Algèbre commutative et géométrie algébrique

Pierron Théo

ENS Ker Lann

Table des matières

1 Futilités d'usage **1**

2 Anneaux nœthériens **3**
2.1 Résultats généraux 3
2.2 Théorème de la base de Hilbert 4
2.3 Ensembles algébriques 5
2.4 Idéal associé à un ensemble algébrique 7

3 Résultant et bases de Gröbner **9**
3.1 Résultant 9
3.2 Base de Gröbner 12
3.3 Base de Gröbner réduite 18
3.4 Application 19
3.4.1 Élimination 19
3.4.2 Théorème d'extension 20
3.5 Théorèmes des zéros de Hilbert 20

4 Dimension **27**
4.1 Localisation 27
4.2 Idéaux 28
4.3 Lemme de Nakayama 30
4.4 Extension entière 31
4.5 Dimension d'un ensemble algébrique 36
4.6 Fonction de Hilbert 37

5 Introduction au langage des schémas **41**
5.1 Spectre d'un anneau 41
5.2 Faisceaux 42
5.3 Schémas 45

Chapitre 1

Futilités d'usage

On considère des anneaux commutatifs unitaires non nuls.

Proposition 1.1 Soit ϕ un morphisme.
L'image réciproque d'un idéal est un idéal.
Si ϕ est surjective, l'image directe d'un idéal est un idéal.

Définition 1.1 On définit la somme des $(I_i)_{i\in S}$ comme étant l'ensemble des $\sum_{i\in S} x_i$ où chaque $x_i \in I_i$ et $x_i = 0$ pour presque tout i. On a

$$\sum_{i=1}^{n} \langle x_i \rangle = \langle x_1, \ldots, x_n \rangle$$

Définition 1.2 On définit le produit de deux idéaux I et J comme l'ensemble des sommes finies de xy où $x \in I$ et $y \in J$. On étend cette définition à n idéaux par récurrence.

Proposition 1.2 Le produit est inclus dans l'intersection.

Remarque 1.1 Quand A est intègre alors l'intersection d'idéaux non nuls est non nulle.

Définition 1.3 On définit le conducteur de J dans I par $(I : J) = \{x \in A, xJ \subset I\}$.
Pour $I = (0)$, on obtient l'idéal annulateur de J.

Théorème 1.1 Krull *Tout idéal propre est inclus dans un idéal maximal.*

Corollaire 1.1 *Un élément est inversible ssi il n'appartient à aucun idéal maximal.*

Proposition 1.3 Soit $\mathfrak{p}$ un idéal premier inclus dans A et I, J deux idéaux de A.
Si $I \cap J \subset \mathfrak{p}$ alors $I \subset \mathfrak{p}$ ou $J \subset \mathfrak{p}$.
Si $IJ \subset \mathfrak{p}$ alors $I \subset \mathfrak{p}$ ou $J \subset \mathfrak{p}$.

Démonstration. Il suffit de montrer le deuxième point. Par l'absurde, si $I \not\subset \mathfrak{p}$ et $J \not\subset \mathfrak{p}$ alors il existe $a \in I$ et $b \in J$ tel que $a \notin \mathfrak{p}$ et $b \notin p$. Alors $ab \in IJ \subset \mathfrak{p}$ donc $a \in \mathfrak{p}$ ou $b \in p$ contradiction. ■

Par récurrence, on étend ce résultat à n idéaux.

Proposition 1.4 Soit $I \in A$ et $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ premiers. Si $I \subset \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$ alors il existe k tel que $I \subset \mathfrak{p}_k$.

Démonstration. Cas $n = 2$: Si $I \not\subset \mathfrak{p}_1$ et $I \not\subset \mathfrak{p}_2$ alors il existe $x, y \in I$ tel que $x \notin \mathfrak{p}_1$ donc $x \in \mathfrak{p}_2$ et $y \in \mathfrak{p}_2$ donc $y \in \mathfrak{p}_1$.

Alors $x + y \in I \subset \mathfrak{p}_1 \cup \mathfrak{p}_2$. Mais $x + y \notin \mathfrak{p}_1$ car $c \notin \mathfrak{p}_1$ et $y \in \mathfrak{p}_1$ et idem pour $\mathfrak{p}_2$. Donc contradiction.

Si $n > 2$, posons $J_i = \bigcup_{j \neq i} \beta_j$ la réunion de $n - 1$ idéaux premiers. On suppose que $I \not\subset \mathfrak{p}_i$ pour tout i.

Par récurrence, $I \not\subset J_i$ on peut alors choisir $a_i \in I$ tel que $a_i \notin J_i$ ie $a_i \in \mathfrak{p}_i$.

On regarde $a := a_1 \ldots a_{n-1} + a_n \in I \subset \bigcup_{i=1}^{n} \mathfrak{p}_1$. Or $a \notin \mathfrak{p}_i$ pour $i < n$ car $a_1 \ldots a_{n-1} \in \mathfrak{p}_i$ mais $a_n \notin \mathfrak{p}_i$ et $a \notin \mathfrak{p}_n$ car $a_n \in \mathfrak{p}_n$ mais pas $a_1 \ldots a_{n-1}$. Contradiction ■

Proposition 1.5 Soit A un anneau et $I \subset A$ un idéal. On définit

$$\sqrt{I} = \{a \in A, \exists n > 0, a^n \in I\} \supset I$$

qui est un idéal.

Définition 1.4 On dit que I est radical ssi $I = \sqrt{I}$. Un idéal premier est radical.

Définition 1.5 $\sqrt{(0)}$ s'appelle le nilradical de A et on le note $\mathrm{Nil}(A)$.

THÉORÈME 1.2 $\mathrm{Nil}(A)$ *est l'intersecton des idéaux premiers de* A.

COROLLAIRE 1.2 *Si* $I \subset A$ *est un idéal alors* $\sqrt{I}$ *est égal à l'intersection des idéaux premiers contenant* I.

Définition 1.6 On appelle radical de Jacobson de A et on note $R(A)$ l'intersection des idéaux maximaux de A. Il contient $\mathrm{Nil}(A)$.

Proposition 1.6 $R(A) = \{a \in A, \forall b, 1 - ab \in A^*\}$.

Chapitre 2

Anneaux nœthériens

2.1 Résultats généraux

Proposition 2.1 Soit A un anneau. Les trois conditions suivantes sont équivalents

(i) Toute suite croissante d'idéaux est stationnaire

(ii) Toute famille non vide d'idéaux admet un élément maximal

(iii) Tous les idéaux de A sont de type fini

Démonstration.

(i) $\Rightarrow$ (ii) Par l'absurde, on aurait une suite $I_0 \subsetneq I_1 \subsetneq \ldots$, ce qui contredit (i).

(ii) $\Rightarrow$ (iii) Soit $I \subset A$ idéal. $\{J \subset I, J \text{ de type fini}\}$ est non vide car il contient (0) donc il admet un élément maximal I'. Si $I' \neq I$ alors il existe $x \in I \setminus I'$ donc $I' \subsetneq I' + \langle x \rangle \subset I$, ce qui contredit la maximalité de I'.

(iii) $\Rightarrow$ (ii) Soit $I_0 \subset I_1 \subset \ldots \subset I_n$. On pose $I = \bigcup_{i \geqslant 0} I_i$ (idéal de A). Il est donc de type fini engendré par $x_1, \ldots, x_k$. Mais il existe $n > 0$ tel que $x_1, \ldots, x_k \in I_n$ donc $I = I_n$ et $I_m = I_n$ pour tout $m > n$. ∎

Exemple 2.1

- Un corps est nœthérien.
- $\mathbb{Z}$ est nœthérien (car principal) : si

$$n_0\mathbb{Z} \subset n_1\mathbb{Z} \subset \ldots$$

alors $n_i \mid n_{i-1}$ donc $|n_0| \geqslant \ldots \geqslant |n_i| \geqslant \ldots$.

- $k[X_1, \ldots, X_n]$ est nœthérien.

- $k[X_n, n \geqslant 1]$ n'est pas nœthérien.

Proposition 2.2 Si A est nœthérien, A/I est nœthérien pour tout I.

Démonstration. Soit $\overline{J} \subset A/I$ un idéal. A est nœthérien donc J est de type fini et $\overline{J}$ aussi. ∎

Proposition 2.3 Si A est nœthérien, tout idéal de A contient une puissance de son radical.

Démonstration. $\sqrt{I}$ est de type fini engendré par $x_1, \ldots, x_r$. Pour tout i, il existe n_i tel que $x_i^{n_i} \in I$.

Soit $n = \max n_i$. Si $x \in \sqrt{I}$, $x = \sum_{i=1}^{r} a_i x_i$ et on a

$$x^{rn} = \sum_{i_1+\ldots+i_r=rn} \alpha_{i_1,\ldots,i_r} x_1^{i_1} \ldots x_r^{i_r} \in I$$

puisqu'au moins un i_j est supérieur à n. ∎

Proposition 2.4 Tout idéal de A contient un produit fini d'idéaux premiers.

Démonstration. Soit $\Sigma = \{I \subset A,\ I$ ne contient aucun produit fini d'idéaux premiers$\}$. Supposons $\Sigma \neq \varnothing$.

Σ admet alors un élément maximal noté I. I n'est pas premier donc il existe $x_1, x_2 \notin I$ tel que $x_1 x_2 \in I$.

Or $I \subsetneq I + \langle x_i \rangle =: I_i$ donc $I_i \notin \Sigma$. Ainsi, $I_1 \supset \mathfrak{p}_1 \ldots \mathfrak{p}_r$ et $I_2 \supset \mathfrak{p}'_1 \ldots \mathfrak{p}'_s$.

On remarque que $I_1 I_2 \subset I$ puisque $x_1 x_2 \in I$ donc $\mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{p}'_1 \ldots \mathfrak{p}'_s \subset I$. Contradiction. ∎

2.2 Théorème de la base de Hilbert

Définition 2.1 Une A-algèbre est un anneau B avec un morphisme d'anneaux $A \to B$. On dit que B est de type fini ssi B est engendrée sur A par un nombre fini d'éléments $b_1, \ldots, b_r$.

Proposition 2.5 B est de type fini ssi B est le quotient de $A[X_1, \ldots, X_r]$ pour un certain r.

THÉORÈME 2.1 DE LA BASE DE HILBERT *Si A est nœthérien alors l'anneau de polynômes $A[X_1, \ldots, X_n]$ est nœthérien.*

COROLLAIRE 2.1 *Toute A-algèbre de type finie est nœthérien.*

Démonstration. Par récurrence, on montre seulement que $A[X]$ est nœthérien. Soit I un idéal de $A[X]$.

Lemme 2.1.1
Soit I un idéal de $A[X]$. Si $k \geqslant 0$, on note $L_k(I)$ l'ensemble des coefficients dominants des polynômes de I de degré k auquel on adjoint 0.

C'est un idéal de A et $L_k(I) \subset L_{k+1}(I)$. De plus, si $I' \subset A[X]$ est un idéal vérifiant $I \subset I'$ et $L_k(I) = L_k(I')$ pour tout k alors $I = I'$.

Démonstration.

- Si $a_k, a'_k \in L_k(I)$ et $a \in A$, on a P et Q de coefficients dominants a_k et a'_k.
  Alors $P + Q$ (resp. aP) est de degré k de coefficient dominant $a_k + a'_k$ (resp. aa_k).
  En considérant XP, on a clairement $L_k \subset L_{k+1}$.
- Il suffit de montrer $I' \subset I$. Soit $g = \sum_{i=0}^{r} a_i X^i \in I'$. $a_r \in L_r(I') = L_r(I)$ donc il existe $f_r \in I$ tel que a_r soit le coefficient dominant de f_r.
  $g - f_r$ est de degré inférieur à $r - 1$ donc on réitère et on obtient $g = f_0 + \ldots + f_r \in I$. ∎

Soit $I_0 \subset I_1 \subset \ldots \subset I_n \subset \ldots$ des idéaux de $A[X]$.

$\Sigma := \{L_i(I_j), i, j \in \mathbb{N}^2\}$ sont des idéaux dans A. Pour i fixé, $L_i(I_j)$ est croissante et idem pour j fixé.

Il suffit de montrer qu'il existe $k \geqslant 0$ tel que pour tout $j \geqslant k$, $L_i(I_j) = L_i(I_k)$ pour tout i.

Comme A est nœthérien, il existe $L_p(I_q)$ élément maximal de Σ. Pour chaque $0 \leqslant i \leqslant p-1$, la suite croissante $(L_i(I_j))_j$ est stationnaire donc il existe p_i tel que pour tout $j \geqslant p_i$, $L_i(I_j) = L_i(I_{p_i})$.

Soit $k = \max\{p_i, i \in [\![0, p-1]\!], \forall p\}$. Ce k vérifie bien $L_i(I_j) = L_i(I_k)$ pour tout i. ∎

2.3 Ensembles algébriques

On fixe un corps k infini. On note $\mathbb{A}_k^n = k^n$.

Définition 2.2 Un ensemble algébrique de $\mathbb{A}_k^n$ est un sous-ensemble de $\mathbb{A}_k^n$ de la forme

$$\nu(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n, \forall f \in S, f(a_1, \ldots, a_n) = 0 \forall f \in S\}$$

où $S \subset k[X_1, \ldots, X_n]$.

Remarque 2.1 Souvent, on va supposer k algébriquement clos.

Lemme 2.1.2
Soit S, S' deux parties de $k[X_1, \ldots, X_n]$.

(i) $S \mapsto \nu(S)$ est décroissante

(ii) $\nu(S) = \nu(\langle S \rangle)$

(iii) $\nu(I) = \nu(\sqrt{I})$.

Démonstration.

(i) Clair

(ii) $\supset$ est claire. Pour $\subset$, on prend $(a_1, \ldots, a_n) \in \nu(S)$ tel que pour tout $f \in S$, $f(a_1, \ldots, a_n) = 0$.
Soit $g \in \langle S \rangle$ qui s'écrit $\sum_{i=1}^{r} g_i f_i$ où $f_i \in S$ et $g_i \in k[X_1, \ldots, X_n]$.
Il est alors clair que $g(a_1, \ldots, a_n) = 0$.

(iii) $\supset$ est aussi claire. Pour $\subset$, on prend $(a_1, \ldots, a_n) \in \nu(I)$ tel que pour tout $f \in I$, $f(a_1, \ldots, a_n) = 0$.
Soit $g \in \sqrt{I}$. On a $g^k \in I$ et $g^k(a_1, \ldots, a_n) = (g(a_1, \ldots, a_n))^k = 0$ donc $g(a_1, \ldots, a_n) = 0$ donc $(a_1, \ldots, a_n) \in \nu(\sqrt{I})$. ∎

Proposition 2.6

(i) L'ensemble $\varnothing$ et $\mathbb{A}_k^n$ sont des ensembles algébriques.

(ii) Une intersection quelconque d'ensembles algébriques est algébrique.

(iii) Une réunion finie d'ensembles algébriques est algébrique.

Démonstration.

(i) $\nu(\{1\}) = \varnothing$, $\nu(\{0\}) = \mathbb{A}_k^n$.

(ii) Soit $V_i = \nu(S_i)$. En écrivant, on obtient $\cap_i V_i = \nu(\cup_i S_i)$.

(iii) Soit $V = \nu(I)$ et $V' = \nu(J)$ avec I, J deux idéaux.
On a $\nu(I) \cup \nu(J) \subset \nu(IJ)$ clairement. Soit $(a_1, \ldots, a_n) \in \nu(IJ)$.
On suppose que $(a_1, \ldots, a_n) \notin \nu(I)$ et $(a_1, \ldots, a_n) \notin \nu(J)$. Il existe donc $f \in I$ et $g \in J$ tel que $f(a_i) \neq 0$ et $g(a_i) \neq 0$.
Alors $(fg)(a_i) \neq 0$ mais $fg \in IJ$. Contradiction. ∎

Remarque 2.2 Les ensembles algébriques sont les fermés d'une topologie appelée topologie de Zariski.

