) \subsetneq \cdots \subsetneq \pi(I(F_0))$ une suite d'idéaux premiers de $\Gamma(V)$.
Donc, $\dim(V) \leqslant \dim(\Gamma(V))$.
Soit $F_0 \subsetneq \cdots \subsetneq F_m$ une chaîne d'idéaux premiers de $\Gamma(V)$. On en déduit $\pi^{-1}(F_0) \subsetneq \cdots \subsetneq \pi^{-1}(F_m)$ une chaîne d'idéaux premiers de $k[X_1, ..., X_n]$, qui contiennent I(V). On en déduit
$V(\pi^{-1}(F_m)) \subsetneq \cdots \subsetneq V(\pi^{-1}(F_0))$ une chaîne de ensembles fermés irréductibles, tels que : $\forall i \in \{1, \cdots, m\}$ $I(V) \subseteq \pi^{-1}(F_i)$ i.e $\forall i \in \{1, \cdots, m\}$, $V(\pi^{-1}(F_i)) \subseteq V$. Ces ensembles algébriques sont bien des ensembles algébrique irréductibles de V .
D'où l'égalité.

□

4.3 Lien avec la transcendance

Notions importantes d'algèbre

Définition 4.3.1. *Soit k un corps commutatif. Soit A une k-algèbre. On dit que A est de type fini si elle est engendrée par un nombre fini d'éléments $f_1, ..., f_n$ (c'est-à-dire que tout élément de A s'écrit comme $P(f_1, ..., f_n)$, où $P(X_1, ..., X_n) \in k[X_1, ..., X_n]$ est un polynôme). On écrit alors $A = k[f_1, ..., f_n]$.*

Proposition 4.3.1. *Une k-algèbre est de type fini si et seulement si elle est isomorphe à un quotient d'un $k[X_1, ..., X_n]$ par un idéal si et seulement s'il existe un morphisme surjectif de $k[X_1, ..., X_n] \to A$.*

Démonstration. "$\Rightarrow$" Supposons que A soit une k-algèbre de type fini, engendrée par $f_1, ..., f_n$. Alors le morphisme suivant :

$$\varphi : k[X_1, ..., X_n] \to A$$
$$X_i \mapsto f_i$$

est surjectif. Donc, d'après l'isomorphisme de Noether, A est isomorphe à $k[X_1, ..., X_n]/\ker(\varphi)$.
"$\Leftarrow$" Supposons que A soit isomorphe à un quotient $k[X_1, ..., X_n]/I$. On note x_i l'image de X_i dans A. Alors les x_i engendrent A comme k-algèbre. □

Exemple 4.3.1. $\Gamma(V)$ *est une k-algèbre de type fini.*

Définition 4.3.2. *(Extension) Soit A un anneau. Une extension de A est un anneau B muni d'un morphisme injectif $i : A \hookrightarrow B$.*

Exemple 4.3.2. $(\mathbb{R}, i)$ *est une extension du corps $\mathbb{Q}$.*

Définition 4.3.3. *Soit B une extension de A et $x \in B$. On dit que x est **entier** (ou algébrique) sur A si $\exists$ $P \in A[X]$ non nul unitaire, tel que $P(x) = 0$. Dans le cas contraire, on dit que x est **transcendant**.
On dit que B est une **extension entière** (ou algébrique) de A si tous les éléments de B sont entiers sur A.*

Exemple 4.3.3. *$\mathbb{R}$ est une $\mathbb{Q}$-algèbre et $\sqrt{2}$ est entier sur $\mathbb{Q}$ car il est annulé par le polynôme $X^2 - 1$.*
Par contre, $\mathbb{R}$ n'est pas une extension entière de $\mathbb{Q}$ car π n'est annulé par aucun polynôme unitaire de $\mathbb{Q}[X]$.

Définition 4.3.4. *Soit $K \subseteq L$ une extension de corps. Une partie B de L est dite **algébriquement libre** sur K si pour toute partie finie $\{x_1, ..., x_s\}$ d'éléments de B, $\forall P \in K[X_1, ..., X_s]$, $P(x_1, ..., x_s) = 0 \Rightarrow P = 0$.*

Définition 4.3.5. *Soit $K \subseteq L$ une extension de corps. Une partie B de L est une **base de transcendance** de L sur K si elle est algébriquement libre et maximale : i.e si on lui rajoute un élément, cette partie n'est plus algébriquement libre.*

Théorème 4.3.1. *Soit $K \subseteq L$ une extension de corps. Alors, il existe une base de transcendance de L sur K, et toutes les bases de transcendance ont même cardinal.*

Démonstration. Lemme de Zorn. □

Définition 4.3.6. *Soit $K \subseteq L$ une extension de corps. Le cardinal d'une base de transcendance de L est appelé le **degré de transcendance** de L et est noté $\partial_K(L)$.*

