Extensions d'anneaux – Introduction à la géométrie algébrique

Marc SAGE

Table des matières

Tous les anneaux seront considérés commutatifs et unitaires.

Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux (ce qui implique $\varphi(1_A) = 1_B$), on munira B d'une structure de A-algèbre via la loi externe $a \cdot b = \varphi(a)\, b$, et quitte à se placer dans $\varphi(A)$, on supposera $A \subset B$.

1 Préliminaires

1.1 Radical de Jacobson d'un anneau

Définition.

Soit A un anneau. On appelle radical de Jacobson *de A l'ensemble des $x \in A$ tels que $1+ax$ soit inversible pour tout $a \in A$. On le note*

$$\operatorname{Rad} A = \{x \in A \text{ tels que } 1 + Ax \subset A^*\}.$$

Propriétés.

• *Le radical de Jacobson est le plus grand idéal I tel que $\forall i \in I$, $1+i$ soit inversible, c'est-à-dire*

$$\operatorname{Rad} A = \max\{I \text{ idéal tel que } 1 + I \subset A^*\}.$$

• *Le radical de Jacobson est l'infimum des idéaux maximaux, c'est-à-dire*

$$\operatorname{Rad} A = \bigcap_{\mathfrak{M} \text{ idéal maximal}} \mathfrak{M}.$$

Démonstration.

• $\operatorname{Rad} A$ est un idéal de A. En effet, $0 \in \operatorname{Rad} A$; si $x, y \in \operatorname{Rad}$ et $a \in A$, alors $1 + a(x+y)$ est inversible car

$$\begin{aligned}(1 + a(x+y))\frac{1}{1+ax}\frac{1}{1+\frac{a}{1+ax}y} &= ((1+ax)+ay)\frac{1}{1+ax}\frac{1}{1+ay\frac{1}{1+ax}} \\ &= \left(1+ay\frac{1}{1+ax}\right)\frac{1}{1+ay\frac{1}{1+ax}} \\ &= 1\,;\end{aligned}$$

enfin, si $x \in \operatorname{Rad} A$ et $a \in A$, alors $\forall b \in A$, $1 + b(ax) = 1 + (ab)x$ est inversible, donc $ax \in \operatorname{Rad} A$.

$\operatorname{Rad} A$ est donc est un idéal de A, qui vérifie clairement $1 + \operatorname{Rad} A \subset A^*$. Soit maintenant I un idéal de A qui vérifie $1 + I \subset A^*$. Soit $x \in I$ et $a \in A$. On a $ax \in I$, donc $1 + ax \in A^*$; d'où $x \in \operatorname{Rad} A$, et $I \subset \operatorname{Rad} A$.

• Soit $x \in \bigcap_{\mathfrak{M} \text{ idéal maximal}} \mathfrak{M}$. Supposons par l'absurde que $x \notin \operatorname{Rad} A$. Il existe donc $a \in A$ tel que $y := 1+ax$ ne soit pas inversible. L'idéal Ay est donc contenu dans un idéal maximal, mettons $\mathfrak{M}' \ni y$. Alors $x \in \mathfrak{M}'$, donc $ax \in \mathfrak{M}'$, d'où $y - ax \in \mathfrak{M}'$, c'est-à-dire $1 \in \mathfrak{M}'$, *absurde*. On a donc $\bigcap_{\mathfrak{M} \text{ idéal maximal}} \mathfrak{M} \subset \operatorname{Rad} A$.

Réciproquement, soit $x \in \operatorname{Rad} A$, et soit $\mathfrak{M}$ un idéal maximal de A. L'idéal $\mathfrak{M} + Ax$ est un idéal qui contient $\mathfrak{M}$, donc qui vaut $\mathfrak{M}$ ou A. Si $\mathfrak{M}+Ax = A$, on aurait $1 = m+ax$ pour un $m \in M$ et un $a \in A$; comme $x \in \operatorname{Rad} A$, $1-ax$ est inversible, c'est-à-dire m inversible, *absurde*. On a donc $\mathfrak{M}+Ax = \mathfrak{M}$, donc $x = 0+1x \in \mathfrak{M}+Ax = \mathfrak{M}$. On en déduit $\operatorname{Rad} A \subset \mathfrak{M}$ et $\operatorname{Rad} A \subset \bigcap_{\mathfrak{M} \text{ idéal maximal}} \mathfrak{M}$.

1.2 Racine d'un idéal.

Définition.

On appelle radical *ou* racine *d'un idéal I d'un anneau A l'ensemble de toutes les racines n-ièmes des éléments I pour n décrivant $\mathbb{N}^*$. On le note $\sqrt{I}$* ou

$$\operatorname{Rad} I = \{a \in A \text{ tels que } \exists n \geq 1 \text{ avec } a^n \in I\}.$$

On dira qu'un idéal I est semi-premier *ou* radical *s'il est égal à sa racine, c'est-à-dire si*

$$I = \operatorname{Rad} I,$$

ou encore si

$$\left\{ \begin{array}{l} \forall x \in A \\ \forall n \geq 1 \end{array} \right. , x^n \in I \implies x \in I.$$

Remarques. La terminologie d'idéal semi-premier vient de ce que tout idéal premier est semi-premier. On utilisera plutôt le terme "radical" par la suite. On retiendra donc

$$\textit{premier} \implies \textit{radical}.$$

Propriété.
Soit $I_1, ..., I_n$ des idéaux de A. Alors

$$\operatorname{Rad}(I_1 \cap ... \cap I_n) = (\operatorname{Rad} I_1) \cap ... \cap (\operatorname{Rad} I_n).$$

Démonstration.
Il suffit de le montrer pour $n = 2$. Soient donc I et J deux idéaux de A.
Si $x \in \operatorname{Rad}(I \cap J)$, on a un $n \geq 1$ tel que $x^n \in I \cap J$, d'où $x^n \in I$, donc $x \in \operatorname{Rad} I$, et de même $x \in \operatorname{Rad} J$, donc $x \in (\operatorname{Rad} I) \cap (\operatorname{Rad} J)$.
Si $x \in (\operatorname{Rad} I) \cap (\operatorname{Rad} J)$, on a des $n, m \geq 1$ tel que $\left\{ \begin{array}{l} x^n \in I \\ x^m \in J \end{array} \right.$, d'où $x^{n+m} \in I \cap J$, donc $x \in \operatorname{Rad}(I \cap J)$.

Corollaire.
*Toute intersection **finie** d'idéaux radicaux est un idéal radical.*

Propriété.
Soit I un idéal de A. Alors $\operatorname{Rad} I$ *est le plus petit idéal J radical contenant I, c'est-à-dire*

$$\operatorname{Rad} I = \bigcap_{J \text{ idéal radical } \supset I} J.$$

En particulier, $\operatorname{Rad} I$ *est radical et contient I, c'est-à-dire*

$$I \subset \operatorname{Rad} I = \operatorname{Rad} \operatorname{Rad} I.$$

Démontration.
$\operatorname{Rad} I$ contient les x^n pour $x \in I$ et $n = 1$, d'où $I \subset \operatorname{Rad} I$.
Montrons que $\operatorname{Rad} I$ est un idéal. Déjà $\operatorname{Rad} I$ contient $0 \in I$. Ensuite, soient $x, y \in \operatorname{Rad} I : \exists p, q \geq 1$ tels que $x^p, y^q \in I$, donc

$$\begin{array}{rcl} (x+y)^{p+q-1} & = & \displaystyle\sum_{i+j=p+q-1} \binom{p+q-1}{i} x^i y^j \\ & = & \displaystyle\sum_{i=0}^{p-1} \binom{p+q-1}{i} x^i y^{p+q-1-i} + \sum_{j=0}^{q-1} \binom{p+q-1}{j} x^{p+q-1-j} y^j \\ & = & \displaystyle\left[\sum_{i=0}^{p-1} \binom{p+q-1}{i} x^i y^{p-1-i} \right] \underbrace{y^q}_{\in i} + \left[\sum_{j=0}^{q-1} \binom{p+q-1}{j} x^{q-1-j} y^j \right] \underbrace{x^p}_{\in I} \\ & \in & I, \end{array}$$

d'où $x + y \in \operatorname{Rad} I$. De plus, si $x^n \in I$, alors $(ax)^n = (a^n) x^n \in I$ pour tout $a \in A$, d'où $ax \in \operatorname{Rad} I$.
Montrons que $\operatorname{Rad} I$ est radical, ce qui montrera $\bigcap_{J \text{ idéal radical } \supset I} J \subset \operatorname{Rad} I$. On a d'une part $\operatorname{Rad} I \subset \operatorname{Rad} \operatorname{Rad} I$ d'après ce qui précède, et d'autre part, on a les implications

$$\begin{array}{rl} & x \in \operatorname{Rad} \operatorname{Rad} I \\ \implies & \exists n \geq 1 \text{ tel que } x^n \in \operatorname{Rad} I \\ \implies & \exists n \geq 1, \exists m \geq 1 \text{ tels que } (x^n)^m \in I \\ \implies & \exists nm \geq 1 \text{ tel que } x^{nm} \in I \\ \implies & x \in \operatorname{Rad} I, \end{array}$$

d'où l'inclusion $\operatorname{Rad}\operatorname{Rad} I \subset \operatorname{Rad} I$.

Soit maintenant J un autre idéal radical qui contient I. Soit $x \in \operatorname{Rad} I$: $\exists n \geq 1$ tel que $x^n \in I \subset J$, donc $x \in \operatorname{Rad} J = J$. Ainsi, $\operatorname{Rad} I \subset \bigcap_{J \text{ idéal radical } \supset I} J$.

Propriété.
Soit I un idéal de A. Alors $\operatorname{Rad} I$ *est l'infimum de tous les idéaux premiers contenant I, c'est-à-dire*

$$\operatorname{Rad} I = \bigcap_{J \text{ idéal premier } \supset I} J.$$

Démontration.
On a déjà $\operatorname{Rad} I = \bigcap_{J \text{ idéal radical } \supset I} J \subset \bigcap_{J \text{ idéal premier } \supset I} J$ car tout idéal premier est radical.

D'autre part, soit $x \notin \operatorname{Rad} I$. On va exhiber un idéal premier J contenant I et pas x.