Remarque 2.3

$$\nu(I) \cup \nu(J) = \nu(IJ) = \nu(\sqrt{IJ}) = \nu(\sqrt{I \cap J}) = \nu(I \cap J)$$

Corollaire 2.2 du théorème de la base de Hilbert *Tout ensemble algébrique est défini par un nombre fini de polynômes.*

2.4 Idéal associé à un ensemble algébrique

Définition 2.3 Soit V une partie de $\mathbb{A}_k^n$, on définit

$$\mathcal{I}(V) = \{f \in k[X_1, \ldots, X_n], \forall a_1, \ldots, a_n \in V, f(a_1, \ldots, a_n) = 0\}$$

Lemme 2.1.3
C'est un idéal radical de $k[X_1, \ldots, X_n]$.

Démonstration. Trivialement un idéal.

Si $f^k \in \mathcal{I}(V)$, $f^k(a_1, \ldots, a_n) = 0$ pour tout $(a_1, \ldots, a_n) \in V$ donc $f \in \mathcal{I}(V)$. ∎

Proposition 2.7 Soient $V, V' \subset \mathbb{A}_k^n$.

(i) Si $V \subset V'$ alors $\mathcal{I}(V') \subset \mathcal{I}(V)$.

(ii) $\mathcal{I}(V \cup V') = \mathcal{I}(V) \cap \mathcal{I}(V')$

(iii) $\forall I \subset k[X_1, \ldots, X_n]$ idéal, $I \subset \mathcal{I}(\nu(I))$

(iv) Supposons V algébrique, on a $V = \nu(I(V))$.

Remarque 2.4 Pour une partie V de $\mathbb{A}_k^n$, $V \subset \nu(\mathcal{I}(V))$ et c'est le plus petit ensemble algébrique contenant V. On l'appelle clôture algébrique de V pour la topologie de Zariski.

Remarque 2.5 ν induit une application entre les idéaux de $k[X_1, \ldots, X_n]$ et les ensembles algébriques de $\mathbb{A}_k^n$. L'image de $\mathcal{I}$ est incluse dans l'ensemble des idéaux radicaux. On va en fait montrer que $\sqrt{I} = \mathcal{I}(\nu(I))$.

On a en fait une bijection entre les idéaux radicaux de $k[X_1, \ldots, X_n]$ et les ensembles algébriques de $\mathbb{A}_k^n$.

Chapitre 3

Résultant et bases de Gröbner

3.1 Résultant

Définition 3.1 Soit $f = \sum_{i=0}^{n} a_i X^i$ et $g = \sum_{i=0}^{m} b_i X^i$. Le résultant est

$$\mathrm{Res}_{n,m}(f,g) = \begin{vmatrix} a_n & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & a_n & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & a_n & \cdots & a_0 \\ b_m & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_0 & \ddots & \vdots \\ \vdots & \ddots & b_m & \cdots & b_0 & 0 \\ 0 & \cdots & 0 & b_m & \cdots & b_0 \end{vmatrix}$$

Cette matrice (de taille $(n+m) \times (n+m)$ est appelée matrice de Sylvester.

Ses lignes sont les coefficients de $X^{m-1}f, \ldots, f$ puis ceux de $X^{n-1}g, \ldots, g$.

Remarque 3.1 Si on note $A_p[X]$ le A-module libre des polynômes de degré inférieur à p qui est de rang $p+1$ sur A, on a une application A-linéaire

$$S : \begin{cases} A_{m-1}[X] \times A_{n-1}[X] & \to & A_{n+m-1}[X] \\ (U,V) & \mapsto & Uf + Vg \end{cases}$$

La matrice de Sylvester est en fait la matrice de S dans les bases canoniques $\{(X^i,0), i<n\} \cup \{(0,X^j), j<m\}$ et $\{X^i, i<n+m\}$.

Lemme 3.0.4

(i) Si $a_n = b_m = 0$ alors $\mathrm{Res}_{n,m}(f,g) = 0$.

(ii) Si $b_m = 0$ alors $\mathrm{Res}_{n,m}(f,g) = a_n \mathrm{Res}_{n,m-1}(f,g)$.

(iii) $\mathrm{Res}_{n,m}(f,g) = (-1)^{mn} \mathrm{Res}_{m,n}(g,f)$.

(iv) $\mathrm{Res}_{n,0}(f,b_0) = b_0^n$.

Proposition 3.1 Soit f, g deux polynômes de degré n et m. Alors il existe $U, V \in A[X]$ tel que $\deg(U) < m$, $\deg(V) < n$ et $\mathrm{Res}_{n,m}(f,g) = Uf + Vg$.

COROLLAIRE 3.1 $\mathrm{Res}_{n,m}(f,g) \in A \cap \langle f, g \rangle$.

Démonstration. On remplace C_{n+m} par $\sum_{i=0}^{n+m} X^{n+m-i} C_i$.

La dernière colonne devient alors $(X^{m-1}f, \ldots, f, X^{n-1}g, \ldots, g)^T$. Le déterminant est donc bien de la forme $Uf + Vg$. ∎

THÉORÈME 3.1 *Si A est un corps, $\mathrm{Res}_{n,m}(f,g) = 0$ ssi $a_n = b_m = 0$ ou f et g ont un facteur non trivial dans $A[X]$.*

Démonstration. S est une application linéaire entre deux espaces vectoriels de dimension $n + m$.

Si S n'est pas injective, il existe $(U, V) \neq 0$ tel que $Uf + Vg = 0$. Si de plus f et g sont premiers entre eux, on a $f \mid V$ et $g \mid U$. Alors $\deg(f) < n$ et $\deg(g) < m$ donc $a_n = b_m = 0$.

Réciproquement, si $a_n = b_m = 0$, le lemme précédent assure que le résultant de f et g est nul. Sinon, si f et g ne sont pas premiers entre eux, il existe $d \in k[X]$ de degré strictement positif qui divise f et g.

On a alors $\mathrm{Res}_{n,m}(f,g) \in A \cap \langle d \rangle = \{0\}$ puisque A est un corps. D'où le résultat. ∎

Proposition 3.2 Soit k un corps, $\overline{k}$ sa clôture algébrique. Soit f, g deux polynômes de $A[X]$ où $A = k[Y]$.

$$f = \sum_{i=0}^{n} f_i(Y) X^i \text{ et } g = \sum_{i=0}^{m} g_i(Y) X^i$$

Alors $y \in \overline{k}$ est racine de $\mathrm{Res}_{n,m}(f,g) \in k[Y]$ ssi $f_n(y) = g_m(y) = 0$ ou $f(X,y)$ et $g(X,y)$ ont une racine commune dans $\overline{k}$.

Soient $f, g \in \overline{k}[X,Y]$. On chercher $(x,y) \in \overline{k}$ qui annulle f et g. Si on a une telle solution, alors $f(X,y)$ et $g(X,y)$ ont une racine commune $x \in \overline{k}$.

Par la proposition, $\mathrm{Res}_{n,m}(f,g)(y) = 0$. Pour trouver x, y, on peut donc :

- Calculer $\mathrm{Res}_{n,m}(f,g) \in k[Y]$
- Résoudre $\mathrm{Res}_{n,m}(f,g) = 0$, ce qui donne les valeurs possibles de y.
- Déterminer les x associés.

Proposition 3.3 Soit A un corps, $f, g_1, g_2 \in A[X]$ de degrés inférieurs à n, m_1 et m_2. Alors

$$\mathrm{Res}_{n,m_1+m_2}(f, g_1g_2) = \mathrm{Res}_{n,m_1}(f, g_1)\,\mathrm{Res}_{n,m_2}(f, g_2)$$

Définition 3.2 En passant à $\mathrm{Res}_{n-1,m_1+m_2}$ ou $\mathrm{Res}_{n,m_1+m_2-1}$, on peut supposer que $\deg(f) = n$ et $\deg g_i = m_i$.

Considérons la A-algèbre $A[X]/(f)$ de dimension n sur A. Si g est de degré m, soit

$$\psi_g : \begin{cases} A[X]/f & \to & A[X]/f \\ X^i & \mapsto & X^i g \mod f \end{cases}$$

qui est linéaire. Les lignes de la matrice de ψ_g dans la base $\{X^{n-1}, \dots, 1\}$ seront les coefficients des r_i, restes de $X^i g$ par f. ($r_i = X^i g - U f_i$). On peut donc mettre le résultant sous la forme

$$\mathrm{Res}_{n,m}(f, g) = \begin{vmatrix} a_n & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & a_n & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & a_n & \cdots & a_0 \\ 0 & \cdots & 0 & & & \\ \vdots & & \vdots & & \psi_g & \\ 0 & \cdots & 0 & & & \end{vmatrix} = a_n^m \det \psi_g$$

Remarque 3.2 $\psi_{g_1g_2} = \psi_{g_1} \circ \psi_{g_2}$. *On en déduit la multiplicativité du résultant en sa deuxième variable.*

Proposition 3.4 Soit $f, g \in k[X]$. On écrit dans $\overline{k}[X]$:

$$f = a_n \prod_{i=1}^{n} (X - \alpha_i) \text{ et } g = b_m \prod_{j=1}^{m} (X - \beta_j)$$

Alors

$$\mathrm{Res}_{n,m}(f, g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i)$$

Remarque 3.3 *En fait on peut écrire* $\mathrm{Res}_{n,m}(f, g) = (-1)^{qqch}\,\mathrm{Res}(g, r)$ *où* r *est le reste de* f *divisé par* g. *On calcule donc un résultant avec l'algorithme d'Euclide.*

Définition 3.3 Discriminant Soit $f = \sum_{i=0}^{n} a_i X^i \in k[X]$, $a_n \neq 0$ et $f = a_n \prod_{i=1}^{n}(X - \alpha_i)$ dans $\overline{k}[X]$.

$$\operatorname{disc}(f) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Proposition 3.5 On a

$$\operatorname{disc}(f) = \frac{1}{a_n (-1)^{\frac{n(n-1)}{2}}} \operatorname{Res}_{n,n-1}(f, f')$$

3.2 Base de Gröbner

On définit un degré sur $k[X_1, \ldots, X_n]$ par $\deg(X_1^{\alpha_1} \ldots X_n^{\alpha_n}) = \alpha_1 + \ldots + \alpha_n$.

On dit que X^α apparaît dans f ssi le coefficient $a_\alpha \neq 0$.

Définition 3.4 Une relation d'ordre $\geqslant$ sur $\mathbb{N}^n$ est dite monomiale ssi

(i) $\alpha \geqslant \beta$ implique $\alpha + \nu \geqslant \beta + \nu$ pour tout ν

(ii) L'ordre $\geqslant$ est bon : toute partie non vide a un plus petit élément.

Exemple 3.1

- Sur $\mathbb{N}$ le seul ordre monomial est $\leqslant$.
- Sur $\mathbb{N}^n$, on a l'ordre lexicographique : $\alpha \geqslant_{\text{lex}} \beta$ ssi le premier coefficient non nul de $\alpha - \beta$ est positif.

  On a aussi l'ordre lexicographique gradué : $\alpha \geqslant_{\text{grlex}} \beta$ ssi $|\alpha| := \sum_{i=1}^{n} \alpha_i > |\beta|$ ou ($|\alpha| = |\beta|$ et $\alpha \geqslant_{\text{lex}} \beta$).

  On peut lire les n-uplets à partir de la droite, on obtient l'ordre lexicographique retourné et on peut alors construire l'ordre lexicographique gradué retourné comme précédemment. On le note $\geqslant_{\text{grevlex}}$.

Exemple 3.2 $(3,2,1) \geqslant_{\text{lex}} (2,3,3)$ mais $(3,2,1) \leqslant_{\text{grlex}} (2,3,3)$.

Définition 3.5 Soit $f = \sum_{\alpha} a_\alpha X^\alpha \in k[X_1, \ldots, X_n]$ et $\geqslant$ un ordre monomial.

(i) On appelle multidegré de f par rapport à $\geqslant$ et on note $\text{multideg}(f) = \max\{\alpha, a_\alpha \neq 0\}$.

(ii) Le coefficient dominant de f : $\text{LC}(f) = a_{\text{multideg}(f)}$.

(iii) Le monôme dominant de f : $\text{LM}(f) = X^{\text{multideg}(f)}$.

(iv) Le terme dominant de f : $\text{LT}(f) = \text{LC}(f)\,\text{LM}(f)$.

Exemple 3.3 Pour $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in k[X, Y, Z]$.

- L'ordre lexicographique donne $f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$. Le multidegré est $(3, 0, 0)$. $\mathrm{LT}(f) = -5X^3$, $\mathrm{LC}(f) = -5$ et $\mathrm{LM}(f) = X^3$.
- L'ordre lexicographique gradué donne $f = 7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2$.

Remarque 3.4

- $\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$.
- $\mathrm{multideg}(f + g) \leqslant \max\{\mathrm{multideg}(f), \mathrm{multideg}(g)\}$ *et on a l'égalité si* $\mathrm{LT}(f) + \mathrm{LT}(g) \neq 0$
- X^α *apparaît dans* $f + g$ *implique que* X^α *apparaît dans* f *ou* g.

THÉORÈME 3.2 *Fixons un ordre monômial sur* $\mathbb{N}^n$ *et un ordre sur la famille* $(f_1, \ldots, f_s)$.

Alors f *peut s'écrire sous la forme* $\sum_{i=1}^{s} a_i f_i + r$ *avec* $a_i \in k[X_1, \ldots, X_n]$ *et soit* $r = 0$, *soit* r *est combinaison linéaire de monômes dont aucun n'est divisible par* $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.

De plus, si $a_i f_i \neq 0$, $\mathrm{multideg}(a_i f_i) \leqslant \mathrm{multideg}(f)$.

Démonstration. On considère l'algorithme :

1. Trouver le premier indice $i \in [\![1, s]\!]$ tel que $\mathrm{LT}(f_i) \mid \mathrm{LT}(f)$. Si un tel i n'existe pas, on met $\mathrm{LT}(f)$ dans le reste, on remplace f par $f - \mathrm{LT}(f)$ et on recommence.
2. On met $\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)}$ dans a_i et on recommence avec $f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} f_i$.

À chaque étape, le multidegré de f diminue donc l'algorithme s'arrête en un nombre fini d'étapes. ∎

Exemple 3.4 On prend $f = X^2Y + XY^2 + Y^2$, $f_1 = XY - 1$ et $f_2 = Y^2 - 1$ en considérant l'ordre lexicographique et $f_1 < f_2$.

- X^2Y est divisible par XY. On divise donc d'abord par f_1 et on obtient $XY^2 + X + Y^2$.
- XY^2 est divisible par XY et Y^2 mais comme $f_1 < f_2$, on divise encore par f_1, on obtient $X + Y^2 + Y$.
- X n'est pas divisible par XY et Y^2 donc on considère Y^2.
- Y^2 est divisible par Y^2 donc on divise par f_2 et il reste $X + Y + 1$.

Finalement, $f = (X + Y)f_1 + f_2 + (X + Y + 1)$.

Remarque 3.5 Le résultat dépend de l'ordre monômial et de l'ordre sur $(f_1, \ldots, f_s)$. *Par exemple en échangeant* f_2 *et* f_1, *on trouve*

$$f = (X + 1)f_2 + Xf_1 + (2X + 1)$$

Remarque 3.6 *S'il existe un ordre monômial et un ordre sur $(f_1, \dots, f_n)$ tel que $f = \sum_{i=1}^{n} a_i f_i + 0$ alors $f \in \langle f_1, \dots, f_s \rangle$.*

Mais $f \in \langle f_1, \dots, f_s \rangle$ n'implique pas que pour tout ordre, $r = 0$.

