Algèbre commutative
Master

Charles De Clercq, Matteo Tamiozzo

Table des matières

1 Idéaux et spectre d'un anneau

1.1 Introduction

On suppose connue la notion d'anneau et de morphisme d'anneaux. Sauf mention contraire, tout anneau dans ce texte et commutatif et unitaire, et tout morphisme d'anneaux $f : A \to B$ envoie l'identité (multiplicative) de A sur celle de B.

L'algèbre commutative, i.e. l'étude des propriétés des anneaux, a été développée à partir du 19ème siècle. Une motivation fondamentale était l'exemple concret des l'anneaux $\mathbb{Z}[e^{2\pi i/p}] \subset \mathbb{C}$, utilisés par Kummer pour essayer de montrer le dernier théorème de Fermat. Les propriétés de ces anneaux furent étudiées plus en détail par Dedekind, qui comprit que les mêmes idées pouvaient être utiles pour développer la théorie des surfaces de Riemann de façon purement algébrique. Plus tard, au 20ème siècle, l'algèbre commutative est devenue l'outil de base pour l'étude des variétés algébriques, jouant un rôle analogue à celui de l'analyse (en plusieurs variables) dans l'étude des variétés différentielles. Dans ce cours, on expliquera les bases de l'algèbre commutative en essayant de mettre en évidence sa relation avec la géométrie. L'idée guide est la suivante.

Penser aux anneaux non pas comme à des objets "abstraits", mais plutôt comme à des anneaux de fonctions sur des espaces géométriques.

Par exemple (pour $k = \mathbb{R}$ ou $\mathbb{C}$).

$k[X]$	fonctions (polynomiales) $k \to k$
$k[X_1, \ldots, X_n]$	fonctions $k^n \to k$
$\{\frac{P(X)}{X^d}, P(X) \in k[X], d \geq 0\}$	fonctions $k \smallsetminus \{0\} \to k$
?	fonctions $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \to \mathbb{R}$
$\mathbb{Z}$	?

On va s'intéresser à l'interaction entre propriétés algébriques des anneaux et propriétés géométriques des espaces correspondants. Voici deux exemples.

— Les espaces $\mathbb{C}$ et $\mathbb{C}^\times$ ne sont pas "le mêmes" (ils ne sont pas homéomorphes). Du côté algébrique, montrer qu'il n'existe pas d'isomorphisme entre anneaux dans la première et troisième ligne ci-dessus qui soit l'identité sur $k = \mathbb{C}$. D'autre part, quelle est la relation entre l'anneau des fonctions polynomiales sur $\mathbb{C} \smallsetminus \{0\}$ et celui des fonctions polynomiales sur le cercle complexe $\{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = 1\} \subset \mathbb{C}^2$?

— Quelle est l'"incarnation algébrique" du ruban de Möbius ?

1.2 Anneaux et idéaux

Soit $(A, +, \cdot, 0, 1)$ un anneau. On rappelle la terminologie suivante.

— Un élément $a \in A \smallsetminus \{0\}$ est un diviseur de zéro s'il existe $b \in A \smallsetminus \{0\}$ tel que $ab = 0$.

— Un élément $a \in A$ est nilpotent s'il existe un entier $n \geq 0$ tel que $a^n = 0$. On dit que A est un anneau réduit si le seul élément nilpotent de A est 0.

— A est un anneau intègre si $1 \neq 0$ et A n'a pas de diviseur de zéro, c'est-à-dire,

$$\forall a, b \in A \smallsetminus \{0\}, ab \neq 0.$$

— Un élément $a \in A$ est une unité s'il existe $b \in A$ tel que $ab = 1$. L'ensemble des unités de A muni de la multiplication $\cdot$ est un groupe abélien, noté $A^\times$.