Définition 4.3.7. *Soit $k \subseteq K$ une extension de corps, et S une partie de K. On note $k[S]$ le sous-anneau de K engendré par k et S, et $k(S)$ le sous-corps de K engendré par k et S.*

Remarque 4.3.1. *Il est clair que $k[S]$ est l'ensemble des éléments de K qui s'écrivent sous la forme $P(x_1, ..., x_n)$ avec $n \in \mathbb{N}$ et $x_1, ..., x_n \in S$, et $P \in k[X_1, ..., X_n]$. De même, $k(S)$ est l'ensemble des éléments $\dfrac{P(x_1, ..., x_n)}{Q(x_1, ..., x_n)}$ de K, avec $n \in \mathbb{N}$, $x_1, ..., x_n \in S$ et $P, Q \in k[X_1, ..., X_n]$ et $Q \neq 0$. D'où $k(S)$ est le corps des fractions de $k[S]$.*

Proposition 4.3.2. *Soit $K \subseteq L$ une extension de corps. Une partie B de L est une **base de transcendance** de L si elle est algébriquement libre et si L est une extension entière de $K(B)$.*

Démonstration. Soit B une partie de L telle que B soit algébriquement libre et que L soit une extension entière de K(B). Montrons que B est une base de transcendance de L sur K : i.e montrons qu'elle est maximale.
Soit $x \in L \setminus B$. On a $x \in L$ donc $\exists P \in K(B)[X]$ tel que $P(x) = 0$.
On peut écrire : $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ avec les a_i dans $K(B)$. Donc, il existe un entier $m \in \mathbb{N}^*$, $b_1, ..., b_m \in B$ deux à deux distincts, et $Q, P_0, ..., P_n \in K[X_1, ..., X_m]$ tels que $Q(b_1, ..., b_m) \neq 0$

et $a_i = P_i(b_1, ..., b_m)/Q$ (on met tout au même dénominateur). On définit $P \in K[X_1, ..., X_m, Y]$ par

$$P(X_1, ..., X_m, Y) = \sum_{i=0}^{n} P_i(X_1, ..., X_m)Y^i$$

P est non nul mais $P(b_1, ..., b_m, x) = 0$ donc B est maximale. Ainsi, B est une base de transcendance de L sur K. □

Remarque 4.3.2. *Soit $k \subset K$ une extension de corps. Alors K est un k-espace vectoriel. En effet, si on muni K de sa loi de groupe et de la loi de composition externe suivante :*

$$k \times K \to K$$

$$(\lambda, a) \mapsto \lambda a$$

Il est clair que K devient ainsi un k-espace vectoriel, et même une k-algèbre.

Lemme 4.3.1. *Soit A un anneau et B un anneau intègre tel que $A \subseteq B$ soit une extension entière. Alors*
A corps $\Leftrightarrow$ B corps.

Démonstration. "$\Rightarrow$" Supposons que A soit un corps. Soit $b \in B$ non nul. Soit $P(X) = X^n + \cdots + a_1X + a_0$ le polynôme minimal dans $A[X]$ tel que $P(b) = 0$. On a :

$$b^n + \cdots + a_1b + a_0 = 0$$

a_0 n'est pas nul, car s'il l'était, on aurait $b(b^{n-1} + \cdots + a_1) = 0$ et comme b est non nul et que B est intègre, on aurait un autre polynôme qui annulerait b, avec un degré plus bas. Donc a_0 est non nul et comme A est un corps, a_0 est inversible. On a donc :

$$b^n + \cdots + a_1b + a_0 = 0$$

$$b(b^{n-1} + \cdots + a_1) = -a_0$$

$$b(b^{n-1} + \cdots + a_1)a_0^{-1} = 1$$

donc b est inversible.
"$\Leftarrow$" Supposons que B est un corps. Soit $a \in A$ non nul. Comme $A \subseteq B$ et que B est un corps, $\exists b \in B$ tel que $ab = 1$. Montrons que $b \in A$. Soit $P(X)$ le polynôme minimal de b dans $A[X]$. On a :

$$b^n + \cdots + c_1b + c_0 = 0$$

En multipliant par a^{n-1}, on obtient :

$$b + c_{n-1} + \cdots + c_1a^{n-2} + c_0a^{n-1} = 0$$

$$b = -(c_{n-1} + \cdots + c_1a^{n-2} + c_0a^{n-1})$$

Donc, $b \in A$. □

Lemme 4.3.2. *Soient A, B deux anneaux tels que $A \subseteq B$ soit une extension entière. Soit J un idéal de B et soit $I = J \cap A$. Alors A/I est un sous-anneau de B/J et B/J est entière sur A/I.*