Définition 3.6 Un idéal I de $k[X_1, \dots, X_n]$ est dit monômial s'il est engendré par les monômes, ie si $I = \langle X^\alpha, \alpha \in A \rangle$ où $A \subset \mathbb{N}^n$.

Proposition 3.6 Soit I un idéal monômial.

(i) $X^\beta \in I$ ssi il existe $\alpha \in A$ tel que $X^\alpha \mid X^\beta$

(ii) $f \in I$ ssi tous les termes de f appartiennent à I.

Démonstration.

(i) $X^\beta \in I$ ssi
$$X^\beta = \sum_{\alpha \in A} h_\alpha X^\alpha = \sum_{\alpha' \in \mathbb{N}^n} a_{\alpha'} X^{\alpha'}$$
avec $a_{\alpha'} \in k$ et $X^{\alpha'}$ divisible par X^α pour un certain $\alpha \in A$. Donc $X^\beta \in I$ ssi $X^\beta = X^{\alpha'}$ pour un certain α'.

(ii) On écrit $f = \sum_{\alpha' \in \mathbb{N}^n} a_{\alpha'} X^{\alpha'}$. Un terme de f est de la forme $a_{\alpha'} X^{\alpha'}$ donc dans I. ∎

Corollaire 3.2 Lemme de Dickson *Soit $I = \langle X^\alpha, \alpha \in A \rangle$ idéal monômial. Il existe $\alpha_1, \dots, \alpha_s \in A$ tel que $I = \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle$.*

Démonstration. Par le théorème de la base de Hilbert, $I = \langle f_1, \dots, f_m \rangle$.

Soit S l'ensemble des monômes appartenant à un f_i. Alors pour tout i, $f_i \in \langle S \rangle$ donc $I \subset \langle S \rangle$.

Par la proposition, chaque $X^\alpha \in I$ donc $I = \langle S \rangle$. ∎

Définition 3.7 Soit I un idéal. On pose $\mathrm{LT}(I) = \{\mathrm{LT}(f), f \in I \neq 0\}$.

Définition 3.8 On dit qu'une partie finie de $\{g_1, \dots, g_t\}$ de I est une base de Gröbner ssi
$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t) \rangle$$

Proposition 3.7

(i) I admet une base de Gröbner

(ii) Une base de Gröbner de I est un système de générateurs de I.

Démonstration.

(i) $\langle \mathrm{LT}(I) \rangle$ est un idéal monômial donc par Dickson, il s'écrit $\langle \mathrm{LT}(I) \rangle = \langle X^{\alpha_1}, \ldots, X^{\alpha_t} \rangle$.
Par définition, chaque X^{α_i} est le monôme dominant d'un polynôme $g_i \in I$. $(g_1, \ldots, g_t)$ fournit une base de Gröbner.

(ii) Soit $f \in I$. Il faut montrer que $f \in \langle g_1, \ldots, g_t \rangle$. Par l'algorithme de division, $f = \sum_{i=1}^{t} a_i g_i + r$.
Si $r \neq 0$, aucun terme de r n'est divisible par $\mathrm{LT}(g_i)$ donc $r \notin \langle LT(I) \rangle$. Mais $r \in I$ donc $r \in \langle \mathrm{LT}(I) \rangle$. Contradiction. On a donc $r = 0$ et $f \in \langle g_1, \ldots, g_t \rangle$. ■

Proposition 3.8 Soit $G = \{g_1, \ldots, g_t\}$ une base de Gröbner de I et $f \in k[X_1, \ldots, X_n]$. Alors il existe un unique $r \in k[X_1, \ldots, X_n]$ tel que $f - r \in I$ et aucun terme de r n'appartient à $\langle \mathrm{LT}(I) \rangle$.

Démonstration. L'existence est assurée par l'algorithme de division. Pour l'unicité, soit r_1, r_2 qui marchent. Alors

$$r_1 - r_2 = (f - r_2) - (f - r_1) \in I$$

et aucun terme de $r_1 - r_2 \in \langle \mathrm{LT}(I) \rangle$, ce qui est impossible, sauf si $r_1 - r_2 = 0$. ■

Corollaire 3.3 *Soient G, I, f comme dans la définition. $f \in I$ ssi le reste est nul pour n'importe quel ordre sur G.*

Définition 3.9

(i) Si X^α et X^β sont des monômes, on pose $X^\gamma = X^\alpha \vee X^\beta$. $(\nu_i = \max\{\alpha_i, \beta_i\})$.

(ii) Soient $f, g \in k[X_1, \ldots, X_n]$. Le S-polynôme de f et g est

$$S(f, g) = \frac{X^\nu}{\mathrm{LT}(f)} f - \frac{X^\nu}{\mathrm{LT}(g)} g$$

où $X^\nu = \mathrm{LM}(f) \vee \mathrm{LM}(g)$.

Remarque 3.7 $S(g_i, g_j) = -S(g_j, g_i)$ *et* $S(g_i, g_i) = 0$.

Proposition 3.9 Soit une somme finie $P = \sum_{i=1}^{t} c_i X^{\alpha_i} g_i$ avec $c_i \in k$, $\alpha_i \in \mathbb{N}^n$ et $g_i \in k[X_1, \ldots, X_n]$ tel que

$$\alpha_i + \mathrm{multideg}(g_i) = \delta$$

soit indépendant de i. Si $\text{multideg}\, P < \delta$, alors il existe $c_{i,j} \in k$ tel que

$$P = \sum_{i<j} c_{i,j} X^{\delta-\gamma_{i,j}} S(g_i, g_j)$$

où $X^{\gamma_{i,j}} = \text{LM}(g_i) \vee \text{LM}(g_j)$. De plus, si $X^{\delta-\gamma_{i,j}} S(g_i, g_j) \neq 0$,

$$\text{multideg}(X^{\delta-\gamma_{i,j}} S(g_i, g_j)) < \delta$$

Démonstration. Notons $\beta_i = \text{multideg}\, g_i$. On a $\delta = \alpha_i + \beta_i$ donc $X^{\beta_i} \mid X^\delta$.
Alors $X^{\gamma_{i,j}} \mid X^\delta$ donc $X^{\delta-\gamma_{i,j}}$ est bien défini. Notons $d_i = \text{LC}(g_i)$.

$$X^{\delta-\gamma_{i,j}} S(g_i, g_j) = \frac{X^{\alpha_i}}{d_i} g_i - \frac{X^{\alpha_j}}{d_j} g_j =: p_i - p_j$$

Par ailleurs,

$$\begin{aligned} P &= \sum_{i=1}^{t} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) \\ &\quad + \ldots + (p_{t-1} - p_t) \sum_{i=1}^{t-1} c_i d_i + p_t \sum_{i=1}^{t} c_i d_i \\ &= \sum_{i<j} c_{i,j} (p_i - p_j) \end{aligned}$$

$p_t \sum_{i=1}^{t} c_i d_i = 0$ car $\text{multideg}(P) < \delta$. ∎

<u>Théorème 3.3</u> Critère de Buchberger *Soit I un idéal et un système de générateurs $G = \{g_1, \ldots, g_t\}$ de I.*

G est une base de Gröbner de I ssi pour tout $i < j$, le reste de $S(i, j)$ par G est nul (pour un ordre quelconque).

Démonstration.

$\Rightarrow$ Si G est Gröbner alors le reste est nul car $S(g_i, g_j) \in I$

$\Leftarrow$ On va montrer que $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. On montre $\subset$, ie pour tout $f \in I$, $\text{LT}(f) \in \langle \text{LT}(g_i) \rangle$.

Soit $f = \sum_{i=1}^{t} h_i g_i$. On note $m_i = \text{multideg}(h_i g_i)$ et $\delta = \max m_i$. On suppose que l'écriture choisie est telle que δ est minimal et $\text{multideg}(f) \leqslant \delta$.

- Si $\text{multideg}(f) = \delta$ alors $\text{multideg}\, f = m_i$ donc $\text{LT}(g_i) \mid \text{LT}(f)$ donc $f \in \langle \text{LT}(g_j) \rangle$.

- Si $\text{multideg}(f) < \delta$, on écrit

$$f = \sum_{m_i=\delta} \text{LT}(h_i)g_i + \sum_{m_i=\delta} (h_i - \text{LT}(h_i))g_i + \sum_{m_i<\delta} h_i g_i$$

Les deux dernières sommes ont un multidegré inférieur strictement à δ. On applique la proposition précédente à la première somme : on écrit $\text{LT}(h_i) = c_i X^{\alpha_i}$ et on a

$$\sum_{m_i=\delta} \text{LT}(h_i)g_i = \sum_{i<j}^{X^{\delta-\gamma_{i,j}}} S(g_i, g_j)$$

Par hypothèse, $S(g_i, g_j) = \sum_{l=1}^{t} a_{i,j,l} g_l$ avec

$$\text{multideg}(a_{i,j,l}g_l) \leqslant \text{multideg}(S(g_i, g_j))$$

donc

$$\sum_{m_i=\delta} \text{LT}(h_i)g_i = \sum_{m_i=m_j=\delta, i<j} \sum_{l=1}^{t} c_{i,j} a_{i,j,l} X^{\delta-\gamma_{i,j}} g_l$$

et $\text{multideg}(a_{i,j,l}X^{\delta-\gamma_{i,j}}g_l) \leqslant \text{multideg}(X^{\delta-\gamma_{i,j}}S(g_i, g_j)) < \delta$. Donc f a une autre écriture avec $\delta' < \delta$, contradiction avec δ minimal. ■

Lemme 3.3.1

Si $\text{LT}(g_i) \wedge \text{LT}(g_j) = 1$ alors $S(g_i, g_j) = \sum_{i=1}^{t} a_{i,j,l} g_l$ avec $\text{multideg}(a_{i,j,l}g_l) \leqslant \text{multideg}(S(g_i, g_j))$. On note $S(g_i, g_j) \to_G 0$.

Démonstration. On écrit $g_i = c_i \,\text{LM}(g_i) + p_i$ et $g_j = c_j \,\text{LM}(g_j) + p_j$ avec $\text{multideg}(p_i) < \text{multideg}(g_i)$ et $\text{multideg}(p_j) < \text{multideg}(g_j)$.

$$\begin{aligned} S(g_i, g_j) &= \frac{\text{LM}(g_i)\,\text{LM}(g_j)}{c_i \,\text{LM}(g_i)}(c_i \,\text{LM}(g_i) + p_i) - \frac{\text{LM}(g_i)\,\text{LM}(g_j)}{c_j \,\text{LM}(g_i)}(c_j \,\text{LM}(g_j) + p_j) \\ &= \frac{1}{c_i}\,\text{LM}(g_j)i - \frac{1}{c_j}\,\text{LM}(g_i)p_j \\ &= g_j \frac{p_i}{c_i c_j} - g_i \frac{p_j}{c_i c_j} \end{aligned}$$

Il faut montrer que

$$\text{multideg}(S(g_i, g_j)) = \max(\text{multideg}(\text{LM}(g_j)p_i), \text{multideg}(\text{LM}(g_i)p_j))$$

On a déjà $\geqslant$.

Si on avait $\text{multideg}(g_i)p_j = \text{multideg}(\text{LM}(g_j)p_i)$ donc $\text{LM}(g_i) \mid \text{LM}(g_j)p_i$. Par hypothèse, $\text{LM}(g_i) \mid p_i$, ce qui est impossible à cause du degré.

On a donc égalité dans la formule

$$\text{multideg}(f+g) \leqslant \max(\text{multideg}\, f, \text{multideg}\, g)$$ ■

Soit $I = \langle f_1, \ldots, f_s \rangle \subset k[X_1, \ldots, X_n]$ et on fixe un ordre monomial.

1. On pose initialement $G = \{f_1, \ldots, f_s\}$. Pour toute paire (i, j) avec iwj, on calcule le reste de $S(f_i, f_j)$ par G et on ajoute à G les restes non nuls.
2. On répète l'étape précédente jusqu'à ce que tous les restes soient nuls.

Exemple 3.5 $I = \langle yz + y, x^3 + y, z^4 \rangle \subset k[x, y, z]$. On a

$$S(f_1, f_2) = x^3(yz + y) - yz(x^3 + y) = x^3y - y^2z$$

$$S(f_1, f_3) = z^3(yz + y) - yz^4 = yz^3$$
$$S(f_2, f_3) = z^4(x^3 + y) - x^3z^4 = yz^4$$

Le reste de la division de yz^4 par G est y donc on remplace G par $\{f_1, f_2, f_3, f_4 := y\}$.

$S(f_1, f_4) = y$, $S(f_2, f_4) = y^2$ et $S(f_3, f_4) = 0$ donc tous les restes sont nuls et $\{f_1, f_2, f_3, f_4\}$ est une base de Gröbner.

Remarque 3.8 *À l'étape 1, il suffit de calculer les restes pour (f_i, f_j) avec $S(f_i, f_j) \not\to_G 0$ (ie $\text{LM}(g_i) \wedge \text{LM}(g_j) \neq 1$).*

Proposition 3.10 L'algorithme termine.

Démonstration. Soit G_n l'ensemble obtenu après n itérations. Soit $r \in G_{n+1}$ un reste non nul ajouté. Alors $\text{LT}(r)$ n'est pas divisible par $\text{LT}(g)$ avec $g \in G_n$ donc $\text{LT}(r) \notin \langle \text{LT}(G_n) \rangle$.

On a donc une suite strictement croissante d'idéaux monomiaux donnée par les $\langle \text{LT}(G_i) \rangle \subsetneq \langle \text{LT}(G_{i+1}) \rangle$.

Par nœthérianité, cette suite est stationnaire donc l'algorithme s'arrête. ■

3.3 Base de Gröbner réduite

Définition 3.10 Une base de Gröbner G de I est dite réduite si

1. $\text{LC}(g) = 1$ pour tout $g \in G$
2. Pour tout g de G, aucun monôme de g n'est divisible par $\text{LT}(g')$ avec $g' \neq g$.

Remarque 3.9 *Une base de Gröbner est dite minimale si elle satisfait (1) et que pour tout $g \in G$, $\mathrm{LT}(g)$ n'est pas divisible par $\mathrm{LT}(g')$ pour tout $g' \neq g$.*

THÉORÈME 3.4 *Tout idéal admet une unique base de Gröbner réduite.*

Démonstration.

∃ Soit G une base de Gröbner. On remplace g par $\frac{g}{\mathrm{LC}(g)}$ pour satisfaire (1).
En supprimant les $g \in G$ tel que $\mathrm{LT}(g)$ est divisible par $\mathrm{LT}(g')$, on ne change pas $\langle \mathrm{LT}(G) \rangle$ et on obtient une base minimale.
Supposant G minimale, pour tout $g_i \in G$, on remplace g_i par r_i le reste de la division de g_i par $G \setminus \{g_i\}$. Alors $\mathrm{LT}(g_i) = \mathrm{LT}(r_i)$ car la base est minimale donc $\{r_i\}$ est une base de Gröbner réduite.

! Soit G, G' deux bases réduites (ie $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(G') \rangle$).
Soit $g \in G$, $\mathrm{LT}(g) \in \langle \mathrm{LT}(G') \rangle$ donc il existe $g' \in G'$ tel que $\mathrm{LT}(g') \mid \mathrm{LT}(g)$. On a $\mathrm{LT}(g') \in \langle \mathrm{LT}(G) \rangle$ donc il existe $h \in G$ tel que $\mathrm{LT}(h) \mid \mathrm{LT}(g') \mid \mathrm{LT}(g)$. Comme g est réduite $g = h$.
Montrons que $g = g'$. Par (2), aucun terme de g ni de g' n'est divisible par $\mathrm{LT}(G \setminus \{g\})$ de même pour $g - g'$.
De plus, aucun terme de $g - g'$ n'est pas divisible par $\mathrm{LT}(g)$ et on a $\mathrm{multideg}(g - g') < \mathrm{multideg}(g)$ donc $g - g' = 0$. ∎

3.4 Application

3.4.1 Élimination

THÉORÈME 3.5 *Soit G une base de Gröbner de I pour l'ordre décroissant $X_1 > \ldots > X_n$. Alors $G \cap k[X_{r+1}, \ldots, X_n]$ est une base de Gröbner pour $I \cap k[X_{r+1}, \ldots, X_n]$.*

En particulier $I \cap k[X_{r+1}, \ldots, X_n] = \langle G \cap k[X_{r+1}, \ldots, X_n] \rangle$.