— A est un corps si $1 \neq 0$ et $A \smallsetminus \{0\} = A^\times$, i.e.

$$\forall a \in A \smallsetminus \{0\}, \exists b \in A : ab = 1.$$

Exemple 1.1. *(Certaines preuves en TD)*

(i) L'anneau $\mathbb{Z}$ est intègre, et $\mathbb{Z}^\times = \{\pm 1\}$. L'anneau

$$\mathbb{Q} = \left\{ \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z} \smallsetminus \{0\} \right\}$$

est un corps ; on remarque que tout corps contenant $\mathbb{Z}$ contient forcement $\mathbb{Q}$.

(ii) Si k est un corps, alors l'anneau $A = k[X]$ des polynômes en X à coefficients dans k est un anneau intègre, et $A^\times = k^\times$.

(iii) Plus généralement, pour tout anneau intègre A, l'anneau $A[X]$ est intègre. En particulier, $k[X_1, \ldots, X_n]$ est un anneau intègre pour tout corps k et tout entier $n \geq 1$.

(iv) Soit k un corps, et $A = \{a + b\varepsilon, a, b \in k, \varepsilon^2 = 0\}$. L'élément $\varepsilon \in A$ est nilpotent ; de plus, $A^\times = \{a + b\varepsilon, a, b \in k, a \neq 0\}$.

Corps des fractions. On peut associer à tout anneau intègre A un corps $K(A)$, appelé le corps des fractions de A ; c'est le plus petit corps contenant A. Sa construction généralise la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$. Précisément, on définit

$$K(A) = \{(a, b), a \in A, b \in B \setminus \{0\}\}/\sim$$

où $(a, b) \sim (a', b')$ si $ab' = a'b$. On définit la somme par $(a, b) + (a', b') = (ab' + a'b, bb')$ et le produit par $(a, b) \cdot (a', b') = (aa', bb')$. On vérifie que ces formules munissent $K(A)$ d'une structure de corps, et que l'application $A \to K(A)$ qui envoie a sur $(a, 1)$ est un morphisme injectif d'anneaux.

Par exemple, pour $A = \mathbb{Z}$ on obtient $K(A) = \mathbb{Q}$, et pour $A = k[X]$, où k est un corps, on obtient $K(A) = k(X) = \{P(X)/Q(X), P(X), Q(X) \in k[X], Q(X) \neq 0\}$. On verra plus tard une généralisation de cette construction, la localisation d'un anneau.

Idéaux. Considérons la parabole $C \subset \mathbb{R}^2$ d'équation $x = y^2$. On se propose de décrire l'anneau A_C des fonctions polynomiales $C \to \mathbb{R}$. Une telle fonction f envoie $(x, y) \in C$ sur $P(x, y)$, pour un certain $P(X, Y) \in \mathbb{R}[X, Y]$. D'autre part, pour tout $Q(X, Y) \in \mathbb{R}[X, Y]$, le polynôme $P(X, Y)+Q(X, Y)\cdot(X-Y^2)$ donne lieu aussi à la fonction f. Dans l'anneau A_C, on doit donc identifier $P(X, Y)+Q(X, Y)\cdot(X-Y^2)$ avec $P(X, Y)$. Pour ce faire, on introduit la notion d'idéal et anneau quotient.

Définition 1.2. *Soit A un anneau. Un idéal $I \subset A$ est un sous-groupe de $(A, +)$ tel que pour tout $a \in A$, si $i \in I$ alors $ai \in I$.*

Opérations avec les idéaux. Soit A un anneau.

Idéaux principaux et de type fini : Si $a \in A$, l'ensemble $(a) = \{ab, b \in A\}$ des multiples de a est un idéal, appelé l'idéal principal engendré par a. Un anneau intègre A dont tout idéal est principal est appelé anneau principal.

Somme : si $I_1, \ldots, I_k \subset A$ sont des idéaux, alors $I_1 + \cdots + I_k = \{i_1 + \cdots + i_k, i_i \in I_i \text{ pour } 1 \leq i \leq k\} \subset A$ est un idéal. Si $a_1, \ldots, a_k \in A$, on note $(a_1, \ldots, a_k) = (a_1) + \cdots + (a_k)$.