Soit $\mathcal{J}$ l'ensemble des idéaux contenant I et ne contenant aucune puissance $x^{n \geq 1}$, ordonné par l'inclusion. $\mathcal{J}$ est non vide car il contient I, et est faiblement inductif car toute chaîne $(J_\omega)_{\omega \in \Omega}$ de $\mathcal{J}$ admet un sup $\bigcup_\Omega J_\omega$ dans $\mathcal{J}$. $\mathcal{J}$ admet donc un élément maximal J. Montrons que J est premier.

Si ce n'est pas le cas, on peut trouver $a, b \notin J$ tels que $ab \in J$. Alors l'idéal $J+(a)$ contenant I est strictement plus grand que J, donc n'est pas dans $\mathcal{J}$, c'est-à-dire contient une puissance x^n, d'où un $j \in J$ et un $\lambda \in A$ tels que $x^n = j + \lambda a$. De même, on aurait une puissance $x^m = i + \mu b$ pour un $i \in J$ et $\mu \in A$. On en déduit

$$\begin{aligned} x^{n+m} &= \underbrace{ij + i\lambda a + j\mu b}_{\in J} + \underbrace{ab}_{\in J}\lambda\mu \\ &\in J, \end{aligned}$$

absurde.

On a donc montré que si $x \in A$, on

$$x \notin \operatorname{Rad} I \implies \exists J \text{ idéal premier } \supset I \text{ tel que } x \notin J,$$

c'est-à-dire (par contraposée)

$$\forall J \text{ idéal premier } \supset I \text{ tel que } x \in J,\ x \in \operatorname{Rad} I,$$

ou encore

$$\bigcap_{J \text{ idéal premier } \supset I} J \subset \operatorname{Rad} I.$$

1.3 Nilradical d'un anneau

Définition.
On appelle nilradical *d'un anneau A l'ensemble de ses éléments nilpotents. On le note*

$$\operatorname{Nilrad} A = \{a \in A \text{ tels que } \exists n \geq 1 \text{ avec } a^n = 0\}.$$

Propriété.
Le nilradical d'un anneau est l'infimum de ses idéaux premiers, c'est-à-dire

$$\operatorname{Nilrad} A = \bigcap_{J \text{ idéal premier}} J.$$

Démonstration.
On a

$$\begin{aligned} \operatorname{Nilrad} A &= \operatorname{Rad}\{0\} \\ &= \bigcap_{J \text{ idéal premier } \supset \{0\}} J \\ &= \bigcap_{J \text{ idéal premier}} J. \end{aligned}$$

1.4 Quelques définitions

Définition.
*On dit que B est une A-*algèbre de type fini *si, en tant que A-algèbre, B est engendrée par un nombre fini d'éléments, c'est-à-dire si*

$$B = A[x_1, ..., x_n]$$

où $x_1, ..., x_n \in B$.
*On dit que B est une A-*algèbre finie *si, en tant que A-module, B est de type fini, c'est-à-dire si*

$$B = Ax_1 + ... + Ax_n$$

où $x_1, ..., x_n \in B$ (c'est l'analogue des extensions finies en théorie des corps).
On dit que $x \in B$ est entier *sur A s'il est annulé par un polynôme* ***unitaire*** *(non constant) à coefficients dans A, c'est-à-dire si*

$$x^n + a_1 x^{n-1} + ... + a_n = 0$$

où $a_1, ..., a_{n\geq 1} \in A$. (c'est l'analogue du caractère algébérique en théorie des corps).
On dit que $A \subset B$ est une extension entière *si tout élément de B est entier sur A.*

La notion d'intégrité (c'est-à-dire le fait d'être entier) sur les anneaux est à rapprocher de la notion d'algébricité en théorie des corps.

2 Théorème de Cayley-Hamilton – Lemme de Nakayama

2.1 Théorème de Cayley-Hamilton et corollaires

Théorème (Cayley-Hamilton).
Soit M un A-module ***de type fini*** *et $u : M \longrightarrow M$ un endomorphisme (A-linéaire). Alors il existe un polynôme annulateur de u* ***unitaire****, c'est-à-dire*

$$u^n + a_1 u^{n-1} + ... + a_n = 0.$$

Si de plus $u(M) \subset IM$ où I un idéal de A (ce que l'on peut toujours supposer, quitte à prendre $I = A$), alors on peut prendre $a_j \in I^j$ pour $1 \leq j \leq n$.

Démonstration.
M est de type fini, donc se décompose en $M = Am_1 + ... + Am_n$. Les $u(m_i)$ se décomposent en $\sum_{j=1}^n \lambda_{i,j} m_j$ où $\lambda_{i,j} \in I$. Soit $\Lambda = (\lambda_{i,j}) \in \mathcal{M}_n(I)$. On regarde $M^n = M \times ... \times M$ comme un $A[X]$-module où X agit via u sur chaque composante, c'est-à-dire $P \cdot x = P(u)(x)$. Alors on a le système

$$u(m_i) = \sum_{j=1}^n \lambda_{i,j} m_j \text{ pour } i = 1, ..., n,$$

c'est-à-dire

$$XI_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \Lambda \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix},$$

ou encore

$$\begin{pmatrix} XI_n - \Lambda \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

On en déduit

$$\left[\det \begin{pmatrix} XI_n - \Lambda \end{pmatrix}\right] \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = {}^t\mathrm{Com} \begin{pmatrix} XI_n - \Lambda \end{pmatrix} \underbrace{\begin{pmatrix} XI_n - \Lambda \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}}_{=0}$$

$$= 0.$$

Ici, $\det\left(\begin{array}{c} XI_n - \Lambda \end{array}\right)$ est un polynôme P unitaire qui annule u sur les générateurs m_i (remarquer que

$$\begin{array}{rcl} \begin{pmatrix} P(u)(m_1) \\ \vdots \\ P(u)(m_n) \end{pmatrix} & = & \left[\det\left(\begin{array}{c} XI_n - \Lambda \end{array}\right)\right]\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \\ & = & 0), \end{array}$$

donc qui annule u partout.

De plus, pour avoir un terme en X^{n-i} dans

$$\det\left(\begin{array}{c} XI_n - \Lambda \end{array}\right) = \begin{vmatrix} X-\lambda_{1,1} & -\lambda_{1,2} & \cdots & -\lambda_{1,n} \\ -\lambda_{2,1} & X-\lambda_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ -\lambda_{n,1} & \cdots & \cdots & X-\lambda_{n,n} \end{vmatrix},$$

il faut prendre un produit de $n-i$ termes X^{n-i} et de i termes $\lambda_{p,q}$ (donc dans I), ce qui fait un produit total dans I^i, d'où $a_i \in I^i$.

Corollaire.

Soit M un A-module de type fini, u un endomorphisme de M. Si u surjectif, alors u est bijectif.

Soit M un A-module de libre type fini, $M \simeq A^n$. Alors tout système de générateurs de M formé de n élements est une base.

Démonstration.

On voit M comme un $A[X]$-module, où x agit via u. Soit I l'idéal engendré par X, c'est-à-dire $I = XA[X]$. u surjectif, donc $M = XM = IM$. On applique Cayley-Hamilton à $v = \mathrm{Id}_M$, d'où un polynôme $P \in A[X][Y]$ annulateur de $v = \mathrm{Id}$, mettons

$$P = Y^n + a_1(X)Y^{n-1} + ... + a_n(X)$$

où $a_i \in A[X]$. On a ainsi

$$\mathrm{Id} + a_1(X)\mathrm{Id} + ... + a_n(X)\mathrm{Id} = 0,$$

c'est-à-dire

$$\mathrm{Id} + a_1(u) + ... + a_n(u) = 0.$$

Or chaque $a_i(X) \in I^i \subset I$, donc s'écrit $a_i(X) = Xb_i(X)$, d'où

$$\begin{array}{rcl} \mathrm{Id} + u(b_1(u) + ... + b_n(u)) & = & 0 \\ \mathrm{Id} + (b_1(u) + ... + b_n(u))u & = & 0 \\ (-b_1(u) - ... - b_n(u))u & = & \mathrm{Id}, \end{array}$$

d'où u injectif.

Corollaire.

Soit M un A-module de type fini, I idéal tel que $M = IM$. Alors $\exists r \in I$ tel que $(1-r)M = \{0\}$.

Démonstration.

M est un A-module, $u = \mathrm{Id}_M$ est un endomorphisme de M tel que $u(M) \subset IM$, d'où un $P \in A[X]$ tel que $\mathrm{Id}^n + a_1\mathrm{Id}^{n-1} + ... + a_n\mathrm{Id}^0 = 0$ avec $a_i \in I^i \subset I$; on prend $r \in -(a_1 + ... + a_n) \in I$.

2.2 Lemme de Nakayama

Proposition (lemme de Nakayama).
Soit M un A-module de type fini, $I \subset \operatorname{Rad} A$ un idéal de A tel que $M = IM$. Alors $M = \{0\}$.

Démonstration.
Comme $M = IM$, $\exists r \in I$ tel que $(1-r)M = \{0\}$. Il suffit de voir que $(1-r)$ est inversible. Si ce n'est pas le cas, $1-r$ engendre un idéal propre de A, donc est contenu dans un idéal maximal $\mathfrak{M}_0$. Or $r \in I \subset \bigcap_{\mathfrak{M} \text{ idéal maximal}} \mathfrak{M} \subset \mathfrak{M}_0$, donc $1 = (1-r) + r \in \mathfrak{M}_0$, *absurde*.

Typiquement, on l'utilise quand A est local, c'est-à-dire quand il existe un unique idéal maximal $\mathfrak{M}$, et à $I = \mathfrak{M}$.