Démonstration. Soit $A \overset{\mathrm{i}}{\hookrightarrow} B \overset{\pi}{\longrightarrow} B/J$
$Ker(\pi \circ i) = \{x \in A \mid \pi \circ i(x) = 0\}$
$Ker(\pi \circ i) = \{x \in A \mid \pi(x) = 0\}$
$Ker(\pi \circ i) = \{x \in A \mid x \in J\}$
$Ker(\pi \circ i) = A \cap J$
Donc $A/(A \cap J) \cong im(\pi \circ i)$, qui est un sous-anneau de B/J.
Montrons que B/J est entière sur A/I. Soit $\overline{b} \in B/J$. $\exists b \in B$ tel que $\overline{b} = b + J$. Soit $P(X) = X^n + \cdots + a_1X + a_0$ un polynôme de $A[X]$, annulateur de b. Soit $\tilde{P}(X) = X^n + \cdots + \overline{a_0}$ où $\overline{a_i}$ est la classe d'équivalence de a_i dans A/I (donc dans B/J). $\tilde{P}(\overline{b}) = \overline{b}^n + \cdots + \overline{a_0} = \overline{b^n + \cdots + a_0} = \overline{0} = 0$. Donc l'extension est entière. □

Définition 4.3.8. *Un anneau **local** est un anneau possédant un unique idéal maximal.*

Lemme 4.3.3. *Soient A, B deux anneaux tels que $A \subseteq B$ soit une extension entière. On suppose que A est local, d'idéal maximal $\mathbf{m}$. Les idéaux premiers de B au-dessus de $\mathbf{m}$ (i.e les q tels que $q \cap A = \mathbf{m}$) sont exactement les idéaux maximaux de B.*

Démonstration. "$\Rightarrow$" Soit q un idéal premier de B tel que $q \cap A = \mathbf{m}$. Montrons que q est maximal. D'après un lemme précédent, on a $A/\mathbf{m} \subseteq B/q$ est une extension entière. q est premier donc B/q est intègre. D'après un autre lemme, on a $A/\mathbf{m}$ corps $\Rightarrow B/q$ corps. Donc q est maximal.
"$\Leftarrow$" Soit q un idéal maximal de B. Montrons qu'il est de la forme : $q \cap A = \mathbf{m}$. On a toujours $A/(q \cap A) \subseteq B/q$ est une extension entière. Comme B/q est un corps, on a $A/(q \cap A)$est un corps et donc $q \cap A$ est maximal. Comme A est local, on obtient $q \cap A = \mathbf{m}$. □

Théorème 4.3.2. *Soit A un anneau. Soit S une partie multiplicative de A. Les applications suivantes :*
$\phi : \{$*Idéaux premiers de A, disjoint de S* $\} \longrightarrow \{$*Idéaux premiers de $S^{-1}A$*$\}$

$$P \longmapsto P.S^{-1}A$$

$\varphi : \{$ *Idéaux premiers de $S^{-1}A$*$\} \longrightarrow \{$*Idéaux premiers de A disjoints de S* $\}$

$$Q \longmapsto Q \cap A$$

induisent des bijections réciproques, croissantes.

Démonstration. — Soit P un idéal premier de A, disjoint de S. Montrons que $P.S^{-1}A$ est un idéal premier de $S^{-1}A$.
Pour commencer, on voit bien que $0/1 \in P.S^{-1}A$.
Soient $a, b \in P.S^{-1}A$. On peut considérer $p_1, p_2 \in P$ et $s_1, s_2 \in S$ tels que $a = p_1/s_1$ et $b = p_2/s_2$. On obtient $a - b = \frac{p_1 s_2 - p_2 s_1}{s_1 s_2} \in P.S^{-1}A$ car P idéal et S partie multiplicative.
Soit $a = p_1/s_1 \in P.S^{-1}A$ et $b \in S^{-1}A$ donc $\exists (a_1, s_2) \in A \times S$ tels que $b = a_1/s_2$. On a alors $ab = p_1 a_1/s_1 s_2 \in P.S^{-1}A$ car P idéal et S partie multiplicative. Donc $P.S^{-1}A$ est un idéal de $S^{-1}A$.
Montrons qu'il est premier. Soit $ab = p/s \in P.S^{-1}A$ On a : $\exists t \in S$ tel que $t(abs - p) = 0$. On obtient : $abst = pt$. Donc $abst \in P$. Comme P est premier, on a $ab \in P$ ou $st \in P$. Si $st \in P$, on a de même $s \in P$ ou $t \in P$. Ceci est impossible car s et t sont dans S et $P \cap S = \emptyset$. Donc $ab \in P$ i.e $a \in P$ ou $b \in P$, d'où $a/1 \in P.S^{-1}A$ ou $b/1 \in P.S^{-1}A$. Donc $P.S^{-1}A$ est premier.