Produit : si $I_1, \ldots, I_k \subset A$ sont des idéaux, le sous-groupe additif de A engendré par les éléments $i_1 i_2 \cdots i_k$, avec $i_i \in I_i$ pour $1 \leq i \leq k$, est un idéal noté $I_1 I_2 \cdots I_k$.

Lemme 1.3.

1. *Soit $f : A \to B$ un morphisme d'anneaux. Le noyau* $\ker(f) = \{a \in A \mid f(a) = 0\}$ *est un idéal de A.*

2. *Soit A un anneau et $I \subset A$ un idéal. Il existe une unique structure d'anneau sur le groupe additif quotient A/I telle que la projection $q : A \to A/I$ soit un morphisme d'anneaux. De plus, pour tout anneau B,*

$$\begin{array}{ccc} \{\bar{f} : A/I \to B\} & \longrightarrow & \{f : A \to B \ t.q.\ I \subset \ker(f)\} \\ \bar{f} & \longmapsto & \bar{f} \circ q \end{array}$$

est une bijection.

3. *Soit A un anneau, $I \subset A$ un idéal et $q : A \to A/I$ la projection. Pour tout idéal $\bar{J} \subset A/I$, l'image réciproque $q^{-1}(\bar{J}) \subset A$ est un idéal, et*

$$\begin{array}{c} \{\text{idéaux de } A/I\} \to \{\text{idéaux } I \subset J \subset A\} \\ \bar{J} \mapsto q^{-1}(\bar{J}) \end{array}$$

est une bijection.

Démonstration. 1. Si $a, b \in \ker(f)$, alors $f(a+b) = f(a) + f(b) = 0$ donc $a + b \in \ker(f)$. Si $b \in \ker(f)$ et $a \in A$ alors $f(ab) = f(a)f(b) = 0$ donc $ab \in \ker(f)$.

2. Pour que q soit un morphisme d'anneaux il faut que les lois $\bar{+}, \bar{\cdot}$ sur A/I soient définies par $q(a)\bar{+}q(b) = q(a+b)$ et $q(a)\bar{\cdot}q(b) = q(ab)$. On vérifie que ces lois sont bien définies, et que $(A/I, \bar{+}, \bar{\cdot}, q(0), q(1))$ est un anneau. Par exemple, vérifions que $\bar{\cdot}$ est bien définie (les autres vérifications sont laissées au lecteur). Soient $a, b \in A$ et $i_1, i_2 \in I$. Alors

$$q(a+i_1)\bar{\cdot}q(b+i_2) = q((a+i_1)\cdot(b+i_2)) = q(ab + ai_2 + bi_1 + i_1 i_2) = q(ab)$$

où la dernière égalité découle du fait que $ai_2 + bi_1 + i_1 i_2 \in I$.
Enfin, l'application $\bar{f} \mapsto \bar{f} \circ q$ est injective car q est surjective. Si $f : A \to B$ est un morphisme tel que $I \subset \ker(f)$, on vérifie que l'application $\bar{f} : A/I \to B$ qui envoie $q(a)$ sur $f(a)$ est bien définie, et est un morphisme d'anneaux tel que $f = \bar{f} \circ q$.

3. Les idéaux de A/I sont les noyaux $\ker \bar{f}$ des morphismes $\bar{f} : A/I \to B$; d'après le point précédent, ils correspondent aux noyaux $q^{-1}(\ker(\bar{f}))$ des morphismes $f = \bar{f} \circ q : A \to B$, i.e. aux idéaux $I \subset J \subset A$.