Exemple 3.6 $I = \langle x^3 + y, z^4, y \rangle$ donc $I \cap k[y, z] = \langle f_2, f_3 \rangle$ et $I \cap k[z] = \langle f_2 \rangle$.

Remarque 3.10 *Pour calculer $I \cap k[X]$, il faut calculer une base de Gröbner de I pour l'ordre $z > y > x$ ou $y > z > x$.*

Démonstration. On pose

$$G_r = G \cap k[X_{r+1}, \ldots, X_n] \text{ et } I_r = I \cap k[X_{r+1}, \ldots, X_n]$$

Si $\mathrm{LT}(g) \mid \mathrm{LT}(f)$ alors $g \in k[X_{r+1}, \ldots, X_n]$ et $f \in k[X_{r+1}, \ldots, X_n]$ car $\mathrm{multideg}(f) = (0, \ldots, 0, \alpha_{r+1}, \ldots, \alpha_n)$ donc de même pour $\mathrm{multideg}(g)$.

Soit $f \in I_r \subset I$ et G une base de Gröbner de I. Le reste de f par G est nul donc $f = \sum_{i=1}^{t} a_i g_i$ et alors seuls les $g_l \in G_r$ sont tels que $a_l \neq 0$, ie

$$f = \sum_{g_l \in G_r} a_l g_l \in \langle G_r \rangle$$

donc G_r est un système de générateurs de I_r.

Par Buchberger, il suffit de vérifier le reste de $S(g_i, g_j)$ par G_r est nul mais le reste de $S(g_i, g_j)$ par G est nul donc pareil pour G_r. ∎

3.4.2 Théorème d'extension

THÉORÈME 3.6 D'EXTENSION *Soit $I = \langle f_1, \ldots, f_s \rangle$. On écrit*

$$f_i = g_i(X_2, \ldots, X_n) X_1^{N_i} + h$$

h est une somme de termes de degrés $< N_i$ en X_1.

Supposons $(a_2, \ldots, a_n) \in \nu(I_1)$. Si $(a_2, \ldots, a_n) \notin \nu(g_1, \ldots, g_s)$ alors il existe $a_1 \in \overline{k}$ tel que $(a_1, \ldots, a_n) \in \nu(I)$.

Démonstration. Considérons le morphisme

$$\begin{cases} I & \to & k[X_1] \\ f & \mapsto & f(X_1, a_2, \ldots, a_n) \end{cases}$$

$I_m(I)$ est un idéal de $k[X_1]$ principal donc il s'écrit $\langle u(X_1) \rangle$.

Si $\deg(u(X_1)) > 0$ ou $u(X_1) = 0$ alors il admet une racine $a_1 \in \overline{k}$ et on a bien $(a_1, \ldots, a_n) \in \nu(I)$.

Sinon, $u(X_1) = u_0 \in k^\times$. On va montrer qu'on aune contradiction. Il existe $f \in I$ tel que $f(X_1, a_2, \ldots, a_n) = u_0$.

Par hypothèse $(a_2, \ldots, a_n) \notin \nu(g_1, \ldots, g_s)$ donc il existe g_i qui n'annule pas $(a_2, \ldots, a_n)$.

On a $P := \mathrm{Res}_{X_1}(f_i, f) \in I_1$ donc $P(a_2, \ldots, a_n) = 0$ mais en $(a_2, \ldots, a_n)$ le résultant vaut $g_i(a_2, \ldots, a_n)^{\deg_{X_1} f} u_0^{N_i} \neq 0$ (quand on écrit le déterminant). Contradiction. ∎

3.5 Théorèmes des zéros de Hilbert

THÉORÈME 3.7 DES ZÉROS DE HILBERT *Si k est algébriquement clos, soit $I \subset k[X_1, \ldots, X_n]$ tel que $V(I) = \varnothing$ alors $I = k[X_1, \ldots, X_n]$.*

Lemme 3.7.1
Soit f un polynôme non nul dans un corps k de cardinal infini. Il existe $(u_1, \dots, u_n) \in k^n$ tel que $f(u_1, \dots, u_n) \neq 0$.

Démonstration. Par récurrence sur n. Si $n = 1$, on sait que f a au plus $\deg(f)$ zéros.

Si $n > 1$, on écrit $f = f_n(X_2, \dots, X_n)X_1^n + P$ où P n'a que des degrés inférieurs à N en x_1. L'hypothèse de récurrence assure qu'il existe $(a_2, \dots, a_n) \in k^{n-1}$ qui n'annule pas f_n. Le polynôme $f(X_1, a_2, \dots, a_n)$ est alors non nul.

Il existe donc a_1 tel que $f(a_1, \dots, a_n) \neq 0$. ∎

Lemme 3.7.2
Soit k un corps infini, $f \in k[X_1, \dots, X_n]$ de degré total N. Il existe une famille $(u_2, \dots, u_n) \in k^{n-1}$ tel que le polynôme

$$\widetilde{f}(X_1, \dots, X_n) := f(X_1, X_2 + u_2X_1, \dots, X_n + u_nX_1)$$

soit de la forme $cX_1^N + P$ où P n'a que des termes de degrés $< N$ en X_1 et $c \neq 0$

Démonstration du théorème. Par récurrence sur n. Si $n = 1$ c'est bon. Supposons la propriété vraie pour $n - 1$.

Soit $I = \langle f_1, \dots, f_s \rangle$. Il est loisible de supposer par symétrie que $f_1 \notin k[X_2, \dots, X_n]$ (sinon c'est bon par l'hypothèse de récurrence).

Par le lemme, il existe $(u_2, \dots, u_n) \in k^{n-1}$ tel que $\widetilde{f_1} = cX_1^N + P$ avec $\deg_{X_1}(P) < N$ et $c \neq 0$.

On sait que $V(I) \neq \varnothing$ ssi $V(\widetilde{I}) \neq \varnothing$ et $I = k[X_1, \dots, X_n]$ ssi $\widetilde{I} = k[X_1, \dots, X_n]$.

Posons $\widetilde{I_1} = \widetilde{I} \cap k[X_2, \dots, X_n]$. Par le théorème d'extension, si $V(\widetilde{I}) = \varnothing$ alors $V(\widetilde{I_1}) = \varnothing$. L'hypothèse de récurrence assure que $\widetilde{I_1} = k[X_2, \dots, X_n]$ donc $1 \in \widetilde{I_1}$ donc $1 \in \widetilde{I}$.

Ainsi, $\widetilde{I} = k[X_1, \dots, X_n]$, ce qui prouve le théorème. ∎

THÉORÈME 3.8 *Si k est algébriquement clos, et $I \subset k[X_1, \dots, X_n]$. Alors $\mathcal{I}(V(I)) = \sqrt{I}$.*

Lemme 3.8.1
Soit k un corps quelconque et $I = \langle f_1, \dots, f_s \rangle$.

Alors $f \in \sqrt{I}$ ssi $1 \in J := \langle f_1, \dots, f_s, 1 - Yf \rangle \subset k[X_1, \dots, X_n, Y]$.

Démonstration.

$\Rightarrow$ Si $f \in \sqrt{I}$, il existe $m > 0$ tel que $f^m \in I \subset J$.
Donc $Y^m f^m \in J$. Or

$$1 = Y^m f^m + (1 - Y^m f^m) = Y^m f^m + (1 - Yf)(1 + Yf + \ldots + Y^{m-1} f^{m-1})$$

Donc $1 \in J$.

$\Leftarrow$ Si $1 \in J$, alors $1 = \sum_{i=1}^{s} p_i f_i + q(1 - Yf)$ où p_i et q appartiennent à $k[X_1, \ldots, X_n, Y]$.
En évaluant en $Y = \frac{1}{f}$, on a

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, \frac{1}{f}) f_i$$

Si on multiplie par f^m avec m assez grand, on aurait

$$f^m = \sum_{i=1}^{s} p'_i f_i \in I$$

avec $p'_i \in k[X_1, \ldots, X_n]$. ■

Démonstration du théorème 3.8. Il reste à montrer que $\mathcal{I}(V(I)) \subset \sqrt{I}$. Notons $I = \langle f_1, \ldots, f_s \rangle$ et $f \in \mathcal{I}(V(I))$.

On considère $J = \langle f_1, \ldots, f_s, 1 - Yf \rangle$.

Alors $V(J) = \varnothing$ car si $(x_1, \ldots, x_n, y) \in V(J)$, $(x_1, \ldots, x_n) \in V(I)$ donc $f(x_1, \ldots, x_n) = 0$ et $(1 - Yf)(x_1, \ldots, x_n, y) = 1 - y \times 0 = 1 \neq 0$.

On a donc $1 \in J$ et par le lemme $f \in \sqrt{I}$. ■

THÉORÈME 3.9 *Si k est algébriquement clos et $m \subset k[X_1, \ldots, X_n]$ maximal. Il existe $(a_1, \ldots, a_n) \in k^n$ tel que*

$$m = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$$

Démonstration. m est maximal donc propre. On a donc $V(m) \neq \varnothing$, il contient alors $(a_1, \ldots, a_n)$.

$$m \subset \mathcal{I}(V(m)) \subset \mathcal{I}(\{(a_1, \ldots, a_n)\}) = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$$

Or m et $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ sont maximaux donc il y a égalité. ■

THÉORÈME 3.10 *Soit k algébriquement clos et $I \subset k[X_1, \ldots, X_n]$ un idéal, $I_1 = I \cap k[X_2, \ldots, X_n]$.*

$V(I_1)$ est le plus petit ensemble algébrique de k^{n-1} contenant $\pi_1(V(I))$ où π_1 est la projection $(x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n)$.

Démonstration. Si W est un ensemble quelconque de k^n, sa clôture pour la topologie de Zariski $V(I(W))$.

Il suffit de montrer que $V(I_1) = V(\mathcal{I}(\pi(V)))$ sachant que $\supset$ est évidente par l'élimination. L'autre inclusion est équivalente à $\mathcal{I}(\pi_1(V)) \subset \sqrt{I_1}$.

Soit $f \in \mathcal{I}(\pi_1(V))$. f s'annule sur $\pi_1(V)$ donc si on voit $f \in k[X_1, \ldots, X_n]$, f s'annule sur V, c'est à dire que $f \in \mathcal{I}(V) = \sqrt{I}$. ∎

THÉORÈME 3.11 *Si k est algébriquement clos, on définit la projection π_l : $(x_1, \ldots, x_n) \mapsto (x_{l+1}, \ldots, x_n)$ et $I_l = I \cap k[X_{l+1}, \ldots, X_n]$. Alors $V(I_l)$ est la clôture de $\pi_l(V(I))$.*

Supposons que $V \subset k^n$ est défini par les paramètres $\{(x_1, \ldots, x_n), x_i = f_i(t_1, \ldots, t_n)\}$.

THÉORÈME 3.12 *Soit $I = \langle X_i - f_i(t_1, \ldots, t_n), i \in [\![1, n]\!] \rangle$. Alors $V(I_{m+1})$ est la clôture de $\pi_m(V(I))$.*

Remarque 3.11 En général, ce n'est pas facile de déterminer si $V(I_{m+1}) = V$.

THÉORÈME 3.13 *Si k est algébriquement clos, soit V l'ensemble*

$$\left\{(x_1, \ldots, x_n) \in k^n, x_i = \frac{f_i(t_1, \ldots, t_m)}{g_i(t_1, \ldots, t_m)}, (t_1, \ldots, t_m) \in k^m \setminus \nu(g_1, \ldots, g_n)\right\}$$

Soit $J = \langle g_1 X_1 - f_1, \ldots, g_n X_n - f_n, 1 - gY \rangle$ avec $g = g_1 \ldots, g_n$ et $J_{m+1} = J \cap k[X_1, \ldots, X_n]$.

Alors $\nu(I_{m+1}) = \overline{V}$.

Exemple 3.7 Soit $V = \{x_1 = \frac{x^2}{v}, x_2 = \frac{v^2}{x}, x_3 = u\}$ défini sur $k^2 \setminus \{(0,0)\}$.

Posons $I = \langle vX_1 - u^2, uX_2 - v^2, u - X_3 \rangle$. $I \cap k[X_1, X_2, X_3] = \langle X_3(X_1^2 X_2 - X_3^3) \rangle \neq \overline{V}$.

Si $J = \langle vX_1 - u^2, uX_2 - v^2, u - X_3, 1 - Yuv \rangle$, $J \cap k[X_1, X_2, X_3] = \langle X_1^2 X_2 - X_3^3 \rangle = \overline{V}$.

Définition 3.11 $V - W := V \cap W^c$.

Proposition 3.11 Si k est algébriquement clos, soit $I, J \subset k[X_1, \ldots, X_n]$ deux idéaux avec I radical.

Alors $\nu(I : J) = \overline{\nu(I) - \nu(J)}$.

Démonstration. I est radical donc $(I : J)$ est radical. Ainsi $\mathcal{I}(\nu(I : J)) = (I : J)$.

La proposition est alors équivalente à $(I : J) = \mathcal{I}(\nu(I) - \nu(J))$.

$\subset$ Soit $f \in (I : J)$ et $a \in \nu(I) - \nu(J)$.

Il existe $g \in J$ tel que $g(a) \neq 0$, $fg \in I$ donc $(fg)(a) = 0$ et $g(a) \neq 0$ donc $f(a) = 0$ et $f \in \mathcal{I}(\nu(I) - \nu(J))$.

$\supset$ Soit $f \in \mathcal{I}(\nu(I) - \nu(J))$. On a $f(a) = 0$ pour tout $a \in \nu(I) - \nu(J)$.
Si $g \in J$, $g(a) = 0$ pour tout $a \in \nu(J)$ donc $(fg)(a) = 0$ pour tout $a \in \nu(J)$. On a aussi $(fg)(a) = 0$ pour tout $a \in \nu(I) - \nu(J)$.
Ainsi, $f(a) = 0$ si $a \in \nu(I)$ donc par Hilbert, $(fg) \in \mathcal{I}(\nu(I)) = \sqrt{I} = I$ donc $f \in (I : J)$. ■

Exemple 3.8

- $I = \langle X^2 \rangle$, $J = \langle X \rangle$. $\nu(I) - \nu(J) = \varnothing$ et $(I : J) = \langle X \rangle$. L'hypothèse de radicalité est donc nécessaire.
- $I = \langle XZ, YZ \rangle$ et $J = \langle Z \rangle$. $\nu(I) = \{z = 0\} \cup \{x = y = 0\}$ et $\nu(J) = \{z = 0\}$.
  On a $\overline{\nu(I) - \nu(J)} = \{x = y = 0\} = \nu(\langle X, Y \rangle)$.

COROLLAIRE 3.4 *Soit k algébriquement clos, $V, W \subset k^n$ deux ensembles algébriques.*

$$\mathcal{I}(V - W) = (\mathcal{I}(V) : \mathcal{I}(W))$$

Proposition 3.12 Soit $V \subset k^n$ et $W \subset k^m$ deux ensembles algébriques d'idéaux $I \subset k[X_1, \ldots, X_n]$ et $J \subset k[Y_1, \ldots, Y_n]$.

Alors $V \times W \subset k^{n+m}$ est un ensemble algébrique défini par $\langle \langle I \rangle, \langle J \rangle \rangle \subset k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$.