— Soit Q un idéal premier de $S^{-1}A$. Montrons que $Q \cap A$ est :
1) Un idéal de A
2) Premier
3) Disjoint de S
1) Soient $a, b \in Q \cap A$. On a $a - b \in A$, $a - b \in Q$ car Q idéal donc $a - b \in Q \cap A$. Soient $a \in Q \cap A$ et $b \in A$. On a $ab \in A$ et $ab \in Q$ car $A \subseteq S^{-1}A$. L'élément neutre est trivialement dans $Q \cap A$.
2) Soit $ab \in Q \cap A$, avec $a, b \in A$. Ainsi, $ab \in Q$ et comme Q premier, on a $a \in Q$ ou $b \in Q$. Donc $Q \cap A$ premier de A.
3) Supposons $Q \cap A \cap S \neq \emptyset$. Soit $x \in Q \cap A \cap S$. On a $1 = x/x \in Q$. Ceci est impossible car Q est premier donc propre.

— Montrons maintenant que ce sont bien des bijections réciproques. Soit P un idéal premier de A, disjoint de S. Montrons que $P.S^{-1}A \cap A = P$. Soit $a \in P$. On a $a \in A$ et $a = a/1 \in P.S^{-1}A$. Montrons l'inclusion réciproque. Soit $a \in P.S^{-1}A \cap A$. On a $a = p/s$ avec $p \in P$ et $s \in S$. Mais comme $p/s \in A$, on a forcément que $s = 1$. Donc $a = p$ et $a \in P$.
Soit Q un idéal premier de $S^{-1}A$. Montrons que $(Q \cap A).S^{-1}A = Q$. Soit $a \in (Q \cap A).S^{-1}A$. On peut écrire $a = q/s$ avec $q \in Q \cap A$ et $s \in S$. On a $q \in Q$ et Q idéal de $S^{-1}A$ donc $q * 1/s \in Q$ car $1/s \in S^{-1}A$. Montrons l'inclusion réciproque. Soit $q \in Q$. On peut écrire $q = p/s$ avec $p \in A$ et $s \in S$. Comme $s \in S \subseteq A \subseteq S^{-1}A$ et que Q est un idéal de $S^{-1}A$, on a $p/s * s = p \in Q$. Donc $p \in Q \cap A$. D'où l'inclusion réciproque.

□

Lemme 4.3.4. *Soient A et B des anneaux tels que $A \subseteq B$ soit une extension entière. Soit p un idéal premier de A. Soit $S = A \setminus p$. On note A_p et B_p les localisés $S^{-1}A$ et $S^{-1}B$. Alors, A_p est local, contenu dans B_p, qui lui même est entier sur A_p.*

Démonstration. D'après le théorème précédent, les idéaux premiers de A_p sont les idéaux de la forme qA_p, pour q idéal premier de A ne rencontrant pas S, i.e, contenu dans p. Donc, tout idéal premier de A_p est contenu dans pA_p ; celui-ci est donc l'unique idéal maximal de A_p (car un idéal maximal est nécessairement premier).
$A_p \subseteq B_p$ clair car $A \subseteq B$. Montrons que $A_p \subseteq B_p$ est entière.
Soit $b/s \in B_p$. Comme B est entier sur A, $\exists P(X) = X^n + \cdots + a_0 \in A[X]$ tel que $P(b) = 0$. Soit
$\tilde{P}(X) = X^n + X^{n-1}a_{n-1}/s + \cdots + Xa_1/s^{n-1} + a_0/s^n$
$\tilde{P}(b/s) = b^n/s^n + b^{n-1}/s^{n-1} * a_{n-1}/s + \cdots + a_o/s^n$
$\tilde{P}(b/s) = 1/s^n(b^n + b^{n-1} * a_{n-1} + \cdots + a_0)$
$\tilde{P}(b/s) = 0$
Donc B_p est entier sur A_p. □

Théorème 4.3.3. *(Going-up de Cohen-Seidenberg) Soient A, B deux anneaux tels que $A \subseteq B$ et B entier sur A. On a :*
1) L'application $q \mapsto q \cap A$ de Spec(B) dans Spec(A) est surjective.
2) $\forall p, p' \in$ Spec(A) avec $p \subseteq p'$ et pour tout q$\in$ Spec(B) tel que $q \cap A = p$, il existe q' $\in$ Spec(B) avec q'$\cap$A=p' et q $\subseteq$q'.
3) Si on a q,q'$\in$ Spec(B) avec q $\subseteq$q' et si $q \cap A = q' \cap A = p$, alors q=q'.
4) $\dim_K(A) = \dim_K(B)$.