3 Extensions finies et entières

3.1 Propriétés basiques

Proposition.
Soient $A \subset B$ et $x \in B$. On a équivalence entre
- *x est entier sur A ;*
- *$A[x]$ est une A-algèbre finie ;*
- *il existe une A-algèbre finie A' telle que*

$$A \subset A[x] \subset A' \subset B.$$

Démonstration.
$(i) \implies (ii)$ Si $x^n + a_1 x^{n-1} + ... + a_n = 0$, alors $A[x] = A + Ax + ... + Ax^{n-1}$ est finie (comme en théorie des corps).
$(ii) \implies (iii)$ Trivial (prendre $A' = A[x]$).
$(iii) \implies (i)$ A' est un A-module de type fini, qui contient x. On considère $u : \left\{ \begin{array}{ccc} A' & \longrightarrow & A' \\ a' & \longmapsto & a'x \end{array} \right.$ A-linéaire. Cayley-Hamilton donne $P \in A[X]$ unitaire tel que $P(u) = 0$, mettons

$$u^n + a_1 u^{n-1} + ... + a_n = 0,$$

d'où (en évaluant en $a' = 1$)

$$x^n + a_1 x^{n-1} + ... + a_n = 0.$$

Corollaire.
Toute extension finie est entière.

Démonstration.
Soit $A \subset B$ finie et $x \in B$. $A[x] \subset B$ est alors finie, donc x est entier sur A.

Proposition.
Soient $A \subset B \subset C$ des anneaux.
- *Si C finie sur B et B finie sur A, alors C est finie sur A ;*
- *Si $y_1, ..., y_n$ sont dans B entiers sur A, alors $A[y_1, ..., y_n]$ est finie (donc entière) sur A ;*
- *Si C entière sur B et B entière sur A, alors C est entière sur A.*

Démonstration.

• Si $C = By_1 + ... + By_n$ et $B = Ax_1 + ... + Ax_m$, alors

$$C = Ax_1y_1 + ... + Ax_1y_n \ + \ Ax_2y_1 + ... + Ax_2y_n \ + ... + \ Ax_my_1 + ... + Ax_my_n$$

(comme en théorie des corps).

• Une récurrence immédiate donne la finitude, et le corollaire précédent donne l'intégrité.

• Soit $c \in C$. C entier sur B, mettons $c^n + b_1c^{n-1} + ... + b_n = 0$ où $b_i \in B$. Notons $A' = A[b_1, ..., b_n]$. D'une part,

$$A'[c] = A' + A'c + ... + A'c^{n-1}$$

est finie sur A', d'autre part A' est finie sur A (car chaque b_i est entier sur A), donc $A \subset A[b_1, ..., b_n, c]$ est finie, a fortiori entière, donc $c \in A[b_1, ..., b_n, c]$ est entier sur A.

3.2 Clôture intégrale

Définition.
Soit $A \subset B$ une extension.
On appelle clôture entière *de A dans B* l'ensemble

$$\widetilde{A} = \{b \in B \text{ tel que } b \text{ entier sur } A\}$$

(remarquer la dépendance de $\widetilde{A}$ en B).

A est dit intégralement clos *dans B si $\widetilde{A} = A$.*

Si A est intègre, on dit que A est intégralement clos *ou* normal *s'il est intégralement clos dans son corps des fractions.*

Propriétés.
• *$\widetilde{A}$ est un anneau, et on a la tour d'extensions $A \subset \widetilde{A} \subset B$;*
• *$A \subset \widetilde{A}$ est entière ;*
• *$\widetilde{\widetilde{A}} = \widetilde{A}$.*

Démonstration.
• Soient $b, b' \in \widetilde{A}$: $b + b'$ et bb' sont dans $A[b, b']$ qui est une A-algèbre finie (cf proposition précédente), donc $b + b'$ et bb' sont entiers sur A, donc restent dans $\widetilde{A}$. Comme $1_A \in \widetilde{A}$, $\widetilde{A}$ est un sous-anneau de B, donc est un anneau.

• $A \subset \widetilde{A}$ est entière par définition.

• On a clairement $\widetilde{A} \subset \widetilde{\widetilde{A}}$. De plus, $\widetilde{\widetilde{A}}$ est entière sur $\widetilde{A}$ et $\widetilde{A}$ est entière sur A, donc (cf proposition précédente) $\widetilde{\widetilde{A}}$ est entière sur A, donc $\widetilde{\widetilde{A}} \subset \widetilde{A}$.

Proposition.
Tout anneau factoriel est intégralement clos.

Démonstration.
Soit $r = \frac{p}{q} \in \text{Frac}\, A$ entier sur A, avec $p \wedge q = 1$. Alors $r^n + a_1r^{n-1} + ... + a_n = 0$, d'où $p^n + q(...) = 0$, donc $q \mid p$, c'est-à-dire $q = 1$, d'où $r = p \in A$.

3.3 Lemme de Gauss - Clôture intégrale de $A[X]$

Lemme.
Soit $A \subset B$ une extension et *$P \in A[X]$* ***unitaire****.*
Si $P = QR$ dans $B[X]$ (avec Q et R ***unitaires****), alors les coefficients de Q et R sont entiers sur A.*

Démonstration.

On fabrique une extension $B \subset C$ dans laquelles Q et R se factorisent, comme on construirait un corps de rupture de P. On considère le B-module $B_1 = {}^{B[X]}\!/_{Q}$, libre de rang $\deg Q$ (on dispose de la division euclidienne, car Q unitaire !), $\alpha_1 = \overline{X} \in B_1$ est alors racine de Q dans B_1, c'est-à-dire $Q(Y) = (Y - \alpha_1) Q_1(Y)$, et on recommence. Ainsi, $Q = \prod (X - \alpha_i)$ et $R = \prod \left(X - \beta_j\right)$ dans une extensions $B \subset C$. Alors les α_i sont racines de P dans C, donc sont entiers sur A, donc les coefficients de Q (qui sont des fonctions symétriques élémentaires en les racines α_i) sont entiers sur A.

Corollaire (lemme de Gauss).
Soit A intégralement clos, $K = \operatorname{Frac} A$, et $P \in A[X]$ ***unitaire****.*
Si $P = QR$ dans $K[X]$ (avec Q et R ***unitaires****), alors Q et R sont dans $A[X]$.*

Proposition.
Si A est intégralement clos, alors $A[X]$ est intégralement clos.

Démonstration.
Remarquons déjà que $\operatorname{Frac}(A[X]) = K(X)$, ce qu'on obtient en simplifiant les dénominateurs des coefficients d'un élément de $K(X)$.
Soit $F \in K(X)$ entier sur $A[X] : \exists a_1(X), ..., a_n(X) \in A[X]$ tels que

$$F^n + a_1(X) F^{n-1} + ... + a_{n-1}(X) F + a_n(X) = 0.$$

K est un corps, donc un anneau factoriel, donc $K[X]$ factoriel, donc intégralement clos (dans $K(X)$). Or F est entier sur $K[X]$, donc sur $K(X)$, donc $F \in K[X]$.
On aimerait travailler avec des polynômes unitaires pour pouvoir appliquer le lemme de Gauss à

$$a_n(X) = -F\left(F^{n-1} + a_1(X) F^{n-2} + ... + a_{n-1}(X)\right).$$

On pose pour cela $G = F - X^r$ où $r > \deg F$, de sorte que

$$F = X^r + G$$

où $-G$ unitaire. On a alors

$$(X^r + G)^n + a_1(X)(X^r + G)^{n-1} + ... + a_n(X) = 0,$$

d'où

$$G^n + b_1(X) G^{n-1} + ... + b_n(X) = 0$$

où $b_n = X^{nr} + a_1(X) X^{(n-1)r} + ... + a_n(X)$ unitaire pour r assez grand. On réécrit

$$b_n(X) = -G\left(G^{n-1} + b_1(X) G^{n-2} + ... + b_{n-1}(X)\right).$$

ce qui est une décomposition de $b_n \in A[X]$ unitaire en produit de facteurs unitaires (pour r assez grand) sur $K[X]$, donc le lemme de Gauss s'applique, c'est-à-dire $-G \in A[X]$, ou encore $F \in A[X]$.

4 Lemme de normalisation de Noether

Définition.
On dira que des éléments $x_1, ..., x_n$ d'une k-algèbre sont algébriquement liés *si $\exists P \in k[X_1, ..., X_n]$ non nul tel que $P(x_1, ..., x_n) = 0$.*
On dit sinon que $x_1, ..., x_n$ sont algébriquement indépendants*, c'est-à-dire si*

$$P(x_1, ..., x_n) = 0 \implies P = 0 \text{ dans } k[X_1, ..., X_n].$$

On dira qu'une k-algèbre A de type fini est une extension algébrique pure *de k si on peut écrire $A = k[x_1, ..., x_n]$ avec $x_1, ..., x_n$ algébriquement indépendants.*
Par convention, $A = k = k[\emptyset]$ est algébrique pure sur k.

Théorème (lemme de normalisation de Noether).
Soit k un corps, A une k-algèbre de type fini. Alors $\exists y_1, ...y_m \in A$ algébriquement indépendants tels que A soit une $\widetilde{A} = k[y_1, ..., y_m]$-algèbre finie, c'est-à-dire

$$\underbrace{\overbrace{k \subset k[y_1, ..., y_m]}^{\text{algébrique pure}} = \overbrace{\widetilde{A} \subset A}^{\text{finie}}.}_{\text{algébrique de type fini}}$$

Lemme.
Soit $A = k[x_1, ..., x_{n\geq 1}]$ une k-algèbre de type fini où les $x_i \in A$ sont algébriquement liés. Alors il existe $x_1^*, ..., x_{n-1}^* \in A$ tels que x_n soit entier sur $A^* = k\left[x_1^*, ..., x_{n-1}^*\right]$ et $A = A^*[x_n]$.

Démonstration .
En notations multi-indices, on a

$$\begin{aligned} x &= (x_1, ..., x_n) \\ P(x) &= \sum_\alpha \lambda_\alpha x^\alpha = 0 \end{aligned}$$

où $(\lambda_\alpha) \neq 0$.