Démonstration.

$$\begin{aligned}
(a, b) \in V \times W \quad &\text{ssi} \quad a \in \nu(I), b \in \nu(J) \\
&\text{ssi} \quad \forall f \in I, g \in J, f(a) = g(b) = 0 \\
&\text{ssi} \quad \forall f \in \langle I \rangle, g \in \langle J \rangle f(a, b) = g(a, b) = 0 \\
&\text{ssi} \quad (a, b) \in \nu(\langle \langle I \rangle, \langle J \rangle \rangle)
\end{aligned}$$

■

Remarque 3.12 La topologie de Zariski sur k^{n+m} est plus fine que le produit des topologies sur $k^n \times k^m$.

<u>Définition 3.12</u> Soit V un ensemble algébrique non vide de k^n. On dit que V est irréductible ssi pour tout V_1, V_2 algébriques vérifiant $V_1 \cup V_2 = V$, $V = V_1$ ou $V = V_2$.

Cette condition est équivalente à $V \subset V_1 \cup V_2 \Rightarrow V \subset V_1$ ou $V \subset V_2$.

Lemme 3.13.1
V est irréductible ssi $\mathcal{I}(V)$ est premier dans $k[X_1, \ldots, X_n]$.

Démonstration.

$\Rightarrow$ Si V est irréductible, soit $fg \in \mathcal{I}(V)$.
Pour tout $a \in V$, $(fg)(a) = 0$ donc $a \in \nu(f)$ ou $a \in \nu(g)$. Ainsi, $V \subset \nu(f) \cup \nu(g)$.
Comme V est irréductible, $V \subset \nu(f)$ ou $V \subset \nu(g)$ donc $f \in \mathcal{I}(V)$ ou $g \in \mathcal{I}(V)$.

$\Leftarrow$ Si $\mathcal{I}(V)$ est premier, soit V_1, V_2 tels que $V = V_1 \cup V_2$.
$\mathcal{I}(V) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2) \supset \mathcal{I}(V_1)\mathcal{I}(V_2)$ donc il existe $i \in \{1, 2\}$ tel que $\mathcal{I}(V_i) \subset \mathcal{I}(V)$. L'autre inclusion est vraie puisque $\mathcal{I}(V) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$.
Ainsi, $V = V_i$. ■

THÉORÈME 3.14 *Tout ensemble algébrique s'écrit de manière unique sous la forme $V_1 \cup \ldots \cup V_m$ avec V_i irréductibles fermés et $V_i \not\subset V_j$ si $i \neq j$.*

On va démontrer l'énoncé correspondant dans les idéaux premiers :

THÉORÈME 3.15 *Tout idéal propre radical de $k[X_1, \ldots, X_n]$ s'écrit de manière unique comme $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$ avec $\mathfrak{p}_i$ premiers et $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ si $i \neq j$. (C'est même vrai si on prend A nœthérien à la place de k).*

Démonstration.
- Pour A quelconque et I idéal propre, il existe des idéaux premiers minimaux contenant I (via Zorn cf. TD).
- Si A est nœthérien, I n'admet qu'une nombre fini d'idéaux premiers minimaux (cf. TD).
- On sait que $I = \sqrt{I} = \bigcap_{\mathfrak{p} \text{ premier minimal, } I \subset \mathfrak{p}} \mathfrak{p}$.
- Pour avoir l'unicité, il suffit de montrer que les $\mathfrak{p}_i$ sont minimaux. C'est le cas car si $I \subset \mathfrak{p} \subset \mathfrak{p}_i$ est premier, $\mathfrak{p}$ contient l'intersection des $\mathfrak{p}_j$ donc il contient un $\mathfrak{p}_j$. On a donc $\mathfrak{p}_j \subset \mathfrak{p}_i$ donc par hypothèse $\mathfrak{p}_i = \mathfrak{p}_j = \mathfrak{p}$. ■

Proposition 3.13 Si k est infini, k^n est irréductible.

Démonstration. Il suffit de montrer que $\nu(k^n) = \langle 0 \rangle$ est premier. Si f s'annule en tout point de k^n et k infini alors $f = 0$. ■

COROLLAIRE 3.5 *Si k est infini, si*

$$V = \{(x_1, \ldots, x_n), x_i = f_i(t_1, \ldots, t_m), t_i \in k\}$$

alors $\overline{V}$ est irréductible.

Démonstration. Soit $F : (t_1, \ldots, t_m) \mapsto (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$.
Il suffit de montrer que $\mathcal{I}(\overline{V}) = \mathcal{I}(V)$ est premier. Soit $gh \in \mathcal{I}(V)$.
On a $(gh)(x_1, \ldots, x_n) = 0$ donc $(gh)(F(t_1, \ldots, t_m)) = 0$ donc comme k est infini, $(gh) \circ F = 0$ donc $g \circ F = 0$ ou $h \circ F = 0$.
Ainsi, $g \in \mathcal{I}(V)$ ou $h \in \mathcal{I}(V)$. ■

Remarque 3.13 Si $F : X \to Y$ est continu et $X_1 \subset X$ irréductible alors $\overline{f(X_1)}$ est irréductible.

Proposition 3.14 Si $V \subset k^n$ et $W \subset k^m$ sont irréductibles alors $V \times W \subset k^{m+n}$ est aussi irréductible.

Démonstration. Supposons $V \times W = X_1 \cup X_2$ avec $V \times W \neq X_2$.

Pour tout $x \in V$, $\{x\} \times W$ est homéomorphe à W donc comme W est irréductible, $\{x\} \times W \subset X_1$ ou $\{x\} \times W \subset X_2$.

Posons $V_i = \{x \in V, \{x\} \times W \subset X_i\}$. Alors $V = V_1 \cup V_2$ et par hypothèse, $V \times W \neq X_2$ donc $V \neq V_2$.

Si V_1 et V_2 sont fermés, comme V est irréductible, on a $V = V_1$. Ainsi, $V \times W = X_1$.

On a $V_1 = \bigcap_{y \in W} V_y$ avec $V_y = \{x \in V, (x, y) \in X_1\}$ qui est fermé car homéomorphe à $V_y \times \{y\} = X_1 \cap (V \times \{y\})$. Ainsi, V_1 est fermé (et V_2 aussi par symétrie. ■

Remarque 3.14 Résumé Les applications ν et $\mathcal{I}$ définissent une bijection entre les idéaux radicaux de $k[X_1, \ldots, X_n]$ et les ensembles algébriques de k^n. En particulier, on a une correspondance entre

Idéaux premiers	*Ensembles irréductibles*
Idéaux maximaux	*Points*
$I_1 \cap I_2$	$\nu(I_1) \cup \nu(I_2)$
$\sqrt{I_1 + I_2}$	$\nu(I_1) \cap \nu(I_2)$

Chapitre 4

Dimension

4.1 Localisation

Définition 4.1 Un anneau A est dit local ssi il admet un unique idéal maximal.

Exemple 4.1

- Les corps sont locaux.
- $k[\![X]\!]$ est local mais pas $k[X]$
- $k[X]/\langle X^n \rangle$ est local.

Lemme 4.0.1
A est local ssi l'ensemble des non inversibles de A est un idéal (l'unique idéal maximal).

Démonstration.

$\Rightarrow$ Si A est local, notons $\mathfrak{m}$ son idéal maximal. Comme x n'est pas inversible il est contenu dans un idéal maximal donc dans $\mathfrak{m}$.
L'inclusion réciproque est claire puisque si $\mathfrak{m}$ contient un inversible, $\mathfrak{m} = A$.

$\Leftarrow$ Posons $\mathfrak{m}$ l'idéal des éléments non inversibles.
Tout idéal propre est inclus dans $\mathfrak{m}$ donc $\mathfrak{m}$ est l'unique idéal maximal.

■

Définition 4.2 Soit S une partie de A. On dit que S est multiplicative ssi S est stable par $\times$ et $1 \in S$.

Si S est multiplicative, on considère la relation sur $A \times S$ donnée par $(a, s) \sim (a', s')$ ssi il existe $r \in S$ tel que $r(as' - a's) = 0$.

Lemme 4.0.2
$\sim$ est une relation d'équivalence.

Démonstration. La réflexivité et la symétrie sont claires. Si $(a,s) \sim (a',s') \sim (a'',s'')$, on a $r, r' \in S$ tel que $r(as'-a's)=0=r'(a's''-a''s')$. Une petite astuce donne

$$s'(as''-a''s) = s''(as'-a's) + s(a's''-a''s')$$

donc $rr's'(as''-a''s)=0$. ∎

Définition 4.3 On note $A[S^{-1}]$ ou $S^{-1}A$ le quotient $A\times S/\sim$ et on l'appelle localisé (ou localisation) de A par rapport à S. On note $\frac{a}{s}$ la classe de (a,s).

Définition 4.4 On munit $S^{-1}A$ d'une structure d'anneau via

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st} \text{ et } \frac{a}{s}\times\frac{b}{t}=\frac{ab}{st}$$

qui sont bien définies.

Remarque 4.1 Pour tout $s \in S$, $\frac{1}{s} \in A[S^{-1}]$ donc $\frac{s}{1}\times\frac{1}{s}=1$ donc les éléments de S deviennent inversibles dans le localisé.

Si $0 \in S$, $A[S^{-1}]=\{0\}$ car $\frac{1}{1}=\frac{0}{1}$.

Définition 4.5 On note i_S le morphisme $a \mapsto \frac{a}{1}$.

Proposition 4.1 $\mathrm{Ker}(i_S)=\{a\in A, \exists s\in S, as=0\}$. En particulier, i_S est injectif ssi S ne contient pas de diviseur de 0 de A.

Démonstration. $i_S(a)=0$ ssi $\frac{a}{1}=\frac{0}{1}$ ssi il existe $s\in S$ tel que $as=0$. ∎

4.2 Idéaux

Définition 4.6 On note $I^e=\langle i_S(I)\rangle$ et $J^c=i_S^{-1}(J)$.

Lemme 4.0.3
$I^e=\{\frac{a}{s}, a\in I, s\in S\}$.

Démonstration.

$$\begin{aligned} I^e &= \left\{\sum_{i=1}^n \frac{a_i}{1}\frac{b_i}{s_i}, a_i\in I, b_i\in A, s_i\in S\right\} \\ &= \left\{\frac{1}{s_1\dots s_n}\sum_{i=1}^n a_i t_i, a_i\in I, t_i\in A, s_i\in S\right\} \\ &= \left\{\frac{a}{s}, a\in I, s\in S\right\} \end{aligned}$$

∎

Corollaire 4.1

(i) $I^e = A[S^{-1}]$ *ssi* $I \cap S = \varnothing$

(ii) $(I_1 \cap I_2)^e = I_1^e \cap I_2^e$

(iii) $(I_1 + I_2)^e = I_1^e + I_2^e$

(iv) $(I_1 I_2)^e = I_1^e I_2^e$

Proposition 4.2

(i) Soit J un idéal de $A[S^{-1}]$. $(J^c)^e = J$.

(ii) Soit I un idéal de A, $(I^e)^c = \bigcup_{s \in S} (I : s) = \{a \in A, \exists s \in S, sa \in I\}$.

Démonstration.

(i) $(J^c)^e \subset J$ c'est bon.
Soit $\frac{a}{s} \in J$. $\frac{a}{1} = \frac{a}{s}\frac{s}{1}$ donc $a \in J^c$ donc $\frac{a}{s} \in (J^c)^e$.

(ii) Soit $a \in (I^e)^c$ ie $\frac{a}{1} \in I^e$. Par le lemme, il existe $b \in I$ et $s \in S$ tel que $\frac{a}{1} = \frac{b}{s}$.
Il existe donc $r \in S$ tel que $ras = rb \in I$ donc $a \in (I : rs) \subset \bigcup_{s \in S} (I : s)$.
Soit $s \in S$ et $a \in (I : s)$. $as \in I$ donc $\frac{a}{1} = \frac{as}{s} \in I^e$ donc $a \in (I^e)^c$. ■

THÉORÈME 4.1 *Les applications* $\mathfrak{p} \mapsto \mathfrak{p}^e$ *et* $\mathfrak{q} \mapsto \mathfrak{q}^c$ *définissent deux bijections réciproques entre les idéaux premiers de* A *qui n'intersectent pas* S *et les idéaux premiers de* $A[S^{-1}]$.

Démonstration. Il faut vérifier que si $\mathfrak{p}$ est premier et $\mathfrak{p} \cap S = \varnothing$ alors $\mathfrak{p}^e$ est premier. Soit $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}^e$.

Il existe $c \in \mathfrak{p}$ et $r \in S$ tel que $\frac{ab}{st} = \frac{c}{r}$.

Il existe donc $r' \in S$ tel que $r'(abr) = r'(stc) \in p$. Or $r, r' \in S$ et $S \cap \mathfrak{p} = \varnothing$ donc $r, r' \notin \mathfrak{p}$.

Alors $ab \in \mathfrak{p}$ donc $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ donc $\frac{a}{s} \in \mathfrak{p}^e$ ou $\frac{b}{t} \in \mathfrak{p}^e$. ■

COROLLAIRE 4.2 *Si* $S = A \setminus \mathfrak{p}$ *(qui est multiplicative car si* $r, s \notin \mathfrak{p}$, $rs \notin \mathfrak{p}$*).*

Notons $A_\mathfrak{p} = A[S^{-1}]$. $A_\mathfrak{p}$ *est un anneau local dont l'unique idéal maximal est* $\mathfrak{p}^e$. *On a de plus une bijection entre les idéaux premiers* $\mathfrak{p}'$ *de* A *inclus dans* $\mathfrak{p}$ *et les idéaux premiers de* $A_\mathfrak{p}$ *qui conserve les inclusions.*

Exemple 4.2

(i) Si A est intègre, $\mathfrak{p} = (0)$. $A_\mathfrak{p} = A_{(0)} = \mathrm{Frac}(A)$.

(ii) Soit $s \in A$, $S = \{1, s, \ldots, s^n, \ldots\}$ multiplicative. $A[S^{-1}] = 0$ ssi s est nilpotent. Les idéaux premiers de $A[S^{-1}]$ sont les idéaux premiers de A qui ne contiennent pas s.

THÉORÈME 4.2 *Pour tout anneau B et tout morphisme $\phi : A \to B$ tel que $\phi(S) \subset B^*$, il existe un unique ψ tel que $\psi \circ i_S = \phi$.*

Démonstration. Définir $\psi(\frac{a}{s}) = \phi(a)\phi(s)^{-1} \in B$. ∎

4.3 Lemme de Nakayama

Définition 4.7 Si I est un idéal de A et M un A-module, alors IM est l'ensemble des sommes finies de $a_i m_i$ avec $a_i \in I$ et $m_i \in M$.

Si de plus, M est de type fini engendré par $x_1, \ldots, x_n$, IM est l'ensemble des $\sum_{i=1}^{n} a_i x_i$, $a_i \in I$.

Définition 4.8 Soit $\phi : A \to B$. On dit que B est fini sur A ssi B est de type fini en tant que A-module.

Si C est fini sur B et B fini sur A alors C est fini sur A.

Lemme 4.2.1
Soit M un A-module de type fini et I un idéal propre de A. Si $IM = M$ alors il existe $z \in I$ tel que $(1 - z)M = 0$.

Démonstration. Si M est engendré par $(x_1, \ldots, x_n)$ et $IM = M$, $x_i \in IM$ donc $x_i = \sum_{j=1}^{n} a_{i,j} x_j$ donc $(x_1, \ldots, x_n)$ annule $H := (a_{i,j})_{i,j}$.

En multipliant à gauche par la comatrice de H, on trouve

$$\det(H)(x_1, \ldots, x_n) = 0$$

Or $\det(H) = \prod_{i=1}^{n}(1 - a_{i,i}) + r = 1 - z$ avec $r, z \in I$. Alors $(1 - z)x_i = 0$ pour tout i donc $(1 - z)M = 0$. ∎

COROLLAIRE 4.3 LEMME DE NAKAYAMA *Soit M un A-module de type fini.*

Soit I un idéal inclus dans le radical de Jacobson de A. Si $IM = M$ alors $M = \{0\}$.