Démonstration. 1) Soit $p \in$ Spec(A). Soit $S = A \backslash p$. Soit A_p et B_p les localisés de A et B en p. On a d'après un lemme précédent $A_p \subseteq B_p$ extension entière. A_p est un anneau local. Donc, $\exists!$ idéal maximal : $I = pA_p$.
Soit q_1 un idéal maximal de B_p. D'après un lemme précédent, on a $q_1 \cap A_p = I$.
Soit $q = q_1 \cap B$
$q \cap A = q_1 \cap B \cap A$
$q \cap A = q_1 \cap A$
$q \cap A = q_1 \cap A_p \cap A$
$q \cap A = I \cap A$
$q \cap A = pA_p \cap A = p$.
Donc l'application est surjective.
2) Soient p, p' $\in$ Spec(A) tels que $p \subseteq p'$.
Soit $q \in$ Spec(B) tel que $q \cap A = p$. D'après le 1), $\exists q' \in Spec(B)$ tel que $q' \cap A = p'$ et l'inclusion est triviale.
3) Soient $q, q' \in$ Spec(B) avec $q \subseteq q'$ et tels que $q \cap A = q' \cap A = p$.
Comme p est un idéal premier de A, on peut localiser A et B en $S = A \setminus p$.
D'après un lemme précédent, $A_p \subseteq B_p$ est entière, et les idéaux maximaux de B_p sont exactement les idéaux I premiers de B_p tels que $I \cap A_p = pA_p$.
Soit $\phi(q) = qB_p$. On a $qB_p \cap A_p = pA_p$. En effet $qB_p \cap A_p \supseteq pA_p$ trivial.
Soit $x \in qB_p \cap A_p$. On a $x \in qB_p$ donc $x = b/s$ avec $b \in q$ et $s \in S$. Or, $x \in A_p$ également, donc $b \in A$. Finalement, $x = b/s$ avec $b \in q \cap A = p$ et $s \in S$. Donc $x \in pA_p$.

Donc $q.B_p$ est un idéal maximal de B_p. Il en est de même pour $q'B_p$. Or, $q \subseteq q'$ donc $qB_p \subseteq q'B_p$. Ils sont donc égaux. On peut donc appliquer la fonction φ qui nous donne $q = q'$.
4) Soit $p_1 \subsetneq \cdots \subsetneq p_n$ une chaîne d'idéaux premiers de A. D'après le 1) et le 2), on en déduit une chaîne $q_1 \subsetneq \cdots \subsetneq q_n$ d'idéaux premiers de B. Donc $\dim(A) \leqslant \dim(B)$
Soit $q_1 \subsetneq \cdots \subsetneq q_m$ une chaîne d'idéaux premiers de B. Alors d'après le 1) et le 3) on en déduit une chaîne d'idéaux $q_1 \cap A \subsetneq \cdots \subsetneq q_m \cap A$ premiers de A. En effet, si deux d'entre eux sont égaux, disons WLOG si $q_1 \cap A = q_2 \cap A$ alors d'après le 3), comme on avait $q_1 \subseteq q_2$, on obtient $q_1 = q_2$ ce qui est impossible. On a donc bien l'égalité demandée. □

Lemme 4.3.5. *(De normalisation de Noether) Soit k un corps, A une k-algèbre de type fini, intègre. Il existe des éléments $x_1, ..., x_n \in A$, algébriquement indépendants sur k tels que A soit entier sur $k[x_1, \cdots, x_n]$.*

Démonstration. Admise. □

Application à la dimension

Théorème 4.3.4. *Soit A une k-algèbre de type fini intègre. On a :*

$$\dim(A) = \partial_k(Frac(A))$$

Démonstration.

— Tout d'abords, montrons que $\partial_k(k(X_1, ..., X_n)) = n$. Soit B=$\{X_1, \cdots, X_n\}$. Montrons que B est algébriquement libre. Soit (sans perte de généralité) $\{X_1, \cdots, X_r\} \subseteq B$. Soit $P \in K[X_1, ..., X_r]$ tel que $P(X_1, ..., X_r) = 0$. $P(X_1, ..., X_r) = P = 0$. Donc B est algébriquement libre.
Montrons que B est maximale. Soit $a \in K[X_1, ..., X_n] \setminus B$.
Montrons que $B \cup \{a\}$ n'est plus libre. On a $a = \sum_i a_i X_1^{\alpha_{1,i}} \cdots X_n^{\alpha_{n,i}}$.
Soit $P = \sum_i a_i T_1^{\alpha_{1,i}} \cdots T_n^{\alpha_{n,i}} - Z \in K[T_1, \cdots, T_n, Z]$. P est trivialement non nul. $P(X_1, \cdots, X_n, a) = 0$. Donc, $B \cup \{a\}$ n'est pas algébriquement libre.
B est donc une base de transcendance de $k(X_1, \cdots, X_n)$ sur k.

— Ensuite, montrons que $\dim_K(k[X_1, \cdots, X_n]) \geq n$. La chaîne

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \cdots, X_n)$$

nous donne la réponse.