Première méthode :
On cherche les x_i^* sous la forme $x_i^* = x_i - x_n^{r_i}$ où r_i à choisir, c'est-à-dire

$$x_i = x_i^* + x_n^{r_i} \text{ pour } 1 \leq i < n.$$

On a déjà

$$\begin{aligned} A^*[x_n] &= k\left[x_1^*, ..., x_{n-1}^*\right][x_n] \\ &= k\left[x_1^*, ..., x_{n-1}^*, x_n\right] \\ &= k[x_1 - x_n^{r_1}, ..., x_{n-1} - x_n^{r_{n-1}}, x_n] \\ &= k[x_1, ..., x_{n-1}, x_n] \qquad (\text{car } x_i = (x_i - x_n^{r_i}) + (x_n)^{r_i}) \\ &= A. \end{aligned}$$

De plus,

$$\begin{aligned} 0 &= P(x_1, ..., x_n) \\ &= P\left(x_1^* + x_n^{r_1}, ..., x_{n-1}^* + x_n^{r_{n-1}}, x_n\right) \\ &= Q\left(x_1^*, ..., x_{n-1}^*, x_n\right) \end{aligned}$$

où $Q \in P[X_1, ..., X_n]$. On voudrait que le coefficient dominant de x_n dans Q soit non nul (pour pouvoir l'inverser dans k), ce qui montrerait alors que x_n est entier sur $k\left[x_1^*, ..., x_{n-1}^*\right]$, d'où le lemme.

Explicitons

$$\begin{aligned} Q\left(x_1^*, ..., x_{n-1}^*, x_n\right) &= P\left(x_1^* + x_n^{r_1}, ..., x_{n-1}^* + x_n^{r_{n-1}}, x_n\right) \\ &= \sum_\alpha \lambda_\alpha x_n^{\alpha_n} \prod_{i=1}^{n-1} \left(x_i^* + x_n^{r_i}\right)^{\alpha_i}. \end{aligned}$$

Pour avoir le coefficient dominant de x_n dans Q, on regarde déjà les termes dominants de x_n de chacun des termes de Q, c'est-à-dire

$$\begin{aligned} \text{terme dominant en } x_n \text{ dans } \lambda_\alpha x^\alpha &= \text{terme dominant en } x_n \text{ dans } \lambda_\alpha x_n^{\alpha_n} \prod_{i=1}^{n-1} \left(x_i^* + x_n^{r_i}\right)^{\alpha_i} \\ &= \lambda_\alpha x_n^{\alpha_n + \sum_{i=1}^{n-1} \alpha_i r_i}. \end{aligned}$$

En posant

$$\nu(\alpha, \overrightarrow{r}) = \alpha_n + \sum_{i=1}^{n-1} \alpha_i r_i,$$

on en déduit

$$\begin{aligned}\text{terme dominant en } x_n \text{ dans } Q &= \text{terme dominant en } x_n \text{ dans} \\ &\quad \sum_{\lambda_\alpha \neq 0} \text{terme dominant en } x_n \text{ dans } \lambda_\alpha x^\alpha \\ &= \text{terme dominant en } x_n \text{ dans } \sum_{\lambda_\alpha \neq 0} \lambda_\alpha x_n^{\nu\left(\alpha, \overrightarrow{r}\right)}.\end{aligned}$$

Si les $\nu\left(\alpha, \overrightarrow{r}\right)$ sont deux à deux distincts quand α varie, la somme ci-dessus (qui est prise sur un ensemble non vide car $(\lambda_a) \neq 0$) ne comportera qu'un seul terme de degré maximal en x_n, et donc le coefficient dominant recherché sera un des $\lambda_\alpha \neq 0$, inversible comme voulu.

Pour ce faire, on choisit $r_i = e^i$ où e est grand devant tous les α_i qui apparaissent. Alors $\nu\left(\alpha, \overrightarrow{r}\right) = \left(\sum_{i=1}^{n-1} \alpha_i e^i\right) + \alpha_n$ est une écriture en base e, donc unique, *CQFD*.

Deuxième méthode (si k infini) :

On cherche les x_i^* sous la forme $x_i^* = x_i - \mu_i x_n$ où les $\mu_i \in k$ sont à choisir, c'est-à-dire

$$x_i = x_i^* + \mu_i x_n \text{ pour } 1 \leq i < n.$$

On a déjà

$$\begin{aligned}A^*\left[x_n\right] &= k\left[x_1^*, ..., x_{n-1}^*\right]\left[x_n\right] \\ &= k\left[x_1^*, ..., x_{n-1}^*, x_n\right] \\ &= k\left[x_1 - \mu_1 x_n, ..., x_{n-1} - \mu_{n-1} x_n, x_n\right] \\ &= k\left[x_1, ..., x_{n-1}, x_n\right] \qquad (\text{car } x_i = (x_i - \mu_i x_n) + \mu_i\left(x_n\right)) \\ &= A.\end{aligned}$$

De plus,

$$\begin{aligned}0 &= P\left(x_1, ..., x_n\right) \\ &= P\left(x_1^* + \mu_1 x_n, ..., x_{n-1}^* + \mu_{n-1} x_n, x_n\right) \\ &= Q\left(x_1^*, ..., x_{n-1}^*, x_n\right)\end{aligned}$$

où $Q \in P\left[X_1, ..., X_n\right]$. On rappelle qu'on cherche à inverser le coefficient dominant de x_n dans Q, c'est-à-dire à ce qu'il soit non nul.

Explicitons

$$\begin{aligned}Q\left(x_1^*, ..., x_{n-1}^*, x_n\right) &= P\left(x_1^* + \mu_1 x_n, ..., x_{n-1}^* + \mu_{n-1} x_n, x_n\right) \\ &= \sum_\alpha \lambda_\alpha x_n^{\alpha_n} \prod_{i=1}^{n-1} \left(x_i^* + \mu_i x_n\right)^{\alpha_i}.\end{aligned}$$

Regardons

$$\begin{aligned}\text{terme dominant en } x_n \text{ dans } \lambda_\alpha x^\alpha &= \text{terme dominant en } x_n \text{ dans } \lambda_\alpha x_n^{\alpha_n} \prod_{i=1}^{n-1} \left(x_i^* + \mu_i x_n\right)^{\alpha_i} \\ &= \lambda_\alpha \left(\prod_{i=1}^{n-1} \mu_i^{\alpha_i}\right) x_n^{\sum_{i=1}^n \alpha_i}.\end{aligned}$$

En posant

$$\begin{aligned}\sigma(\alpha) &= \sum_{i=1}^n \alpha_i \text{ et} \\ \alpha' &= \left(\alpha_1, ..., \alpha_{n-1}\right),\end{aligned}$$

on en déduit

$$\begin{aligned}
\text{terme dominant en } x_n \text{ dans } Q &= \text{terme dominant en } x_n \text{ dans} \\
&\quad \sum_{\lambda_\alpha \neq 0} \text{terme dominant en } x_n \text{ dans } \lambda_\alpha x^\alpha \\
&= \text{terme dominant en } x_n \text{ dans } \sum_{\lambda_\alpha \neq 0} \lambda_\alpha \mu^{\alpha'} x_n^{\sigma(\alpha)} \\
&= \text{terme dominant en } x_n \text{ dans } \sum_{s \geq 0} \sum_{\substack{\lambda_\alpha \neq 0 \\ \sigma(\alpha)=s}} \lambda_\alpha \mu^{\alpha'} x_n^{\sigma(\alpha)} \\
&= \text{terme dominant en } x_n \text{ dans } \sum_{s \geq 0} \left[\sum_{\substack{\lambda_\alpha \neq 0 \\ \sigma(\alpha)=s}} \lambda_\alpha \mu^{\alpha'} \right] x_n^s.
\end{aligned}$$

Remarquer que, puisque $(\lambda_\alpha) \neq 0$, on a $\exists \lambda_{\alpha_0} \neq 0$, et donc le domaine des $\lambda_\alpha \neq 0$ vérifiant $\sigma(\alpha) = \sigma(\alpha_0)$ est non vide. Soit maintenant $s_0 \geq 0$ le plus grand $s = \sigma(\alpha)$ qui vérifie cette propriété (noter que $s \leq$ deg total de P). On a ainsi

$$\text{terme dominant en } x_n \text{ dans } \sum_{s \geq 0} \left[\sum_{\substack{\lambda_\alpha \neq 0 \\ \sigma(\alpha)=s}} \lambda_\alpha \mu^{\alpha'} \right] x_n^s = \left(\sum_{\substack{\lambda_\alpha \neq 0 \\ \sigma(\alpha)=s_0}} \lambda_\alpha \mu^{\alpha'} \right) x_n^{s_0},$$

donc on veut précisément

$$\sum_{\substack{\lambda_\alpha \neq 0 \\ \sigma(\alpha)=s_0}} \lambda_\alpha \mu^{\alpha'} \neq 0.$$

Il suffit pour cela de montrer que, pour $s \geq 0$ avec $\{\lambda_\alpha \neq 0 \text{ tels que } \nu(\alpha) = s\} \neq \emptyset$, on peut trouver des μ_i tels que

$$\sum_{\substack{\lambda_\alpha \neq 0 \\ \nu(\alpha)=s}} \lambda_\alpha \mu^{\alpha'} \neq 0\,;$$

on procède par récurrence sur $n \geq 1$.

Si $n = 1$, fixer $\nu(\alpha)$ revient à fixer α_1, c'est-à-dire α, donc la somme ci-dessus ne comporte qu'un terme λ_a avec $\lambda_\alpha \neq 0$, comme voulu. Pas de μ_i dont se soucier.

Si $n \geq 2$, en posant

$$\mu^{\alpha''} = \prod_{i=1}^{n-2} \mu_i^{\alpha_i},$$

on a

$$\begin{aligned}
\sum_{\nu(\alpha)=s} \lambda_\alpha \mu^{\alpha'} &= \sum_{\alpha_{n-1}=0}^{s} \left(\sum_{\alpha_1+\ldots+\alpha_{n-2}=s-\alpha_{n-1}} \lambda_\alpha \mu^{\alpha'} \right) \\
&= \sum_{\alpha_{n-1}=0}^{s} \left(\sum_{\alpha_1+\ldots+\alpha_{n-2}=s-\alpha_{n-1}} \lambda_\alpha \mu^{\alpha''} \mu_{n-1}^{\alpha_{n-1}} \right) \\
&= \sum_{k=0}^{s} \underbrace{\left(\sum_{\alpha_1+\ldots+\alpha_{n-2}=s-k} \lambda_\alpha \mu^{\alpha''} \right)}_{:=\xi_k} \mu_{n-1}^k,
\end{aligned}$$

et puisque $s - k \geq 0$, on peut choisir par hypothèse de récurence $\mu_1, \ldots, \mu_{n-2}$ de façon à ce que $\xi_s \neq 0$. Alors $\sum_{k=0}^{s} \xi_k \mu_{n-1}^k$ est un polynôme non nul en μ_{n-1} à coefficients ξ_k dans un corps infini, donc on peut trouver une valeur de μ_{n-1} où le dit-polynôme ne s'annule pas, c'est-à-dire $\sum_{\nu(\alpha)=s} \lambda_\alpha \mu^{\alpha'} \neq 0$, *CQFD.*

Démonstration du théorème.