Démonstration. Pour tout $z \in I$, $1 - z$ est inversible et par le lemme $(1 - z)M = 0$ donc $M = 0$. ∎

COROLLAIRE 4.4 *Si A est local, $I \subset A$ est propre, M est un A-module de type fini et $IM = M$ alors $M = 0$.*

Démonstration. Si A est local et $\mathfrak{m}$ est l'unique idéal maximal, le radical de Jacobson est $\mathfrak{m}$ donc par Nakayama, $M = 0$. ∎

4.4 Extension entière

Définition 4.9 $b \in B$ est dit entier sur $A \subset B$ ssi il est racine d'un polynôme unitaire de $A[X]$.

On dit que B est entier sur A ssi tous les éléments de B sont entiers sur A.

Remarque 4.2 On peut définir la notion pour $\phi : A \to B$ en disant que b est entier sur A ssi b est entier sur $\phi(A)$.

Proposition 4.3 Soit $A \subset B$ et $b \in B$. Les conditions suivantes sont équivalentes :

(i) b est entier sur A

(ii) $A[b]$ est fini sur A

(iii) il existe une sous-A-algèbre R de B tel que $A[b] \subset R \subset B$ et R fini sur A.

Démonstration.

(i) $\Rightarrow$ (ii) Il existe $P \in A[X]$ unitaire tel que $P(b) = 0$. Alors $A[b]$ est engendrée par $\{1, b, \dots, b^{\deg(P)-1}\}$.

(ii) $\Rightarrow$ (iii) clair ($R = A[b]$)

(iii) $\Rightarrow$ (i) R est fini sur A engendré par $x_1, \dots, x_n \in R$.

$b \in R$ donc $bx_i \in R$. Ainsi, $bx_i = \sum_{j=1}^{n} a_{i,j} x_j$ donc $(x_1, \dots, x_n)$ annule $H := b\,\mathrm{Id} - (a_{i,j})_{i,j}$.

Alors $\det(H)(x_1, \dots, x_n) = 0$ mais R est engendré par $\{x_1, \dots, x_n\}$ donc $\det(H)R = 0$ et $1 \in R$ donc $\det(H) = 0$.

Or $\det(H)$ est un polynôme en b donc b est entier sur A. ∎

Corollaire 4.5 *Soient $b_1, \dots, b_n$ entiers sur A. L'algèbre $A[b_1, \dots, b_n]$ est un A-module de type fini. En particulier, $A[b_1, \dots, b_n]$ est entière sur A.*

Démonstration. $A \hookrightarrow A[b_1] \hookrightarrow \dots \hookrightarrow A[b_1, \dots, b_n]$ qui sont tous finis donc $A[b_1, \dots, b_n]$ fini sur A.

On applique (iii). Pour tout $b \in A[b_1, \dots, b_n]$, on pose $R = A[b_1, \dots, b_n]$ et on a donc que b est entier. ∎

Corollaire 4.6 *Soit $A \subset B$. L'ensemble des éléments de B entiers sur A est un sous-anneau de B.*

Définition 4.10 On appelle clôture intégrale de A dans B l'ensemble des éléments de B entiers sur A. Si A est intègre, soit K son corps de fractions, la fermeture intégale de A dans K est appelée la clôture intégrale de A.

Proposition 4.4 Soit $A \subset B$ entier.

(i) Soit q premier de B et $\mathfrak{p} = q^c$ premier de A. Alors $A/\mathfrak{p} \subset B/q$ est entier.

(ii) Soit $S \subset A$ une partie multiplicative alors $S^{-1}A \subset S^{-1}B$ est entier.

Démonstration.

(i) Il suffit de passer les équations polynômiales au quotient.

(ii) Soit $\frac{b}{s} \in S^{-1}B$ alors en divisant par s^n l'équation polynômiale en b, on obtient une équation polynômiale en $\frac{b}{s}$ à coefficients dans $S^{-1}A$. ∎

Proposition 4.5 Soit $A \subset B$ anneaux intègres avec B entier sur A. Alors A est un corps ssi B est un corps.

Démonstration.

⇒ Soit $b \in B$ non nul. On prend une équation polynômiale de degré minimal en b.

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

$a_0 \neq 0$ sinon n ne serait pas minimal (factoriser par b). Comme A est un corps, a_0 est inversible et on a alors

$$b(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1) = -a_0$$

Donc b est inversible d'inverse $-a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1)$.

⇐ Soit $a \in A$ non nul. a est inversible dans B donc il existe $b \in B$ tel que $ab = 1$. On multiplie une équation polynômale de degré n pour b par a^{n-1}, ce qui donne

$$b + a_{n-1} + aa_{n-1} + \ldots + a^{n-1}a_0 = 0$$

donc $b \in A$ et a est inversible dans A. ∎

Corollaire 4.7 *Soit $A \subset B$ entière, $q \in \mathrm{Spec}(B)$, $\mathfrak{p} = q^c \in \mathrm{Spec}(A)$. Alors $\mathfrak{p}$ est maximal ssi q l'est.*

Démonstration. $A/\mathfrak{p} \subset B/q$ est entière et ce sont deux anneaux intègres donc $A/\mathfrak{p}$ est un corps ssi B/q l'est, ce qui assure le résultat. ∎

Corollaire 4.8 *Soit $A \subset B$ entière, $q_1 \subsetneq q_2 \in \mathrm{Spec}\, B$. Alors $q_1^c \subsetneq q_2^c$.*

Démonstration. Si $\mathfrak{p} = q_1^c = q_2^c$, soit $S = A \setminus \mathfrak{p}$ multiplicative. $A_\mathfrak{p}$ est local et $S^{-1}B$ est entier sur $A_\mathfrak{p}$.

$q_1(S^{-1}B) \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ est maximal donc $q_1(S^{-1}B)$ est maximal, ce qui contredit $q_1(S^{-1}B) \subsetneq q_2(S^{-1}B)$. ∎

Définition 4.11 Si $\iota : A \to B$, on note $\iota^* : q \mapsto q^c$ pour $q \in \mathrm{Spec}(B)$.

Proposition 4.6 Si $\iota : A \to B$ est entière, ι^* est surjective.

Démonstration. Soit $S = A \setminus \mathfrak{p}$. $A_\mathfrak{p} \subset S^{-1}B$ est entière. Soit $m \subset S^{-1}B$ un idéal maximal.

$m^c = m \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Il suffit de prendre $q = m \cap B$. On a $q \cap A = (m \cap A_\mathfrak{p}) \cap A = \mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}$. ∎

Exemple 4.3 $A = k[X, Y]$, $B = k[X, Y, Z]/(XZ - Y^2)$. $A \subset B$ n'est pas entière car $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ n'est pas surjectif.

En effet, si $q^c = (X, Y - 1)$, q contient $X, Y - 1, XZ - Y^2$ donc contient $Y^2 = Zf_1 - f_3$ et $Y^2 - 1 = (Y + 1)f_2$ donc 1. Alors q n'est pas premier.

Si $A = k[X, Z]$, $A \subset B$ est entière car Y est entier sur A.

THÉORÈME 4.3 GOING UP *Soit $\iota : A \subset B$ entière. Soit $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ deux idéaux premiers de A.*

Soit q_1 tel que $\iota^*(q_1) = \mathfrak{p}_1$. Il existe $q_2 \in \mathrm{Spec}(B)$ tel que $q_1 \subset q_2$ et $\iota^*(q_2) = \mathfrak{p}_2$.

Démonstration. $A/\mathfrak{p}_1 \subset B/q_1$ est entière et $\mathfrak{p}_2/\mathfrak{p}_1$ est premier dans $A/\mathfrak{p}_1$ donc par surjectivité de ι^*, on a $q_2/q_1 \in \mathrm{Spec}(B/q_1)$ image réciproque de $\mathfrak{p}_2/\mathfrak{p}_1$.

Ainsi, $q_2 \in \mathrm{Spec}(B)$ et $\iota^*(q_2) = \mathfrak{p}_2$. ∎

Définition 4.12 Dimension de Krull On appelle dimension de Krull de A notée $\dim(A)$ l'entier

$$\sup\{n, \exists \mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n \text{ premiers}\}$$

Si $\mathfrak{p} \in \mathrm{Spec}(A)$, on définit la hauteur de $\mathfrak{p}$ par

$$\mathrm{ht}(\mathfrak{p}) = \sup\{n, \exists \mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}\} = \dim A_\mathfrak{p}$$

Exemple 4.4

- La dimension d'un corps est nulle.
- $\dim(k[X]) = 1$ car $k[X]$ est principal donc les seule chaînes qu'on peut faire sont de la forme $(0) \subsetneq (f)$ avec f irréductible.
- On montrera que $\dim k[X_1, \ldots, X_n] = n$. Il est déjà évident que

  $$\dim k[X_1, \ldots, X_n] \geqslant n$$

  puisque

  $$(0) \subsetneq (X_1) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$$

- Si $\alpha : A \twoheadrightarrow B$ alors $\dim A \geqslant \dim B$.

THÉORÈME 4.4 COHEN-SEIDENBERG *Soit $A \subset B$ entière. Alors* $\dim(A) = \dim(B)$.

Démonstration. Soit $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ une suite de premiers de A. On obtient une suite de premiers dans B (Going up) donc $\dim(A) \leqslant \dim(B)$.

Soit $q_0 \subsetneq \ldots \subsetneq q_n$ une suite de premiers de B. On obtient une suite de premiers dans A (q_i^c) donc $\dim(A) \geqslant \dim(B)$. ∎

Exemple 4.5 $k[X,Z] \to k[X,Y,Z]/(XZ - Y^2)$ est entière donc

$$\dim(k[X,Y,Z]/(XZ - Y^2)) = 2$$

Définition 4.13 Soit A une k-algèbre. Des éléments $a_1, \ldots, a_n \in A$ sont dits algébriquement indépendants ssi

$$\forall P \in k[X_1, \ldots, X_n], P(a_1, \ldots, a_n) = 0 \Rightarrow P = 0$$

THÉORÈME 4.5 LEMME DE NORMALISATION DE NŒTHER *Soit k un corps, A une k-algèbre de type fini. Il existe $a_1, \ldots, a_n \in A$ algébriquement indépendants tels que*

$$k \hookrightarrow k[a_1, \ldots, a_n] \hookrightarrow A$$

soit entière.

Remarque 4.3 Les a_i ne sont pas uniques mais n l'est (c'est $\dim(A)$*).*

Lemme 4.5.1
Soit A une k-algèbre de type fini engendrée par $x_1, \ldots, x_m$ supposés algébriquement liés.

Alors il existe $y_1, \ldots, y_{m-1} \in A$ tels que x_m est entier sur $k[y_1, \ldots, y_{m-1}]$ et $A = k[y_1, \ldots, y_{m-1}][x_m]$.

Démonstration valable si $|k| = \infty$. On cherche des y_i de la forme $x_i - \lambda_i x_m$. On aura alors clairement $A = A'[x_m]$.

Soit $P \in k[X_1, \ldots, X_m]$ non nul tel que $P(x_1, \ldots, x_m) = 0$. On note $d = \deg P$ et on a $x_i = y_i + \lambda_i x_m$ donc

$$0 = P(y_1 + \lambda_1 x_m, \ldots, y_{m-1} + \lambda_{m-1} x_m, x_m) = Q(\lambda_1, \ldots, \lambda_{m-1}) x_m^d + R$$

avec R de degré $< d$ en x_m à coefficients dans $k[y_1, \ldots, y_{m-1}]$.

On choisit alors λ_i tel que $Q(\lambda_i) \neq 0$. Alors x_m est entier sur A'. ∎

Remarque 4.4 Dans le cas général, on fait $y_i = x_i - x_m^{k^{m-i}}$ avec k suffisemment grand.

Démonstration du lemme de normalisation. Soit A de type fini engendrée par $x_1, \dots, x_m$. On fait une récurrence sur m.

Pour $m = 1$, $A = k[x_1]$. Si x_1 est transcendant sur k, $A \simeq k[X]$ donc on prend $a_1 = x_1$ sinon, $k \to k[x_1]$ est algébrique donc c'est bon.

Si c'est vrai pour $m-1$, soit les x_i sont algébriquement indépendants, on prend $a_i = x_i$.

Sinon les x_i sont liés. Il existe donc $y_1, \dots, y_{m-1} \in A$ tel que $A = k[y_1, \dots, y_{m-1}, x_m]$ et $A' = k[y_1, \dots, y_{m-1}] \to A$ entière.

On applique l'hypothèse de récurrence à A' qui donne $a_1, \dots, a_n \in A'$ indépendantes tels que $k[a_1, \dots, a_n] \to A'$ soit entière.

Ainsi, A est entier sur $k[a_1, \dots, a_n]$. ∎

THÉORÈME 4.6 $\dim k[X_1, \dots, X_n] = n$.

Démonstration. On a vu que $\geqslant$ était claire. On montre $\leqslant$ par récurrence sur n. Si $n = 1$ c'est bon.

Si l'énoncé est vrai pour $n-1$, soit $\mathfrak{p}_0 = (0) \subsetneq \dots \subsetneq \mathfrak{p}_m$ une chaîne de longueur m.

Soit $P \in \mathfrak{p}_1$ non nul. On pose $B = A/(P)$ qui est une k-algèbre de type fini engendré par les images x_i des X_i dans B.

De plus, les x_i sont liés par P. Par le lemme, il existe $y_1, \dots, y_{n-1} \in B$ tels que $k[y_1, \dots, y_{n-1}] \to B$ soit entière. Alors $\dim B = \dim k[y_1, \dots, y_{n-1}]$ et comme on a une surjection de $k[X_1, \dots, X_{n-1}]$ dans $k[y_1, \dots, y_{n-1}]$, $\dim B \leqslant \dim k[X_1, \dots, X_{n-1}] < n$.

Or $\mathfrak{p}_1/(P) \subsetneq \dots \subsetneq \mathfrak{p}_m/(P)$ est une suite de premiers de B de longueur $m-1$ donc $\dim B \geqslant m-1$.

On a donc bien $m \leqslant n$. Par récurrence, ça marche. ∎

COROLLAIRE 4.9 *Soit k un corps, A une k-algèbre de type fini. Soit $\mathfrak{m}$ un idéal maximal de $k[X_1, \dots, X_n]$.*

Alors $A/\mathfrak{m}$ est une extension finie de k. Si de plus k est algébriquement clos, $A/\mathfrak{m} \simeq k$.

Démonstration. Soit $L := A/\mathfrak{m}$ un corps. L est une k-algèbre de type fini donc il existe $a_1, \dots, a_n \in L$ tel que $k \hookrightarrow k[a_1, \dots, a_n] \hookrightarrow L$. $k[a_1, \dots, a_n]$ est une extension entière donc c'est un corps.

Alors $n = 0$ donc L/k est finie. ∎

Remarque 4.5 *Soit $\mathfrak{m}$ un idéal maximal. $k[X_1, \dots, X_n]/\mathfrak{m} \simeq k$ donc il existe $a_1, \dots, a_n \in k$ tel que $X_i = a_i \mod \mathfrak{m}$.*

Ainsi, $(X_1 - a_1, \dots, X_n - a_n) \subset \mathfrak{m}$ d'où l'égalité par maximalité de $(X_1 - a_1, \dots, X_n - a_n)$.

COROLLAIRE 4.10 *La dimension de toute k-algèbre de type fini est finie.*

4.5 Dimension d'un ensemble algébrique

Définition 4.14 Soit $V \subset k^n$ un ensemble algébrique.

$$\dim(V) = \sup\{r, \exists V_0 \subsetneq \ldots \subsetneq V_r \subset V, V_i \text{ irréductibles}\}$$

Proposition 4.7 Si k est algébriquement clos,

$$\dim V = \dim k[X_1, \ldots, X_n]/\mathcal{I}(V)$$

En particulier $\dim V < \infty$.