— Nous allons utiliser ce lemme : Soit A une k-algèbre de type fini intègre. Soit p un idéal premier, non nul, minimal pour l'inclusion.
Alors $\partial_k(Frac(A/p)) = \partial_k(Frac(A)) - 1$.

— Prouvons maintenant le théorème.
Soit A une k-algèbre de type fini intègre. D'après le lemme de normalisation de Noether, il existe $\{x_1, \cdots, x_n\}$ tels que A soit une extension entière de $k[x_1, \cdots, x_n]$. Donc A est une extension entière de $K[X_1, ..., X_n]$, donc $\dim_K(A) = \dim_K(k[X_1, \cdots, X_n]) \geq n$ (d'après le going-up). On a alors :

$$k[x_1, \cdots, x_n] \hookrightarrow A \hookrightarrow Frac(A)$$

Donc, par propriété universelle du corps des fractions, on obtient $k(x_1, \cdots, x_n) \hookrightarrow Frac(A)$.
Montrons que cette extension est entière.
Pour cela, nous allons montrer cette affirmation :
Soit $R \subsetneq S$ une extension entière. Alors Frac$(S) = (R \setminus 0)^{-1}S$. Une inclusion est triviale. Pour l'autre, soit $a/b \in$ Frac(S). On a $a \in S$ et $b \in S \setminus 0$. Comme S est entière sur R, $\exists a_i \in R$ tels que $b^n + \cdots + a_1 b + a_0 = 0$
i.e $-a_0 = b(b^{n-1} + \cdots + a_1)$. Soit $b' = (b^{n-1} + \cdots + a_1)$. On a $b' \in S$ et $bb' = -a_0 \in R$. Donc $\frac{a}{b} = \frac{ab'}{bb'}$ avec $ab' \in S$ et $bb' \in R \setminus \{0\}$. D'où l'inclusion inverse.
Donc ici, soit x un élément de Frac(A). Il s'écrit de a forme a/b avec $a \in A$ et $b \in k[x_1, ..., x_n]$. Comme A entier sur $k[x_1, ..., x_n]$, $\exists a_i \in k[x_1, ..., x_n]$ tels que $a^n + \cdots + a_1 a + a_0 = 0$
Soit $P(X) = X^n + \cdots + a_1/b^{n-1}X + a_0/b^n$. On a $P \in k(x_1, ..., x_n)[X]$ d'après ce qui a été dit précédemment. Et P(a/b)=0. Donc $\{x_1, ..., x_n\}$ est une base de transcendance de Frac(A) sur k et donc $\partial_k(Frac(A)) = n$.
Montrons maintenant par récurrence sur n que :
Si A est une k-algèbre de type fini intègre telle que $\partial_k(Frac(A)) = n$, alors on a $dim_K(A) = \partial_k(Frac(A))$.
(I) $n = 0$. On a alors $\partial_k(Frac(A)) = 0$ A ne possède donc pas d'éléments transcendants sur k. Donc $k \subsetneq A$ est une extension entière. Comme A est intègre, on a que A est un corps et donc $\dim_K(A) = 0 = \partial_k(Frac(A))$.
(H) On suppose l'hypothèse vraie au rang $n-1$. Soit $m = \dim_K(A)$. On a déjà que $m \geq n$. Soit

$$(0) \subsetneq p_1 \subsetneq \cdots \subsetneq p_m$$

une chaîne maximale d'idéaux premiers de A. Alors, p_1 est un idéal premier, minimal pour l'inclusion. D'après le lemme, on a que $\deg_k(A/p_1) = \deg_k(Frac(A)) - 1 = n - 1$.
On peut donc appliquer l'hypothèse de récurrence pour obtenir : $\dim_K(A/p_1) = n - 1$. Or,

$$(0) \subsetneq \overline{p_2} \subsetneq \cdots \subsetneq \overline{p_m}$$

où les $\overline{p_i}$ sont les images des p_i par la surjection canonique est une chaîne d'idéaux premiers de A/p_1, de taille $m-1$. D'où
$\dim_K(A/p_1) = n-1 \geq m-1$.
Donc $n \geq m$ et on a l'égalité voulue.

$\square$

5 Résumé

Nous allons ici résumer ce que nous venons de faire par le dictionnaire Algèbre $\longleftrightarrow$ géométrie que nous avons crée.