A est une algèbre de type fini, donc s'écrit $A = k[x_1, ..., x_n]$. On fait une récurrence sur le nombre n de générateurs de A.

• Si $n = 0$, on a $A = k$, et alors

$$\underbrace{k \subset k[\emptyset]}_{\text{algébrique pure}} = \underbrace{\widetilde{A} \subset A}_{\text{finie}}.$$

• Supposons $n \geq 1$.

Si les x_i sont algébriquement indépendants, on pose $y_i = x_i$, d'où

$$\widetilde{A} = k[y_1, ..., y_n] = k[x_1, ..., x_n] = A,$$

donc A est bien une $\widetilde{A}$-algèbre finie, et $\widetilde{A}$ est algébrique pure sur k.

Sinon, le lemme s'applique : on écrit $A = A^*[x_n]$ où x_n est entier sur $A^* = k\left[x_1^*, ..., x_{n-1}^*\right]$. On récurre sur A^* :

$$\underbrace{k \subset k[y_1^*, ..., y_m^*]}_{\text{algébrique pure}} = \underbrace{\widetilde{A^*} \subset A^*}_{\text{finie}}.$$

Alors $A = A^*[x_n]$ est finie sur A^* (car x_n est entier sur A^*) et A^* est finie sur $\widetilde{A^*}$, donc A est finie sur $\widetilde{A^*}$, d'où

$$\underbrace{k \subset k[y_1^*, ..., y_m^*]}_{\text{algébrique pure}} = \underbrace{\widetilde{A^*} \subset A}_{\text{finie}}.$$

5 Nullstellensatz

5.1 Nullstellensatz faible k-algèbres de type fini qui sont des corps

Proposition.
*Soit $A \subset B$ une extension entière d'anneaux **intègres**. Alors*

$$A \text{ est un corps} \iff B \text{ est un corps.}$$

Démonstration.

$\boxed{\Longrightarrow}$ Soit $x \in B$, $x \neq 0$. x est entier sur A, donc

$$x^n + a_1 x^{n-1} + ... + a_n = 0.$$

On peut même supposer $a_n = 0$ car B est intègre. Alors

$$x\left(-\frac{x^{n-1} + a_1 x^{n-2} + ... + a_{n-1}}{a_n}\right) = 1,$$

donc x est inversible.

$\boxed{\Longleftarrow}$ Soit $x \in A$, $x \neq 0$. x est inversible dans B, mettons d'inverse $y \in B$, qui doit être entier sur A, disons

$$y^n + a_1 y^{n-1} + ... + a_0 = 0.$$

On multiplie par x^{n-1}, d'où

$$y + a_1 + a_2 x + ... + a_0 x^{n-1} = 0$$

et

$$y = -a_1 - a_2 x - ... - a_0 x^{n-1} \in A.$$

Théorème (Nullstellensatz faible).
Soit k un corps, K une k-algèbre de type fini qui est un corps. Alors l'extension de corps $k \subset K$ est algébrique finie.

Démonstration.
$K = k[x_1, ..., x_n]$. Le lemme de Noether dit que $\exists y_1, ..., y_m \in K$ algébriquement indépendants tels que K soit finie sur $k[y_1, ..., y_m]$, donc entière, donc la proposition précédente s'applique : $k[y_1, ..., y_m]$ est un corps. Or $k[y_1, ..., y_m] \simeq k[X_1, ..., X_m]$ en tant qu'algèbres de polynômes car les y_i sont algébriquement indépendants. C'est un corps ssi $m = 0$, c'est-à-dire $k[y_1, ..., y_m] = k$. Ainsi $k \subset K$ est finie.

Remarque. A quoi ressemblent les k-algèbres A de type fini ? Ce sont, comme toute k-algèbre de type fini qui se respecte, des quotients d'un anneau de polynômes sur k, c'est-à-dire des $k[X_1,...,X_n]/I$ où I idéal de $k[X_1, ..., X_n]$. Si l'on veut en plus que ce soit des corps, l'idéal I peut et doit être maximal.

Ainsi, *une k-algèbre K de type fini est un corps ssi*

$$K \simeq k[X_1,...,X_n]/\mathfrak{M}$$

où $\mathfrak{M}$ est un idéal maximal de $k[X_1, ..., X_n]$ (et alors $k \subset K$ est algébrique finie).

Donnons une caractérisation des idéaux maximaux de $k[X_1, ..., X_n]$ dans le cas où k algébriquement clos.

Corollaire (idéaux maximaux de $k[X_1, ..., X_n]$).
Supposons k algébriquement clos.
Alors tout idéal maximal de $k[X_1, ..., X_n]$ est de la forme

$$\mathfrak{M} = (X_1 - a_1, ..., X_n - a_n)$$

où $(a_1, ..., a_n) \in k^n$.
En d'autres termes, K est une k-algèbre de type fini qui est un corps ssi

$$K \simeq k[X_1,...,X_n]/(X_1-a_1,...,X_n-a_n)$$

où $(a_1, ..., a_n) \in k^n$.

Démonstration.
Soit $\mathfrak{M}$ un idéal maximal de $k[X_1, ..., X_n]$ et $K = k[X_1,...,X_n]/\mathfrak{M}$. D'après le Nullstellensatz faible, l'extension $k \subset K$ est algébrique, donc de degré 1 puisque k est algébriquement clos (tout x de K admet un polynôme minimal μ irréductible sur $k[X]$, donc de degré 1, mettons $\mu = X - \lambda$ où $\lambda \in k$, d'où $x = \lambda \in k$).

En notant $\overline{P}$ la classe de P modulo $\mathfrak{M}$, l'injection canonique

$$i : \left\{ \begin{array}{ccc} k & \longrightarrow & K \\ \lambda & \longmapsto & \overline{\lambda} \end{array} \right.$$

devient donc un isomorphisme (de corps). Posons $a_i = i^{-1}\left(\overline{X_i}\right) \in k$ et considérons le morphisme d'évaluation

$$f : \left\{ \begin{array}{ccc} k[X_1, ..., X_n] & \longrightarrow & k \\ P & \longmapsto & P(a_1, ..., a_n) \end{array} \right. ,$$

dont le noyau vaut

$$\operatorname{Ker} f = \mathfrak{M}.$$

En effet,

$$\begin{array}{rl} & P(a_1, ..., a_n) = 0 \\ \iff & i(P(a_1, ..., a_n)) = i(0) \\ \iff & P(i(a_1), ..., i(a_n)) = \overline{0} \\ \iff & P\left(\overline{X_1}, ..., \overline{X_n}\right) = \overline{0} \\ \iff & \overline{P(X_1, ..., X_n)} = \overline{0} \\ \iff & \overline{P} = \overline{0} \\ \iff & P \in \mathfrak{M}. \end{array}$$

D'autre part, $\operatorname{Ker} f$ contient les $X_i - a_i$ car

$$f(X_i - a_i) = [X_i - a_i](a_1, ..., a_n) = a_i - a_i = 0,$$

donc l'idéal $I = (X_1 - a_1, ..., X_n - a_n)$ est inclus dans $\text{Ker}\, f = \mathfrak{M}$. Enfin, I est un idéal maximal, car ${}^{k[X_1,...,X_n]}\!/_I$ est un corps : en notant $\widetilde{P}$ la classe de P modulo I, on a

$$\widetilde{P} = P\left(\widetilde{X_1, ..., X_n}\right) = P\left(\widetilde{X_1}, ..., \widetilde{X_n}\right) = P\left(\widetilde{a_1}, ..., \widetilde{a_n}\right) = P\left(\widetilde{a_1, ..., a_n}\right),$$

donc

$$\widetilde{P} \neq \widetilde{0} \implies P(a_1, ..., a_n) \neq 0 \implies \widetilde{P} \text{ admet un inverse } P\left(\widetilde{a_1, ..., a_n}\right)^{-1}.$$

On a ainsi $I \subset \mathfrak{M}$ avec I maximal et $\mathfrak{M} \subsetneq k[X_1, ..., X_n]$, d'où $\mathfrak{M} = I$, *CFQD.*

5.2 Variétés algébriques

Définition.

On appelle sous-variété algébrique *de k^n une partie de k^n défini par l'ensemble des zéros d'une famille de polynômes de $k[X_1, ..., X_n]$. On parlera abusivement de* variété *de k^n.*

Si J est un idéal de $k[X_1, ..., X_n]$, on définit une variété de k^n par le lieu d'annulation $V(J)$ des polynômes de J, c'est-à-dire

$$V(J) = \{(x_1, ..., x_n) \in k^n \text{ tels que } \forall P \in J,\ P(x) = 0\}$$

(V comme variété).

Si S est une partie de k^n, on définit un idéal de $k[X_1, ..., X_n]$ par l'ensemble $I(S)$ des polynômes qui s'annulent sur S, c'est-à-dire

$$I(S) = \{P \in k[X_1, ..., X_n] \text{ tels que } \forall x \in S,\ P(x) = 0\}$$

(I comme idéal).

Remarques.

• *Toute variété V de k^n peut s'écrire comme un $V(J)$.*

En effet, si V est le lieu d'annulation de la famille $(P_i)_{i \in I}$ de polynômes, prendre pour J l'idéal engendré par les P_i.

• *Les variétés $V(J)$ sont définie par un nombre fini d'équations.*

Il suffit de dire que, $k[X_1, ..., X_n]$ étant noethérien, les idéaux J sont finiment engendrés.

5.2.1 Variétés et idéaux maximaux

Proposition.

Si k est algébriquement clos et J idéal de $k[X_1, ..., X_n]$, les idéaux maximaux de ${}^{k[X_1,...,X_n]}\!/_J$ sont en correspondance bijective avec les points de $V(J)$, via

$$\Psi : \left\{ \begin{array}{ccc} \text{points de } V(J) & \longrightarrow & \text{idéaux maximaux de } {}^{k[X_1,...,X_n]}\!/_J \\ a & \longmapsto & {}^{k[X_1,...,X_n]}\!/_{(X_1 - a_1, ..., X_n - a_n)} \end{array} \right. .$$

Démontration.