Démonstration. La correspondance entre les ensembles algébriques et les idéaux radicaux de $k[X_1, \ldots, X_n]$ donne une correspondance entre une chaine $V_i \subsetneq V_{i+1}$ et $\mathcal{I}(V_{i+1}) \subsetneq \mathcal{I}(V_i)$. ∎

Proposition 4.8

- Si $W \subset V$ alors $\dim W \leqslant \dim V$
- Si $V = \bigcup_{i=1}^{n} V_i$ est la décomposition en irréductibles alors $\dim V = \max \dim V_i$.

Exemple 4.6

- $I = \langle X^2YZ \rangle$, $\sqrt{I} = \langle XYZ \rangle$ donc $\nu(I) = \nu(XYZ) = H_x \cup H_y \cup H_z$ avec H_t le plan $t = 0$ de dimension 2 donc $\dim \nu(I) = 2$.
- $I = \langle X^2YZ, X^2Z^2, Y^2Z \rangle$, $\sqrt{I} = \langle XZ, YZ \rangle$ donc

  $$\nu(\sqrt{I}) = \nu(XZ) \cap \nu(YZ) = H_z \cup (H_x \cap H_y)$$

  Ainsi $\dim \nu(I) = 2$.

Proposition 4.9 Soit I un idéal monomial. $\nu(I)$ est une réunion finie de sous espaces coordonées de k^n (ie de la forme $H_{i_1} \cap \ldots H_{i_k}$).

Démonstration. $\nu(I) = \nu(m_1) \cap \ldots \nu(m_t)$ si $I = \langle m_1, \ldots, m_k \rangle$ et chaque $\nu(m_i) =$. ∎

Définition 4.15 Soit $I = \langle m_1, \ldots, m_t \rangle$ monomial propre.

Pour $j \in [\![1, t]\!]$, on pose $M_j = \{k, X_k \mid m_j\}$ ie $\nu(m_j) = \bigcup_{k \in M_j} H_k$.

Proposition 4.10

$$\dim(\nu(I)) = n - \min\{|J|, \forall j, J \cap M_j \neq \varnothing\}$$

Démonstration. $\nu(m_j) = \bigcup_{k \in M_j} H_k$ et $\nu(I) = \bigcap_{j=1}^{t} \nu(m_j)$.

Pour $J \subset [\![1, n]\!]$, soit $H_J = \bigcap_{k \in J} H_k$. Alors $H_J \subset m_j$ ssi $H_J \subset H_k$ pour un $k \in M_j$ ssi $J \cap M_j \neq \varnothing$.

Ainsi, si $J \cap M_j \neq \varnothing$ pour tout j alors $H_J \subset \nu(I)$ et $\dim \nu(I) \geqslant \dim H_j = n - |J|$.

D'autre part, $\nu(I) = V_1 \cup \ldots \cup V_m$ avec V_i de la forme H_{J_i} et

$$\dim(\nu(I)) = \max_i(\dim V_i) = n - \max\{|J_i|, J_i \cap M_j \neq \varnothing \forall j\}$$ ■

Lemme 4.6.1
$\forall j \in [\![1, t]\!]$, $J \cap M_j \neq \varnothing$ ssi $I \cap k[X_i, i \notin J] = (0)$.

Démonstration. Montrons que $J \cap M_j = \varnothing$ pour au moins un j ssi $I \cap k[X_i, i \notin J] \neq (0)$.

$I \cap k[X_i, i \notin J] \neq (0)$ ssi il existe $m \in k[X_i, i \notin J] \cap I$ ssi il existe $j \in [\![1, t]\!]$ tel que $m_j \mid m$ ssi il existe j tel que $m_j \in k[X_i, i \notin J]$.

Ceci est équivalent à l'existence de j tel que $J \cap M_j = \varnothing$. ■

Corollaire 4.11

$$\dim(\nu(I)) = \max\{r, \exists i_1, \ldots, i_r, I \cap k[X_{i_1}, \ldots, X_{i_r}] = (0)\}$$

4.6 Fonction de Hilbert

Définition 4.16 Soit $I \subset k[X_1, \ldots, X_n]$. Notons $k[X_1, \ldots, X_n]_{\leqslant s}$ l'ensemble des polynômes de degré total au plus s et $I_{\leqslant s} = I \cap k[X_1, \ldots, X_n]_{\leqslant s}$.

La fonction de Hilbert HF_I associe à s l'entier $\dim_k k[X_1, \ldots, X_n]_{\leqslant s} - \dim_k I_{\leqslant s}$.

Exemple 4.7

- Si $I = (0)$, $HF_I(s) = \dim k[X_1, \ldots, X_n]_{\leqslant s} = \binom{n+s}{n}$.
  En effet, si $n = 1$, c'est $s + 1$ (cardinal de $\{1, X, \ldots, X^s\}$).
  Par récurrence, si c'est vrai pour $n - 1$, on prend $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ avec $\alpha_1 + \ldots + \alpha_n \leqslant s$ et
  $$HF_{I,n}(s) = \sum_{\alpha_1=0}^{s} HF_{I,n-1}(s - \alpha_i) = \sum_{\alpha_1=0}^{s} \binom{s - \alpha_1 + (n-1)}{n-1} = \binom{s+n}{n}$$
- Si $I = \langle X^\alpha \rangle$.
  $$\dim I_{\leqslant s} = \begin{cases} 0 & \text{si } s < |\alpha| \\ HF_{(0)}(s - |\alpha|) = \binom{n+s-|\alpha|}{n} & \text{sinon} \end{cases}$$

- Soit $I = \langle X^2Y^4, X^4Y^2\rangle$. On note $m_1 = X^2Y^4$, $m_2 = X^4Y^2$. On a $\langle m_1\rangle \cap \langle m_2\rangle = \langle X^4Y^4\rangle$ donc :

$$\dim I_{\leqslant s} = \dim\langle m_1\rangle_{\leqslant s} + \dim\langle m_2\rangle_{\leqslant s} - \dim\langle X^4Y^4\rangle_{\leqslant s} = \frac{s^2 - 5s - 2}{2}$$

Définition 4.17 Soit $C(I) = \{\alpha, X^\alpha \notin I\}$. Soit $(e_1, \ldots, e_n)$ base canonique de $\mathbb{N}^n$.

On note $[e_{i_1}, \ldots, e_{i_r}] = \{a_1e_{i_1} + \ldots + a_re_{i_r}, a_j \in \mathbb{N}, 1 \leqslant j \leqslant r\}$

Si $\alpha \notin [e_{i_1}, \ldots, e_{i_r}]$ alors on note

$$\alpha + [e_{i_1}, \ldots, e_{i_r}] = \{\alpha + \beta, \beta \in [e_{i_1}, \ldots, e_{i_r}]\}$$

Proposition 4.11 Soit I un idéal monomial propre.

(i) $C(I) = T_1 \cup \ldots \cup T_n$ avec T_i une translation d'un sous-espace coordonnée de $\mathbb{N}^n$

(ii) $\dim(\nu(I)) = \max_i \dim T_i$

THÉORÈME 4.7 *Soit I monômial propre.*

(i) *Pour $s \gg 0$, $HF_I(s)$ est un polynôme en s noté HP_I*

(ii) $\dim \nu(I) = \deg HP_I(s)$.

Démonstration. $HF_I(s) = |C(I)_{\leqslant s}|$. Or $C(I) = T_1 \cup \ldots \cup T_m$ donc

$$|C(I)_{\leqslant s}| = \sum_{k=1}^{n} (-1)^k \sum_{i_1 < \ldots < i_k} |(T_{i_1})_{\leqslant s} \cap \ldots \cap (T_{i_k})_{\leqslant s}|$$

Si $T_i \neq T_j$, $T_i \cap T_j$ est soit vide, soit une translation d'un sous-espace coordonnée de simension inférieure à $\max\{\dim T_i, \dim T_j\}$.

Pour $s \gg 0$, $|C(I)_{\leqslant s}|$ est un polynôme en s de degré $\max(\deg((T_i)_{\leqslant s})) = \dim \nu(I)$. ∎

Définition 4.18 Un ordre monomial sur $\mathbb{N}^n$ est dit gradué ssi $|\alpha| > |\beta|$ implique $X^\alpha > X^\beta$.

THÉORÈME 4.8 *Fixons un ordre gradué et I un idéal de $k[X_1, \ldots, X_n]$.*

On a $HF_I = HF_{\langle \mathrm{LT}(I)\rangle}$.

Démonstration. $\langle \mathrm{LT}(I)\rangle_{\leqslant s} = \{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\}$ qui est donc une base de $\langle \mathrm{LT}(I)\rangle_{\leqslant s}$ sur k.

Pour conclure, on montre que $\{f_1, \ldots, f_m\}$ est une base pour $I_{\leqslant s}$. Ils sont linéairement indépendants car les monômes dominants le sont. Soit $f \in I_{\leqslant s} \setminus \mathrm{Vect}\{f_1, \ldots, f_m\}$ de degré minimal.

$\mathrm{LT}(f) \in \langle \mathrm{LT}(I)\rangle_{\leqslant s}$ donc $\mathrm{LT}(f) = a_1 \mathrm{LM}(f_1) + \ldots + a_m \mathrm{LM}(f_m)$.

Alors $f - (a_1f_1 + \ldots + a_mf_m) \in I_{\leqslant s} \setminus \mathrm{Vect}\{f_1, \ldots, f_m\}$ de degré inférieur à $\deg(f)$. Absurde. On a donc $I_{\leqslant s} = \mathrm{Vect}\{f_1, \ldots, f_m\}$. ∎

THÉORÈME 4.9 *Soit $I \subset k[X_1, \dots, X_n]$ propre.*
Soit $A = k[X_1, \dots, X_n]/I$. Alors $\deg(HP_I) = \dim A = \dim \nu(I)$ si k est algébriquement clos

Démonstration.

- On montre que $\dim A \leqslant \deg HP_I$. Par le lemme de normalisation, il existe $a_1, \dots, a_d \in A$ algébriquement indépendants tels que l'injection $\iota : k[a_1, \dots, a_d] \to A$ soit entière.
  Soit $f_i \in k[X_1, \dots, X_n]$ qui annule les $\iota(a_i)$

  $$k[f_1, \dots, f_d] \cap I = (0)$$

  car si $P \in I$, $P(\iota(a_1), \dots, \iota(a_d)) = 0$ dans A, ce qui est absurde.
  Notons N le maximum des degrés totaux des f_i. $\{f_1^{\alpha_1} \dots f_d^{\alpha_d}, \alpha_1 + \dots + \alpha_d \leqslant s\}$ est un sous-ensemble de $k[X_1, \dots, X_n]_{\leqslant Ns}$ composé de polynômes linéairement indépendants dans $k[X_1, \dots, X_n]_{\leqslant Ns}/I_{\leqslant Ns}$.
  Ainsi, $HF_I(SN) \geqslant \text{Card}\{(\alpha_1, \dots, \alpha_d), \alpha_1 + \dots + \alpha_d \leqslant s\} = \binom{d+s}{s}$ donc $\deg HP_I \geqslant d = \dim A$.
- On montre que

  $$\begin{aligned}\dim A \geqslant \deg HP_I &= \deg HP_{\langle \text{LT}(I)\rangle} \\ &= \max\{r, \exists i_1, \dots, i_r, k[X_{i_1}, \dots, X_{i_r}] \cap \langle \text{LT}(I)\rangle = (0)\}\end{aligned}$$

  Si $\exists i_1, \dots, i_r, k[X_{i_1}, \dots, X_{i_r}] \cap \langle \text{LT}(I)\rangle = (0)$, alors il existe une injecton de $k[X_{i_1}, \dots, X_{i_r}] \to A$. Le lemme suivant conclut. ∎

Lemme 4.9.1
Si A est une k-algèbre de type finie et si on a une injection de $k[X_1, \dots, X_r] \to A$ alors $\dim A \geqslant r$.

Démonstration. Par le lemme de normalisation, il existe $a_1, \dots, a_d \in A$ tel que $k[a_1, \dots, a_d] \to A$ soit entière. On montre que $d \geqslant r$.

Montrons qu'il existe i tel que $\{a_i, X_2, \dots, X_r\}$ soient algébriquement indépendants. Par symétrie, on pourra supposer $i = 1$ et en réappliquant le résultat, on aura $\{a_1, a_2, X_3, \dots, X_r\}$ indépendants donc finalement on aura $\{a_1, \dots, a_r\}$ indépendants, d'où $d \geqslant r$.

Par l'absurde, si pour tout i, $\{a_i, X_2, \dots, X_r\}$ est liées alors

$$P_{m,i}(X_2, \dots, X_r)a_i^m + \dots + P_{0,i}(X_2, \dots, X_r) = 0$$

Soit $S = k[X_2, \dots, X_r] \setminus \{0\}$. a_i sont entiers dans $k(X_2, \dots, X_r)$ donc $A[S^{-1}]$ est entier sur $k(X_2, \dots, X_r)$ donc X_1 est entier sur $k(X_2, \dots, X_r)$, ce qui est absurde. ∎

COROLLAIRE 4.12 *On prend un ordre gradué. Alors* $\dim k[X_1, \ldots, X_n]/I = \dim k[X_1, \ldots, X_n]/\langle \mathrm{LT}(I) \rangle$.

COROLLAIRE 4.13

(i) *Soit* $f \in k[X_1, \ldots, X_n]$ *non constant. Alors* $\dim k[X_1, \ldots, X_n]/\langle f \rangle = n - 1$.

(ii) *Pour tout idéal premier* $\mathfrak{p}$ *de hauteur* 1, $\dim k[X_1, \ldots, X_n]/\mathfrak{p} = n - 1$.

Démonstration.

(i) $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f) \rangle$ avec $\mathrm{LT}(f)$ non constant. Or

$$\dim k[X_1, \ldots, X_n]/\langle \mathrm{LT}(f) \rangle = n - 1$$

Donc $\dim k[X_1, \ldots, X_n]/I = 1$.

(ii) $k[X_1, \ldots, X_n]$ est factoriel. Soit $f \in \mathfrak{p}$ non constant. f se décompose en irréductibles sous la forme $f_1^{a_1} \ldots f_d^{a_d}$.
Comme $\mathfrak{p}$ est premier, il existe i tel que $f_i \in \mathfrak{p}$. Alors $0 \subsetneq \langle f_i \rangle \subset \mathfrak{p}$ donc $\mathfrak{p} = \langle f_i \rangle$. Le premier point conclut alors. ∎

Remarque 4.6 Le point (ii) est vrai pour une k-algèbre de type fini. On a $\dim(A/\mathfrak{p}) = n - 1$ *si* $\mathrm{ht}(\mathfrak{p}) = 1$. *Plus généralement,* $\dim A/\mathfrak{p} = n - r$ *si* $\mathrm{ht}(\mathfrak{p}) = r$.

Définition 4.19 Un anneau est dit caténaire ssi $\dim A/\mathfrak{p} + \dim \mathfrak{p} = \dim A$ pour tout $\mathfrak{p}$.

COROLLAIRE 4.14 *Soient* A, B *deux k-algèbres de type fini. Si* $A \hookrightarrow B$ *alors* $\dim A \leqslant \dim B$.

Chapitre 5

Introduction au langage des schémas

5.1 Spectre d'un anneau

A sera un anneau commutatif non nul.

Définition 5.1 Spec(A) est muni de la topologie de Zariski. Les fermés sont les $V(I) = \{\mathfrak{p} \in \text{Spec}(A), I \subset \mathfrak{p}\}$.