Algèbre	**Géométrie**
Idéal radical I $\mathscr{I}(V)$	Ensemble algébrique V(I) V
Addition d'idéaux I+J	Intersection de ensembles algébrique $V(I) \cap V(J)$
Produit d'idéaux IJ	Union de ensembles algébriques $V(I) \cup V(J)$
Idéal premier Idéal maximal	Ensemble irréductible Point
Chaîne croissante	Chaîne décroissante
Décomposition de polynômes en polynômes irréductibles	Décomposition d'ensemble algébrique en ensembles algébriques irréductibles
Dimension de Krull, degrés de transcendance	Dimension d'un ensemble algébrique

6 Applications

6.1 Définitions

Définition 6.1.1. *Soit X un ensemble algébrique affine irréductible de k^n. On dit que X est **ensemblistement intersection complète** (EIC) si X est le lieu des zéros de codim(X) élements de $k[x_1, ..., x_n]$, i.e si on a*
$X = V(f_1, .., f_c)$ *où* $c = codim(X)$ *et* $\forall i \in \{1, ..., c\}, f_i \in k[x_1, .., x_n]$.

Définition 6.1.2. *Soit X un ensemble algébrique affine irréductible de k^n. On dit que X est **schématiquement intersection complète** (SIC) si l'idéal de X, $I(X)$, est engendré par codim(X) éléments.*

Remarque 6.1.1. *Si X est SIC, alors X est EIC. En effet supposons que X soit SIC. On a alors $I(X) =< f_1, ..., f_s >$ pour des certains $f_i \in k[X_1, \cdots, X_n]$ et avec s=codim(X). Alors $V(I(X)) = V(< f_1, ..., f_s >)$ i.e $X = V(f_1, ..., f_s)$. Mais la réciproque est fausse. En effet si $X = V(f_1, ..., f_s)$, on a*
$I(X) = I(V(f_1, ..., f_s)) = I(V(< f_1, ..., f_s >)) = \sqrt{< f_1, ..., f_s >}$ *d'après le Nullstellensatz.*

6.2 Contre-exemple

Soit $Y \subseteq \mathbb{R}^3$ la courbe définie paramétriquement par
$x = t^3$, $y = t^4$, $z = t^5$. Alors, Y n'est pas SIC, mais il est EIC.

Démonstration. — Montrons tout d'abord que codim(Y)=2, i.e montrons que $\dim(Y) = 1$.
Soit

$$\begin{aligned} \phi : \mathbb{R}[X, Y, Z] &\to \mathbb{R}[T] \\ X &\mapsto T^3 \\ Y &\mapsto T^4 \\ Z &\mapsto T^5 \end{aligned}$$

$\ker(\phi) = \{P \in \mathbb{R}[X, Y, Z] | P(T^3, T^4, T^5) = 0\}$
$\ker(\phi) = \mathscr{I}(Y)$
D'après le théorème d'isomorphisme de Noether, $\Gamma(Y)$ s'identifie à une sous-$\mathbb{R}$-algèbre A de $\mathbb{R}[T]$. D'après de précédents théorèmes, on a $\dim(Y) = \dim_K(A) = \partial_{\mathbb{R}}(Frac(A))$.
On a A =im(ϕ)
D'où $T^4 \in A$ et $T^3 \in A$. Donc $T^4/T^3 = T \in$ Frac(A).
Or on a $A \hookrightarrow \mathbb{R}[T] \hookrightarrow \mathbb{R}(T)$ donc d'après la propriété universelle du corps des fractions, Frac(A)$\hookrightarrow \mathbb{R}(T)$. Comme $T \in$ Frac(A) et que Frac(A) est un corps, on a $K(T) \subseteq$ Frac(A) donc Frac(A)=$\mathbb{R}(T)$.
Donc $\dim(Y) = \partial_{\mathbb{R}}(Frac(A)) = 1$.