Les idéaux maximaux de ${}^{k[X_1,...,X_n]}\!/_J$ sont exactement les ${}^{\mathfrak{M}}\!/_J$ où $\mathfrak{M}$ est un idéal maximal de $k[X_1, ..., X_n]$ contenant J. Il suffit donc de trouver une correspondance bijective entre ces $\mathfrak{M}$ et les poins de $V(J)$.

Un tel $\mathfrak{M}$ s'écrit $\mathfrak{M} = (X_1 - a_1, ..., X_n - a_n)$, et on a

$$P \in J \implies P \in \mathfrak{M} \implies P = \sum_{i=1}^{n} P_i \times (X_i - a_i) \implies P(a) = P(a_1, ..., a_n) = 0,$$

c'est-à-dire $\forall P \in J,\ P(a) = 0$, ou encore $a \in V(J)$.

Réciproquement, soit $a \in V(J)$ et $\mathfrak{M} = (X_1 - a_1, ..., X_n - a_n)$. On a $\forall P \in J,\ P(a) = 0$, donc J est inclus dans le noyau de

$$f : \left\{ \begin{array}{ccc} k[X_1, ..., X_n] & \longrightarrow & k \\ P & \longmapsto & P(a_1, ..., a_n) \end{array} \right.$$

qui n'est autre que $(X_1 - a_1, ..., X_n - a_n)$ (cf proposition précédente), c'est-à-dire $J \subset \mathfrak{M}$.

On dispose donc d'une correspondance entre les idéaux maximaux de $k[X_1, ..., X_n]$ contenant J et les points de $V(J)$ via les applications :

$$\Phi \ : \ \left\{ \begin{array}{ccc} \text{idéaux maximaux contenant } J & \longrightarrow & \text{points de } V(J) \\ \mathfrak{M} & \longmapsto & \left(i^{-1}\left(\overline{X_1}\right), ..., i^{-1}\left(\overline{X_n}\right)\right) \end{array} \right.$$

$$\Psi \ : \ \left\{ \begin{array}{ccc} \text{points de } V(J) & \longrightarrow & \text{idéaux maximaux contenant } J \\ a & \longmapsto & (X_1 - a_1, ..., X_n - a_n) \end{array} \right. .$$

Il reste à vérifier que Φ et Ψ sont bien réciproques l'une de l'autre. On a déjà

$$\begin{aligned} \Phi\Psi(a) &= \Phi(X_1 - a_1, ..., X_n - a_n) \\ &= \left(i^{-1}\left(\overline{X_1}\right), ..., i^{-1}\left(\overline{X_n}\right)\right) \\ &= \left(i^{-1}\left(\overline{a_1}\right), ..., i^{-1}\left(\overline{a_n}\right)\right) \\ &= (a_1, ..., a_n) \\ &= a. \end{aligned}$$

De plus,

$$\begin{aligned} \Psi\Phi(\mathfrak{M}) &= \Psi\left(i^{-1}\left(\overline{X_1}\right), ..., i^{-1}\left(\overline{X_n}\right)\right) \\ &= \left(X_1 - i^{-1}\left(\overline{X_1}\right), ..., X_n - i^{-1}\left(\overline{X_n}\right)\right) ; \end{aligned}$$

Si l'on note $\lambda_k = i^{-1}\left(\overline{X_k}\right)$, on a

$$\overline{X_k} = i\left(i^{-1}\left(\overline{X_k}\right)\right) = i(\lambda_k) = \overline{\lambda_k},$$

d'où $X_k - \lambda_k \in \mathfrak{M}$, donc

$$\begin{aligned} \Psi\Phi(\mathfrak{M}) &= \left(X_1 - i^{-1}\left(\overline{X_1}\right), ..., X_n - i^{-1}\left(\overline{X_n}\right)\right) \\ &= (X_1 - \lambda_1, ..., X_n - \lambda_n) \\ &\subset \mathfrak{M}, \end{aligned}$$

et on conclut l'égalité par la maximalité de $(X_1 - \lambda_1, ..., X_n - \lambda_n)$.

5.2.2 Variétés et idéaux en général

On dispose d'une correspondances entre les parties de k^n et les idéaux de $k[X_1, ..., X_n]$ via I et V. Que peut-on en dire ?

Propriétés.

Soient $\left\{ \begin{array}{c} J, J_1, J_2 \text{ des idéaux de } k[X_1, ..., X_n] \\ X, X_1, X_2 \text{ des parties de } k^n \end{array} \right.$ *. Alors :*

• *Les applications V et I sont décroissantes pour l'inclusion, c'est-à-dire*

$$\left\{ \begin{array}{l} J_1 \subset J_2 \implies V(J_2) \subset V(J_1) \\ X_1 \subset X_2 \implies I(X_2) \subset I(X_1) \end{array} \right. ;$$

• *$J \subset I(V(J))$ avec $=$ ssi (cf théorème suivant) ;*

• *$X \subset V(I(X))$ avec $=$ ssi X est une variété de k^n.*

Démonstration.

• Soit $x \in V(J_2)$. x est annulé par tous les polynômes de J_2, a fortiori de J_1, c'est-à-dire $x \in V(J_1)$.
Soit $P \in I(X_2)$. P annule tous les points de X_2, a fortiori de X_1, c'est-à-dire $P \in I(X_1)$.

• Soit $P \in J$. Pour $x \in V(J)$ on a $P(x) = 0$, et ce $\forall x \in V(J)$, donc $P \in I(V(J))$.

• Soit $x \in X$. Pour $P \in I(X)$ on a $P(x) = 0$, et ce $\forall P \in I(X)$, donc $x \in V(I(X))$.

Si on a égalité, X est la variété associée à $I(X)$. Réciproquement, si X est une variété $V(J)$, le deuxième point nous donne $J \subset I(V(J))$, d'où (en appliquant le premier point) $V(I(X)) = V(I(V(J))) \subset V(J) = X$, et on dispose déjà de l'inclusion inverse.

Types de problèmes pour le cas d'égalité $J = I(V(J))$:

• *k non algébriquement clos :*

Typiquement, $\mathbb{R}$. Prendre par exemple $J = \left(X^2 + Y^2\right)$: on a $V(J) = \{(0,0)\}$ puis $I(\{(0,0)\}) = (X, Y)$, d'où l'inclusion stricte $J \subsetneq I(V(J))$.

• *les puissances :*

Si $P \in k[X_1, ..., X_n]$, on a en effet $V((P)) = V((P^r))$ pour $r \geq 1$. Donc si l'égalité était vraie partout, elle le serait en P et en P^2, d'où $(P) = I(V(P)) = I(V(P^r)) = \left(P^2\right)$, *absurde.*

5.2.3 Nullstellensatz fort

Théorème (Nullstellensatz fort).

Soit k algébriquement clos et J un idéal propre de $k[X_1, ..., X_n]$. Alors :

• $V(J) \neq \emptyset$;

• $I(V(J)) = \operatorname{Rad} J$.

Lemme.

Soit I un idéal de $k[X_1, ..., X_n]$ engendré par des poynômes n'ayant aucune racine commune. Alors $I = k[X_1, ..., X_n]$ tout entier.

Démontration.

Si $I \subsetneq k[X_1, ..., X_n]$, on peut l'inclure dans un idéal maximal $(X_1 - a_1, ..., X_n - a_n)$, donc tous les éléments de I s'annulent en $(a_1, ..., a_n)$, *absurde.*

Démontration du théorème.

• Soit $\mathfrak{M}$ un idéal maximal contenant J (possible car $J \subsetneq k[X_1, ..., X_n]$). A $\mathfrak{M}$ correspond un point de $V(J)$ via la dernière proposition, donc $V(J) \neq \emptyset$.

• Soit P non nul dans $I(V(J))$. On plonge J dans $k[X_1, ..., X_n, Y]$ – où Y est là pour inverser P. Posons $J' = (J, PY - 1)$. Montrons que $1 \in J'$ à l'aide du lemme.

Soient $j_1, ..., j_k$ des générateurs de J. Alors les j_i et $PY - 1$ ne peuvent avoir de racines communes. En effet, si $\exists a = (a_1, ..., a_{n+1}) \in k^{n+1}$ annulant tous les j_i, on a que $a' = (a_1, ..., a_n)$ annule tous les j_i, donc a' annule tous les éléments de J, c'est-à-dire $a' \in V(J)$, d'où $[PY - 1](a) = P(a')\, a_{n+1} - 1 = -1 \neq 0$. Par le lemme, on en déduit que $J' = k[X_1, ..., X_n, Y]$, c'est-à-dire $1 \in J'$.

On décompose ensuite 1 sur les générateurs $j_1, ..., j_k, PY - 1$ de J' :

$$1 = \sum_{i=1}^{k} \lambda_i(X_1, ..., X_n, Y) \times j_i + \lambda_0(X_1, ..., X_n, Y) \times (PY - 1).$$

On envoie tout ça dans $k(X_1, ..., X_n)$ via le morphisme

$$\left\{ \begin{array}{ccc} k[X_1, ..., X_n, Y] & \longrightarrow & k(X_1, ..., X_n) \\ X_i & \longmapsto & X_i \\ Y & \longrightarrow & \frac{1}{P} \end{array} \right. ,$$

ce qui donne

$$1 = \sum_{i=1}^{k} \lambda_i\left(X_1, ..., X_n, \frac{1}{P}\right) \times j_i + \lambda_0\left(X_1, ..., X_n, \frac{1}{P}\right) \times \left(P\frac{1}{P} - 1\right),$$

c'est-à-dire

$$1 = \sum_{i=1}^{k} \lambda_i\left(X_1, ..., X_n, \frac{1}{P}\right) \times j_i.$$

On multiplie alors par un $P^{N \geq 1}$ pour retomber dans $k[X_1, ..., X_n]$, ce qui donne

$$\begin{array}{rcl} P^N & = & \displaystyle\sum_{i=1}^{k} \Lambda_i(X_1, ..., X_n) \times j_i \\ & \in & J, \end{array}$$

c'est-à-dire $P \in \operatorname{Rad} J$, doù $I(V(J)) \subset \operatorname{Rad} J$ comme voulu.