On note $D(I) = V(I)^c$. En particulier, $D(f) = \{\mathfrak{p}, f \notin \mathfrak{p}\}$.

Lemme 5.0.2

(i) Les ouverts $D(f)$ forment une base de la topologie

(ii) Les $D(f_i)$ recouvrent Spec(A) ssi $1 \in \langle f_i, i \in I\rangle$

(iii) $D(f)$ est isomorphe à Spec(A_f)

Démonstration.

(i) Soit U ouvert et $\mathfrak{p} \in U = V(I)^c$. On a $I \not\subset \mathfrak{p}$ donc il existe $f \in I$ tel que $f \notin \mathfrak{p}$ et $\mathfrak{p} \in D(f) \subset I$.
Alors $V(I) \subset V(f)$ donc $D(f) \subset U$.

(ii) $\bigcup_i D(f_i) = V(\langle f_i, i \in I\rangle)^c$. Ainsi, l'union vaut Spec(A) ssi $V(\langle f_i, i \in I\rangle) = \varnothing$ ssi $1 \in \langle f_i, i \in I\rangle$.

(iii) $D(f) = \{\mathfrak{p}, f \notin \mathfrak{p}\} = \{\mathfrak{p}, \mathfrak{p} \cap S = \varnothing\} = \text{Spec}(A_f)$ et si f est nilpotent, $A_f = 0$ et $D(f) = \varnothing$. ∎

Corollaire 5.1 Spec(A) *est quasi-compact.*

Démonstration. Soit $\bigcup_{i\in I} D(f_i)$ un recouvrement ouvert de $\mathrm{Spec}(A)$. Par (ii), $1 \in \langle f_i, i \in I\rangle$.

On écrit donc $1 = \sum_{i=1}^{d} a_i f_i$ donc $1 \in \langle f_1, \dots, f_d\rangle$ donc $\mathrm{Spec}(A) = \bigcup_{i=1}^{d} D(f_i)$. ■

COROLLAIRE 5.2 *$D(f)(\simeq \mathrm{Spec}(A_f))$ est quasi-compact.*

Proposition 5.1 Si $V(I_1) \subset V(I_2)$ alors $\sqrt{I_1} \supset \sqrt{I_2}$.

Lemme 5.0.3
Soit $f : A \to B$. Alors $f^{\#} : \mathrm{Spec}\, B \to \mathrm{Spec}\, A$, $q \mapsto f^{-1}(q)$ est continue pour la topologie de Zariski.

5.2 Faisceaux

Définition 5.2

(i) Soit X un espace topologique. Un préfaisceau F sur X est la donnée de
- Pour tout ouvert U de X, un ensemble $F(U)$
- Pour tout $V \subset U$ ouvert, une application $\gamma_{UV} : F(U) \to F(V)$ tel que $\gamma_{UU} = \mathrm{Id}$ et $\gamma_{UW} = \gamma_{VW} \circ \gamma_{UV}$ si $W \subset V \subset U$. (on note $f|_V = \gamma_{UV}(f)$.)

(ii) On dit que F est un faisceau ssi
- Pour tout ouvert $U = \bigcup_i U_i$, si $f \in F(U)$ vérifie $f|_{U_i} = g|_{U_i}$ pour tout i alors $f = g$.
- Soit $f_i \in \prod_i F(U_i)$ tel que $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ alors il existe (un unique par ce qui précède) $f \in F(U)$ tel que $f|_{U_i} = f_i$ pour tout i.

Exemple 5.1 Les fonctions lisses analytiques forment un faisceau pour $\gamma_{UV}(f) = f|_V$.

Les fonctions continues bornées forment un préfaisceau qui n'est pas un faisceau : en effet, $\mathbb{R} = \bigcup_{i\in\mathbb{N}} [-i, i]$. La fonction $x \mapsto x$ est bornée sur $[-i, i]$ mais il n'y a pas de f bornée tel que $f|_{[-i,i]} = x$ pour tout i.

Définition 5.3 La fibre de F en $x \in X$ est F_x la limite inductive des $F(U)$ pour les U contenant x, ie

$$\bigcup_{x\in U} F(U)/\sim$$

où $F(U_1) \ni a \sim b \in F(U_2)$ ssi il existe $U_3 \subset U_1 \cap U_2$ tel que $a|_{U_3} = b|_{U_3}$.

Définition 5.4 Soit F et G deux (pré)faisceaux sur X. Un morphisme $\varphi : F \to G$ est la donnée pour tout U d'une application $\varphi_U : F(U) \to G(U)$ qui est compatible avec les restrictions : $\varphi_V \circ \gamma^F_{UV} = \gamma^G_{UV} \circ \varphi_U$.

Définition 5.5 Soit $f : X \to Y$ continue. Si F est un faisceau sur X, on définit f_*F sur Y par $f_*F : U \to F(f^{-1}(U))$ qui est un faisceau sur Y.

Remarque 5.1 Soit G un faisceau sur Y. L'image inverse $f^{-1}G$ est le fasiceau associé au préfaisceau $f^{-1}G(U) = \lim\limits_{f(U)\subset V} G(V)$.

Définition 5.6 On définit un faisceau sur $\mathrm{Spec}(A)$ en disant que pour tout U ouvert, on prend

$$O_{\mathrm{Spec}(A)}(U) = \left\{ (S_\mathfrak{p}) \in \prod_{\mathfrak{p}\in U} A_\mathfrak{p}, \forall \mathfrak{p} \in U, \exists V, a, f \text{ tel que } \mathfrak{p} \in V \subset U, f \notin \mathfrak{p} \text{ et } \frac{a}{f} \in A_q \forall q \in V \cap D(f) \right\}$$

Lemme 5.0.4
C'est un faisceau. On l'appelle faisceau structurel de $\mathrm{Spec}(A)$. On note souvent $O = O_{\mathrm{Spec}(A)}$.

Un élément de $O(U)$ s'appelle une section.

Proposition 5.2

(i) $O(D(f)) \simeq A_f$

(ii) $O_\mathfrak{p} \simeq A_\mathfrak{p}$

Démonstration.

(i) Il s'agit de montrer que si $D(f_i)$ est un recouvrement fini de $D(f) = \mathrm{Spec}(A)$ et si $s = \frac{a_i}{f_i}$ sur $D(f_i)$ alors $s = \frac{a}{f}$ pour un certain $a \in A$.
On définit un morphime (bien défini)

$$\begin{cases} A_f & \to & O(D(f)) \\ \frac{a}{f^m} & \mapsto & \frac{a}{f^m} \end{cases}$$

Ce morphisme est bien défini et injectif car si $\frac{a}{f^m} = 0$ dans tous les $A_\mathfrak{p}$ pour $\mathfrak{p} \in D(f)$, alors il existe $s \notin \mathfrak{p}$ tel que $sa = 0$ (pour tout $\mathfrak{p} \in D(f)$).
Notons $I = (0 : a)$ l'idéal annulateur de $a \in A$. Alors si $s \in I$ et $s \notin \mathfrak{p}$ alors $\mathfrak{p} \notin V(I)$ donc $V(I) \subset V(f)$ donc $\sqrt{(f)} \subset \sqrt{I}$.
Il existe donc $n \geqslant 1$ tel que $f^n \in I$ et $f^n a = 0$ dans A donc $a = 0$ dans A_f.
Si $s_i = \frac{a_i}{f_i}$ sur chaque $D(f_i)$ on a $s_i|_{D(f_i)\cap D(f_j)} = s_j|_{D(f_i)\cap D(f_j)}$.

On a alors $\frac{a_i}{f_i} = \frac{a_j}{f_j}$ sur $D(f_i) \cap D(f_j)$ donc par injectivité, $\frac{a_i}{f_i} = \frac{a_j}{f_j}$ sur $A_{f_i f_j}$.
Il existe donc n_i tel que $(f_i f_j)^{n_i}(a_i f_j - a_j f_i) = 0$. Soit $n = \max n_i$. On a alors

$$(f_i f_j)^n (a_i f_j - a_j f_i) = 0$$

Donc $(a_i f_i^n) f_j^{n+1} - (a_j f_j^n) f_i^{n+1} = 0$. Or $s_i = \frac{a_i}{f_i} = \frac{a_i f_i^n}{f_i^{n+1}} \in O(D(f_i))$ (égalité dans chaque $A_\mathfrak{p}$, $\mathfrak{p} \in D(f_i)$). quitte à remplacer f_i^{n+1} par f_i ($D(f_i) = D(f_i^{n+1})$), on peut supposer $s_i = \frac{a_i}{f_i}$ avec $a_i f_j = a_j f_i$.
Comme $D(f) = \bigcup_{i=1}^{r} D(f_i)$, $\sqrt{f} = \sqrt{\langle f_i, i \leqslant r \rangle}$. Il existe donc N tel que $f^N = \sum_{i=1}^{r} b_i f_i =: a$ avec $b_i \in A$. Alors

$$f_j a = \sum_{i=1}^{r} b_i a_i f_j = \left(\sum_{i=1}^{r} b_i f_i \right) a_j = f^N a_j$$

Donc $\frac{a}{f^N} = \frac{a_j}{f_j}$, ce qui donne la surjectivité.

(ii) On prend le morphisme $\varphi : O_\mathfrak{p} \to A_\mathfrak{p}$ qui à $\overline{s}$ associe $s_\mathfrak{p}$. Il est bien défini car si $\overline{s} = \overline{s'}$ alors il existe $U'' \subset U \cap U'$ tel que $s|_{U''} = s'|_{U''}$ donc pour tout $\mathfrak{p} \in U''$, $s_\mathfrak{p} = s'_\mathfrak{p}$.
Ce morphisme est surjectif : tout élément de $A_\mathfrak{p}$ s'écrit $\frac{a}{f}$ avec $f \notin \mathfrak{p}$ donc $D(f)$ est un ouvert contenant $\mathfrak{p}$ et $\frac{a}{f} \in O(D(f))$ s'envoie donc sur $\frac{a}{f}$.
Pour l'injectivité, il faut montrer que si $s_1 \in O(U_1)$ et $s_2 \in O(U_2)$ sont tels que $\varphi(\overline{s_i}) = \varphi(\overline{s_2})$ dans $A_\mathfrak{p}$ alors il existe $U_3 \subset U_1 \cap U_2$ tels que $s_1 = s_2$ sur U_3.
On peut supposer $U_i = D(f_i)$ et $s_i = \frac{a_i}{f_i}$. Par hypothèse, $\frac{a_1}{f_1} = \frac{a_2}{f_2}$ dans $A_\mathfrak{p}$ donc il existe $k \notin \mathfrak{p}$ tel que $k(a_1 f_2 - a_2 f_1) = 0$ dans A.
Pour tout $q \in D(f_1) \cap D(f_2) \cap D(k) =: U_3$ et on a $\frac{a_1}{f_1} = \frac{a_2}{f_2}$ dans A_q donc $s_1 = s_2$ sur U_3 ce qui prouve l'injectivité. ∎

Remarque 5.2 On a deux applications

$$d_0 : \begin{cases} O(U) & \to & \prod_i O(U_i) \\ s & \mapsto & (s|_{U_i})_i \end{cases}$$

et

$$d_1 : \begin{cases} \prod_i O(U_i) & \to & \prod_{i,j} O(U_i \cap U_j) \\ (s_i)_i & \mapsto & s_i|_{U_i \cap U_j} - s_j|_{U_i \cap U_j} \end{cases}$$

d_0 est injectif car si $s = s'$ sur tous les U_i, $s = s'$.

De plus, $\mathrm{Ker}(d_1) = \mathrm{Im}(d_0)$ *car si* $d_1(s_i) = 0$ *alors il existe* $s \in O(U)$ *avec* $d_0(s) = (s_i)_i$ *ie* $s|_{U_i} = s_i$.

Définition 5.7 Si U est quelconque, on prend $(D(f_i))$ un recouvrement de U et on définit $O(U)$ comme $\mathrm{Ker}(d_1)$ où $d_1 : \prod_i A_{f_i} \to \prod_{i,j} A_{f_i f_j}$.

Définition 5.8 Soit (X, F) un faisceau. Les éléments de $F(U)$ sont appelés sections sur U ou fonctions régulières sur U. Un élément de $F(X)$ est appelé section globale.

5.3 Schémas

Définition 5.9 On appelle espace annelé la donné d'un espace topologique X et d'un faisceau O_X d'anneaux : pour tout U, $O_X(U)$ est un anneau et pour tout $V \subset U$, $O_X(U) \to O_X(V)$ est un morphisme d'anneaux.

Un espace localement annelé est un espace annelé où les tiges sont des anneaux locaux.

Définition 5.10 Soit A, B deux anneaux locaux. Un morphisme $\varphi : A \to B$ est dit local ssi il envoie l'unique idéal maximal de A sur celui de B.

Définition 5.11 Soient (X, O_X) et (Y, O_Y) deux espaces localement annelés. $(f, f^\#)$ est un morphisme de $(X, O_X) \to (Y, O_Y)$ ssi f est continue, $f^\#$ est un morphisme de faisceaux et pour tout x, $O_{y,f(x)} \to O_{X,x}$ est un morphime local.

Proposition 5.3

(i) Soit $A \to B$ un morphisme d'anneaux. Alors $(\mathrm{Spec}(B), O_{\mathrm{Spec}(B)}) \to (\mathrm{Spec}(A), O_{\mathrm{Spec}(A)})$ est une morphisme d'espaces annelés.

(ii) Tout morphisme d'espaces localement annelés $(\mathrm{Spec}(B), O_{\mathrm{Spec}(B)}) \to (\mathrm{Spec}(A), O_{\mathrm{Spec}(B)})$ provient d'un morphisme d'anneaux.

Démonstration.

(i) Soit $\varphi : A \to B$. Alors $f := \varphi^{-1}$ est continue de $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$. $f^\# : A_h \to B_{f(h)}$ est un morphisme de faiceaux et pour tout $\mathfrak{p} \in \mathrm{Spec}(B)$,

(ii) Soit $(f, f^\#)$. Par définition, il existe une morphisme de $O_{\mathrm{Spec}(A)}(A) \to O_{\mathrm{Spec}(B)}(\mathrm{Spec}(B))$ donc de $A \to B$.
Il faut vérifier que φ induit $(f, f^\#)$. Soit $\mathfrak{p} \in \mathrm{Spec}(B)$. Par hypothèse, on dispose d'un morphisme de $f^\#_{\mathfrak{p}} : A_{f(\mathfrak{p})} \to B_{\mathfrak{p}}$ et un diagramme commutatif qui donne $f = \varphi^{-1}$. ∎

Exemple 5.2 Soit R un anneau local intègre de dimension 1. $\mathrm{Spec}(R) = \{x_0, x_1\}$. Les tiges sont $R_{x_0} = R_{\mathfrak{m}} = R$ et $R_{x_1} = R_{(0)} = \mathrm{Frac}(R)$.

L'inclusion $R \subset K := \mathrm{Frac}(R)$ induit un morphisme $\mathrm{Spec}(K) = \{y\} \to \mathrm{Spec}(R)$ qui envoie y sur x_1. (on ne peut pas envoyer y sur x_0 sinon $f_y^{\#}$ ne serait pas un morphisme local).

Définition 5.12 Un schéma est un espace localement annelé (X, O_X) qui est isomorphe à $(\mathrm{Spec}(A), O_{\mathrm{Spec}(A)})$ pour un certain A.

Un schéma est affine ssi c'est un espace localement annelé tel qu'on ait un recouvrement U_i de X tel que $(U_i, O_X|_{U_i})$ soit affine, ie

$$\forall x \in X, \exists U \ni x \text{ ouvert }, (U, O_X|_U) \text{ est affine}$$

Proposition 5.4 Soit X un schéma, A un anneau. On a une bijection entre l'ensemble des morphismes de $X \to \mathrm{Spec}(A)$ dans les morphismes d'anneaux de $A \to O_X(X)$.