- Cherchons des générateurs de $\mathscr{I}(Y)$. On voit trivialement que les polynômes $P = XZ - Y^2, Q = X^3 - YZ, R = YX^2 - Z^2$ appartiennent à $\mathscr{I}(Y)$. Maintenant, soit $f \in \mathscr{I}(Y)$. On peut écrire :
$f(X,Y,Z) = \sum_{a_1,a_2,a_3} c_{a_1,a_2,a_3} X^{a_1}Y^{a_2}Z^{a_3}$ avec $a_1, a_2, a_3 \in \mathbb{N}$. On a alors :
$f(T^3,T^4,T^5) = \sum_{a_1,a_2,a_3} c_{a_1,a_2,a_3} T^{3a_1+4a_2+5a_3}$
Ce polynôme est un polynôme en une variable, on peut donc indexer la somme de cette manière :
$f(T^3,T^4,T^5) = \sum_{3a_1+4a_2+5a_3=s} (\sum_{a_1,a_2,a_3} c_{a_1,a_2,a_3})T^s = 0$ car $f \in \mathscr{I}(Y)$.
On voit alors que, $\forall s$, $\sum_{3a_1+4a_2+5a_3=s} c_{a_1,a_2,a_3} = 0$.
Prenons $s = 5$. On voit clairement que la seule combinaison possible est $a_1 = a_2 = 0$ et $a_3 = 1$. D'où, $c_{0,0,1=0}$. De la même façon, pour $s = 10$, on voit que les seules combinaisons possible sont $a_1 = 2, a_2 = 1$ et $a_3 = 0$ et $a_1 = a_2 = 0$ et $a_3 = 2$. D'où $c_{2,1,0} - c_{0,0,2} = 0$.
En faisant des calculs similaires, on se rend compte que f ne possède pas de termes constants, ni de termes en x, y, z, x^2, xy et que les termes en xz et y^2, x^3 et yz, x^2y et z^2 ont des coefficients opposés.
Les polynômes P, Q et R engendrent donc $\mathscr{I}(Y)$.
- Avec un calcul, on remarque que P, Q et R sont linéairement indépendants modulo $M^3 =< X^iY^jZ^k >_{i+j+k=3}$.
- On conclue donc que $\mathscr{I}(Y)$ ne peut pas être engendré par moins de 3 éléments car : Soit $S \in I$. On suppose que $I =< f, g >$. Alors, comme on l'a vu précédemment,f et g sont forcément engendrés par P, Q et R. On a donc :
$S = Q_1f + Q_2g$ avec $Q_1, Q_2 \in \mathbb{R}[X,Y,Z]$. Cela nous donne $S = Q_1(f_1P + f_2Q + f_3R) + (g_1P + g_2Q + g_3R)$ avec $f_i, g_i \in \mathbb{R}[X,Y,Z]$. En regardant cette relation modulo M^3, on se rend compte que pour des raisons de degrés, on a forcément que Q_1 et $Q_2\mathbb{R}$.
On se place alors dans le $\mathbb{R}$-espace vectoriel $I/(I \cap M^3)$. On considère la surjection canonique de I dans $I/(I \cap M^3)$. J'appelle P' l'image de P par ce morphisme, Q' l'image de Q et R' l'image de R. On a alors que P', Q' et R' sont linéairement indépendants. Or, si I est engendré par deux éléments f et g, alors $I/(I \cap M^3)$ est engendré par f' et g' en tant que $\mathbb{R}$-espace vectoriel. On voit donc trivialement que c'est impossible de trouver 3 éléments linéairement indépendants dans cet espace.
- Par contre on vérifie que $Y = V(XZ - Y^2, X^5 + Z^3 - 2X^2YZ)$. En effet, on a $\mathscr{I}(Y) =< P, Q, R >$ donc $Y = V < P, Q, R >$. Montrons que $V(XZ - Y^2, X^5 + Z^3 - 2X^2YZ) = V < P, Q, R >$.
Soit $(x, y, z) \in V(< P, Q, R >)$. On a $xy - y^2 = 0$
et $x^5 + z^3 - 2x^2yz = x^3x^2 + z^3 - 2z^2z = yzx^2 - z^3 = 0$.

Donc $(x, y, z) \in V(XZ - Y^2, X^5 + Z^3 - 2X^2YZ)$.
Soit $(x, y, z) \in V(XZ - Y^2, X^5 + Z^3 - 2X^2YZ)$.
On a déjà $P(x, y, z) = 0$.
$Q(x, y, z) = x^3 - yz$ d'où
$Q^2(x, y, z) = x^6 - 2x^3yz + y^2z^2 = x^6 - x(x^5 + z^3) + y^2z^2 = -xz^3 + y^2z^2 = -xz^3 + xz^3 = 0$
Et enfin soit $(x, y, z) \in V(XZ - Y^2, X^5 + Z^3 - 2X^2YZ)$. Si $x = 0$, alors $z^3 = 0$ et donc $z = 0$ d'où $R(x, y, z) = yx^2 - z^2 = 0$. On suppose alors $x \neq 0$. On a $xR(x, y, z) = x^3y - xz^2 = y^2z - xz^2 = xz^2 - xz^2 = 0$. Donc $R(x, y, z) = 0$.

$\square$

Bibliographie :

Perrin, D. (1995). *Géométrie algébrique : une introduction.* Paris : Jouve. (CNRS Éditions)

Cox, D., Little, J., O'Shea, D. (1992) *Ideals, varieties and algorithms.* USA. (Springer-Verlag)

Tauvel, P. (2007). *Corps commutatifs et théorie de Galois.* Paris. (Calvage et Mounet)

Mumford, D. *The red book on varieties and schemes.* (Springer-Verlag)

Bourbaki, N. (2006). *Element de mathématiques : Chapitre 8 et 9 Algèbre commutative.* (Springer)

Hartshorne, R. (1977). *Algebraic Geometry.* (Springer-Verlag)

Atiyah, M.F, Macdonald, I.G. *Introduction to commutative algebra.*

`http://wstein.org/edu/2010/581b/books/atiyah-macdonald-introduction_to_commutative_algebra.pdf`

Pierron, T. *Algèbre commutative et géométrie algébrique.*

`http://perso.eleves.ens-rennes.fr/~tpier758/cours/acga.pdf`