Réciproquement, soit $P \in \operatorname{Rad} J$. Alors $\exists n \geq 1$ tel que $P^n \in J$, donc $\forall x \in V(J)$, $P^n(x) = 0$, c'est-à-dire $P(x) = 0$, donc $P \in I(V(J))$. On a ainsi $\operatorname{Rad} J \subset I(V(J))$.

5.3 Topologie de Zarinski sur k^n

Proposition.
Les variétés $V(J)$ où J idéal de $k[X_1, ..., X_n]$ sont les fermés d'une topologie de k^n. On a plus précisément :
• $\bigcap V(J_i) = V(\sum J_i)$;
• $V(J_1) \cup V(J_2) = V(J_1 \cap J_2) = V(J_1 J_2)$.

Démontration.
• $x \in \bigcap V(J_i) \iff x$ annulé par les $J_i \iff x$ annulé par $\sum J_i$;
• $J_1 J_2 \subset J_1 \cap J_2 \subset J_i$, donc

$$V(J_i) \subset V(J_1 \cap J_2) \subset V(J_1 J_2),$$

d'où

$$V(J_1) \cup V(J_2) \subset V(J_1 \cap J_2) \subset V(J_1 J_2).$$

Si $x \notin V(J_1) \cup V(J_2)$, $\exists P_i \in J_i$ tel que $P_i(x) \neq 0$ $(\forall i = 1, 2)$, donc $[P_1 P_2](x) = P_1(x) P_2(x) \neq 0$; or $P_1 P_2 \in J_1 J_2$, donc $x \notin V(J_1 J_2)$. Ceci montre l'inclusion inverse.

Cette topologie est assez grossière.

Proposition.
Pour $n = 1$, les fermés sont $\emptyset$, k, et les parties finies de k. Si de plus k est infini, alors la topologie de Zarinski n'est jamais séparée.

Démonstration.
• Soit $V(J)$ un fermé. J est un idéal de $k[X]$ principal, donc $J = (P)$, et $V(J)$ n'est autre que l'ensemble des racines de P, qui est soit k tout entier (si $P = 0$), soit $\emptyset$ (si $\deg P = 0$), soit fini (si $\deg P \geq 1$)
• Soit $a, b \in k$ distincts. Si on peut les séparer par deux ouverts U_a et U_b non vides, alors $U_a \cap U_b = \emptyset$, c'est-à-dire $F_a \cup F_b = k$ où F_a et F_b sont des fermés, mettons $\begin{cases} F_a = V(I_a) \\ F_b = V(I_b) \end{cases}$, avec $\begin{cases} I_a = (A) \\ I_b = (B) \end{cases}$ donc

$$k = V(I_a) \cup V(I_b) = V(I_a \cap I_b) = V((A) \cap (B)) = V(A \vee B),$$

d'où $A \vee B = 0$ car k infini, c'est-à-dire $A = B = 0$, c'est-à-dire $I_a = I_b = \{0\}$, c'est-à-dire $F_a = F_b = k$, ou encore $U_a = U_b = \emptyset$, *absurde* car $\begin{cases} a \in U_a \\ b \in U_b \end{cases}$.

Propriété.
Soit X une variété de k^n. Les fermés de la topologie (de Zarinski) induite sur X sont encore des fermés pour la topologie de Zarinski sur k^n.

Démonstration.
Tout fermé F pour la topologie induite s'écrit $F = X \cap F'$ où F' fermé de la "vraie" topologie sur k^n. Comme X est par définition fermé, $X \cap F'$ est fermé, c'est-à-dire F est fermé.

Définition.
Une variété X est dite irréductible *si elle n'est pas réunion de deux fermés propres de X.*

Propriété.
Soit X une variété. On a équivalence entre :
• *X est irréductible ;*
• *Si X_1 et X_2 sont des variétés,*

$$X = X_1 \cup X_2 \implies X = X_1 \text{ ou } X = X_2 \ ;$$

• *Deux ouverts non vides de X ont une intersection non vide ;*
• *Tout ouvert non vide de k^n est dense dans X.*

Démonstration.

$(i) \implies (ii)$ Les $X_i = X_i \cap X$ sont des fermés de X, donc l'un d'eux n'est pas propre, c'est-à-dire $X_i \cap X = X$ pour un $i = 1$ ou 2, c'est-à-dire $X \subset X_i$; comme de plus $X_i \subset X_1 \cup X_2 = X$, on en déduit l'égalité $X_i = X$.

$(ii) \implies (iii)$ Soit U_1 et U_2 deux ouverts non vide de X. Ils s'écrivent $U_i = X \cap \Omega_i$ où Ω_i est un ouvert non vide de k^n, c'est-à-dire $\Omega_i = {}^cV(J_i)$. Si l'intersection $U_1 \cap U_2$ était vide, on aurait

$$\begin{aligned} X &= X \cap k^n \\ &= X \cap {}^c(U_1 \cap U_2) \\ &= X \cap {}^c[(X \cap \Omega_1) \cap (X \cap \Omega_2)] \\ &= X \cap {}^c[X \cap {}^cV(J_1) \cap {}^cV(J_2)] \\ &= X \cap [{}^cX \cup V(J_1) \cup V(J_2)] \\ &= [X \cap V(J_1)] \cup [X \cap V(J_2)], \end{aligned}$$

d'où (pour un $i = 1$ ou 2)

$$\begin{aligned} & X = X \cap V(J_i) \\ \implies \quad & X \subset V(J_i) \\ \implies \quad & \Omega_i = {}^cV(J_i) \subset {}^cX \\ \implies \quad & U_i = X \cap \Omega_i = \emptyset, \end{aligned}$$

absurde.

$(iii) \implies (iv)$ Soit Ω un ouvert non vide. Soit $x \in X$, et U un ouvert de X contenant x. Alors $\Omega \cap X$ et U sont deux ouvert non vides de X, donc ont une intersection non vide, a fortiori Ω et U également, d'où Ω dense dans X.

$(iv) \implies (i)$ Soit X_1 et X_2 des fermés de X tels que $X = X_1 \cup X_2$. On a alors

$$\begin{aligned} (X \cap {}^cX_1) \cap (X \cap {}^cX_2) &= X \cap ({}^cX_1 \cap {}^cX_2) \\ &= X \cap {}^c(X_1 \cup X_2) \\ &= X \cap {}^cX \\ &= \emptyset, \end{aligned}$$

donc l'un des ouverts (de X) $X \cap {}^cX_i$ est vide, c'est-à-dire $X \subset X_i$. Comme de plus $X_i \subset X_1 \cup X_2 = X$, on en déduit l'égalité $X_i = X$.

Un corollaire immédiat du troisième point est que la topologie induite sur une variété irréductible n'est jamais séparée.

Donnons maintenant un critère sur l'idéal J pour que $V(J)$ soit iiréductible.

Proposition.
Soit X une variété. Alors

$$X \text{ irréductible} \iff I(X) \text{ premier.}$$

Démontration.

On montre la contraposée

• Si $X = X_1 \cup X_2$ où $X_i \subsetneq X$ $(\forall i = 1, 2)$, c'est-à-dire $V(I(X_i)) \subsetneq V(I(X))$, d'où $I(X) \subsetneq I(X_i)$, on peut prendre un $P_i \in I(X_i) \backslash I(X)$, c'est-à-dire $P_i \notin I(X)$ qui annule X_i. Alors P_1P_2 est nul sur $X_1 \cup X_2 = X$, c'est-à-dire $P_1P_2 \in I(X)$, donc $I(X)$ ne peut être premier.

• Supposons $I(X)$ non premier : $\exists P_1, P_2 \in k[X_1, ..., X_n] \backslash I(X)$ tel que $P_1P_2 \in I(X)$. Soit $I_i = \langle I(X), P_i \rangle = I(X) + kP_i$ et $X_i = V(I_i)$. On veut $X = X_1 \cup X_2$. On a déjà $X_1 \cup X_2 \subset X$. De plus, si $x \in X$, $P_1P_2(x) = 0$, alors $P_1(x)$ ou $P_2(x) = 0$, c'est-à-dire $x \in X_1$ ou X_2. Reste à voir que $X_i \subsetneq X$, sinon $X_i = X$ et

$$I(X) = I(X_i) = I(V(X_i)) = \operatorname{Rad} I_i \supset I_i \supsetneq I(X),$$

absurde.

Définition.
Une topologie est dite noethérienne *si toute suite croissante d'ouverts stationne.*

Remarque. Soit T une topologie. On a clairement équivalence entre :
• T est noethérienne ;
• toute suite croissante d'ouverts stationne ;
• toute famille non vide d'ouverts admet un élément maximal ;
• toute suite décroissante de fermés stationne ;
• toute famille non vide de fermés admet un élément minimal.

Proposition.
La topologie de Zariski sur k^n est noethérienne.

Démontration.
Soit $(X_\omega)_{\omega\in\Omega}$ une famille non vide de fermés. La famille $(I(X_\omega))_{\omega\in\Omega}$ d'idéaux de $k[X_1,...,X_n]$ (qui est noethérien) est non vide, donc admet un élément maximal $I(X_{\omega_0})$. Alors $\forall\omega\in\Omega$, on a $I(X_\omega)\subset I(X_{\omega_0})$, d'où $V(I(X_{\omega_0}))\subset V(I(X_\omega))$, c'est-à-dire $X_{\omega_0}\subset X_\omega$, donc X_{ω_0} est un élément minimal de $(X_\omega)_{\omega\in\Omega}$.

Proposition.
Toute variété X se décompose en réunion finie de variétés irréductibles, c'est-à-dire

$$X = X_1 \cup ... \cup X_n$$

où les X_i sont irréductibles.
On peut de plus supposer que pour $i\neq j$, $X_i\not\subseteq X_j$. Alors les X_k sont uniques (à permutation près). On les appelle les composantes irréductibles *de X.*

Démontration.
Soit $\mathcal{S}$ l'ensemble des variétés ne possédant pas la propriété. Si $\mathcal{S}\neq\emptyset$, par noethérianité, il existe un élément minimal X. X n'est pas irréductible (car $\in\mathcal{S}$), donc $X=X_1\cup X_2$ avec $X_i\subsetneq X$. Par minimalité, $X_i\notin S$, donc se décomposent, et leur décomposition donne une décompostion de X, d'où $X\notin\mathcal{S}$, *absurde*. Donc $\mathcal{S}=\emptyset$.
Pour l'uncité, supposons $X=X_1\cup...\cup X_r=Y_1\cup...\cup Y_s$. On a $Y_i\subset X$, donc

$$\begin{aligned} Y_i &= Y_i\cap X \\ &= Y_i\cap\left(\bigcup_{j=1}^{r} X_j\right) \\ &= \bigcup_{j=1}^{r}(Y_i\cap X_j) \end{aligned}$$

qui est une décomposition en fermés de Y_i (qui est irréductible), donc $\exists j$ tel que $Y_i=Y_i\cap X_j$, c'est-à-dire $Y_i\subset X_j$. On fabrique ainsi une application

$$\sigma : \{1,...,s\}\longrightarrow\{1,...,r\}$$

telle que $Y_i\subset X_{\sigma(i)}$. De même, on a

$$\tau : \{1,...,r\}\longrightarrow\{1,...,s\}$$

telle que $X_i\subset Y_{\tau(i)}$. Ainsi, $Y_i\subset X_{\sigma(i)}\subset Y_{\tau\sigma(i)}$, et l'hypothèse $X_i\not\subseteq X_j$ pour $i\neq j$ donne $Y_i=Y_{\sigma\tau(i)}$ pour tout i, d'où σ inversible.

Corollaire.
Un idéal radical est une intersection finie d'idéaux premiers.

Démontration.

Soit J un idéal radical. On décompose $V(J) = V(I_1) \cup ... \cup V(I_k) = V(I_1 \cap ... \cap I_k)$ en composantes irréductibles, où les I_i sont donc premiers. On a alors successivement :

$$\begin{aligned} I(V(J)) &= I(V(I_1 \cap ... \cap I_k)) \\ \operatorname{Rad} J &= \operatorname{Rad}(I_1 \cap ... \cap I_k) \\ J &= I_1 \cap ... \cap I_k \end{aligned}$$

car une intersection finie d'idéaux premiers (donc radicaux) est un idéal radical.

Exemple : hyersurface de k^n.

On appelle hypersurface *de k^n une variété définie par un idéal momogène de $k[X_1, ..., X_n]$.*

Soit $P \in k[X_1, ..., X_n]$ (anneau factoriel, rappelons-le), que l'on décompose en $P = P_1^{n_1} ... P_r^{n_r}$ où P_i est irréductible – et donc l'idéal (P_i) est premier. Notons par abus $V(P)$ pour $V((P))$. On a alors

$$\begin{aligned} & x \in V(P) \\ \iff \quad & P_1^{n_1} ... P_r^{n_r}(x) = 0 \\ \iff \quad & \exists i \text{ tel que } P_i(x) = 0 \\ \iff \quad & \exists i \text{ tel que } x \in V(P_i) \\ \iff \quad & x \in V(P_1) \cup ... \cup V(P_r), \end{aligned}$$

d'où

$$V(P) = V(P_1) \cup ... \cup V(P_r),$$

et c'est la décomposition en composantes irréductibles. En effet, d'une part les (P_i) sont premiers, donc les $V(P_i)$ sont irréductibles, d'autre part

$$\begin{aligned} & V(P_i) \subset V(P_j) \\ \Longrightarrow \quad & I(V(P_j)) = I(V(P_i)) \\ \Longrightarrow \quad & \operatorname{Rad}(P_j) = \operatorname{Rad}(P_i) \\ \Longrightarrow \quad & P_j \in \operatorname{Rad}(P_i) \\ \Longrightarrow \quad & \exists n \geq 1 \text{ tel que } P_j^n \in (P_i) \\ \Longrightarrow \quad & \exists n \geq 1 \text{ tel que } P_i \mid P_j^n \\ \Longrightarrow \quad & i = j \end{aligned}$$

car les P_i sont irréductibles.

Bilan du dictionnaire.

idéaux quelconques	variétés quelconques : parties X de k^n telles que $X = V(I(X))$
idéaux radicaux	variétés $X = V(J)$ telles que $I(V(J)) = J$
idéaux premiers	variétés irréductibles

Si k est algébriquement clos, on peut aussi regarder le cas des idéaux maximaux $\mathfrak{M}$:

$$\begin{aligned} V(\mathfrak{M}) &= V((X_1 - a_1, ..., X_n - a_n)) \\ &= \{(a_1, .., a_n)\}, \end{aligned}$$

donc aux idéaux maximaux correspondent les variétés "singletons".

En raffinant encore (sans grand intérêt, d'ailleurs...), on peut regarder le cas où l'idéal est l'espace tout entier, auquel cas

$$V(k[X_1, ..., X_n]) = \emptyset;$$

En effet, tout élément a de $V(k[X_1, ..., X_n])$ doit être annulé par $(X_1 - a_1) ... (X_n - a_n) + 1$, donc ne peut exister.

On peut donc prolonger le bas du dictionnaire si k est algébriquement clos :

idéaux quelconques	variétés quelconques : parties X de k^n telles que $X = V(I(X))$
idéaux radicaux	variétés $X = V(J)$ telles que $I(V(J)) = J$
idéaux premiers	variétés irréductibles
idéaux maximaux	variétés singletons
idéal maximum	variété vide

Remarque. Soit J un idéal de $k[X_1, ..., X_n]$. On a vu que $V(J)$ paramétrise les idéaux maximaux de ${}^{k[X_1,...,X_n]}\!/_J$ (on dit aussi le *spectre maximal* de ${}^{k[X_1,...,X_n]}\!/_J$) via

$$(a_1, ..., a_n) \longmapsto (X_1 - a_1, ..., X_n - a_n).$$

On peut ainsi reconstruire une variété X en étudiant le spectre maximal de ${}^{k[X_1,...,X_n]}\!/_{I(X)}$ puis en utilisant la correspondance ci-dessus pour avoir en retour les points de $V(I(X)) = X$.

Ce qui nous amène à l'étude des quotients ${}^{k[X_1,...,X_n]}\!/_{I(X)}$

5.4 Fonctions polynomiales.

Soit X une variété de k^n.

Définition.
On appelle fonction polynomiale *sur V la restriction d'une fonction polynomiale sur k^n.*
On dira que $f : V \longrightarrow W$ est polynomiale *si chacune des applications coordonnées l'est.*

Proposition.
L'algèbre des fonctions polynomiale sur une variété V peut se voir comme le quotient

$$k[V] := {}^{k[X_1,...,X_n]}\!/_{I(V)}.$$

Démonstration.
Soit f polynomiale sur V. On a donc $f = P_{/V}$ où P polynôme de $k[X_1, ..., X_n]$. Si Q est un autre tel polynôme, alors

$$0 = f - f = P_{/V} - Q_{/V} = (P - Q)_{/V},$$

c'est-à-dire $P - Q \in I(V)$.

Si $f : V \longrightarrow W$ est polynomiale (où $V \subset k^n$ et $W \subset k^m$ sont des variétés), elle détermine un morphisme d'algèbres

$$f^* : \begin{cases} k[W] & \longrightarrow & k[V] \\ \overline{P} & \longmapsto & \widetilde{P \circ f} \end{cases}$$

(où les barres et les tildes représentent les classes des polynômes modulo ce qu'il faut).

Réciproquement, on montre que tout tel morphisme d'algèbres provient d'une telle application polynomiale.

Proposition.
Soit $\varphi : k[W] \longrightarrow k[V]$ un morphisme d'algèbres. Il existe $f : V \longrightarrow W$ polynomiale telle que $\varphi = f^*$.

Démontration.
Soit $\varphi : k[W] \longrightarrow k[V]$ morphisme d'algèbre. En notant $k[W] = {}^{k[Y_1,...,Y_m]}\!/_{I(W)}$ et $\widetilde{Y_i}$ la classe de Y_i modulo $I(W)$, remarquons que $k[W]$ est engendrée par les $\widetilde{Y_i}$. Posons

$$f_i = \varphi\left(\widetilde{Y_i}\right).$$

$f_i \in k[V]$, donc s'écrit

$$f_i = \overline{P_i}$$

où P_i polynôme de $k[X_1, ..., X_n]$ et $\overline{P_i}$ sa classe modulo $I(V)$. On pose ensuite

$$f = (P_1, ..., P_m)$$

polynomiale sur V à valeurs dans k^m.

On aimerait que f soit à valeurs dans W, car on pourrait alors définir f^* sur $k[W]$ et on aurait

$$f^*\left(\widetilde{Y_i}\right) = \overline{Y_i \circ f} = \overline{P_i} = f_i = \varphi\left(\widetilde{Y_i}\right),$$

donc φ et f^* coïncideraient sur des générateurs de $k[W]$, donc seraient égales comme souhaité.

Soit $x \in V$; on veut : $f(x) \in W = V(I(W))$. Soit donc $Q \in I(W)$; on veut $Q(f(x)) = 0$. On regarde

$$Q(f(x)) = Q(P_1(x), ..., P_m(x)) = [Q(P_1, ..., P_m)](x).$$

Puisque $x \in V$, pour tout polynôme A de congru à $Q(P_1, ..., P_m)$ modulo $I(V)$, on a $[Q(P_1, ..., P_m)](x)$ vaut $A(x)$. On calcule donc le résidu de $Q(P_1, ..., P_m)$ modulo $I(V)$:

$$\begin{aligned}
\overline{Q(P_1, ..., P_m)} &= Q\left(\overline{P_1}, ..., \overline{P_m}\right) = Q\left(\varphi\left(\widetilde{Y_1}\right), ..., \varphi\left(\widetilde{Y_m}\right)\right) \\
&= \varphi\left(Q\left(\widetilde{Y_1}, ..., \widetilde{Y_m}\right)\right) = \varphi\left(\widetilde{Q}\right) = \varphi\left(\widetilde{0}\right) \\
&= \overline{0}.
\end{aligned}$$

On a donc $Q(f(x)) = 0$, et ce $\forall Q \in I(W)$, d'où $f(x) \in V(I(W)) = W$, *CQFD.*