□

Exemple 1.4. *(Certaines preuves en TD)*

— *$\mathbb{Z}$ est un anneau principal ; si k est un corps, alors $k[X]$ est un anneau principal. Dans les deux cas, la preuve repose sur l'algorithme d'Euclide.*

— *L'anneau $\mathbb{C}[X, Y]$ n'est pas principal : par exemple, l'idéal (X, Y) n'est pas principal.*

— *Soit k un corps, $A = k[X]$ et $I = (X^2)$. Le quotient A/I est (isomorphe à) l'anneau dans l'Exemple 1.1(iv).*

— *Pour $A = \mathbb{R}[X, Y]$ et $I_1 = (X - Y^2)$, le quotient A/I peut s'interpréter comme l'anneau des fonctions (polynomiales) $C_1 \to \mathbb{R}$, où C_1 est la parabole d'équation $x = y^2$. D'autre part, soit $I_2 = (XY)$; le quotient A/I_2 est l'anneau des fonctions à valeurs réelles sur la courbe*

$$C_2 = \{(x, y) \in \mathbb{R}^2 \mid xy = 0\}.$$

L'anneau A/I_1 est intègre, mais A/I_2 ne l'est pas, car $x \in A/I_1$ est un diviseur de zéro. Géométriquement, ceci correspond au fait que C_2 est l'union de deux droites, mais C_1 ne peut pas "se couper en deux pièces".

Lemme 1.5. *(Théorème des restes chinois) Soit A un anneau et soient $I_1, \ldots, I_k \subset A$ des idéaux tels que, pour tout $i \neq j$, on a $I_i + I_j = A$. Alors $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$ et l'application naturelle $A \to A/I_1 \times \cdots \times A/I_k$ induit un isomorphisme $A/I_1 \cdots I_k \simeq A/I_1 \times \cdots \times A/I_k$.*

Démonstration. Montrons d'abord que $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$ par induction sur $k \geq 1$. Pour $k = 1$ il n'y a rien a démontrer ; supposons $k \geq 2$. On a $1 \in I_1 + I_j$ pour $2 \leq j \leq k$, donc $1 \in (I_1 + I_2) \cdots (I_1 + I_k) = I_1 + I_2 \cdots I_k$. Soient $i_1 \in I_1$ et $i' \in J = I_2 \cdots I_k$ tels que $i_1 + i' = 1$. Si $i \in I_1 \cap J$ alors $i = i \cdot (i_1 + i') \in J \cdot I_1 + I_1 \cdot J = I_1 I_2 \cdots I_k$. Donc $I_1 \cap J = I_1 J$. Comme $J = I_2 \cap \cdots \cap I_k$ par induction, on obtient $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$.

Maintenant, le noyau de $q : A \to A/I_1 \times \cdots \times A/I_k$ est $I_1 \cap \cdots \cap I_k$, donc il reste à montrer que q est surjective. On a $q(i') = (1, 0, 0, \ldots, 0)$; plus généralement, pour $2 \leq i \leq k$ l'argument ci-dessus avec I_i à la place de I_1 montre que $(0, \ldots, 0, 1, 0, \ldots, 0)$ (1 est à la place i) est dans l'image de q, donc q est surjective. □

Exemple 1.6. — *Soit $n \in \mathbb{Z}_{>0}$; écrivons $n = \prod_{i=1}^{r} p_i^{e_i}$ où les p_i sont des nombres premiers distincts. Si $i \neq j$ alors $(p_i^{e_i}) + (p_j^{e_j}) = \mathbb{Z}$, donc*

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/(p_i^{e_i}).$$

— *Soit $A = \mathbb{R}[X, Y]$ et $I = (X^2 - X)$. Alors $I = I_1 I_2$ avec $I_1 = (X)$ et $I_2 = (1 - X)$. Comme $I_1 + I_2 = A$, on obtient $A/I \simeq \mathbb{R}[X, Y]/(X) \times \mathbb{R}[X, Y]/(X - 1) \simeq \mathbb{R}[Y] \times \mathbb{R}[Y]$. Géométriquement, cette écriture de A/I correspond au fait que l'ensemble $\{(x, y) \in \mathbb{R}^2 : x^2 = x\}$ est l'union des deux droites $x = 0$ et $x = 1$.*

Lemme 1.7. *Soit A un anneau. L'ensemble $\sqrt{A}$ des éléments nilpotents de A est un idéal ; l'anneau quotient $A/\sqrt{A}$ est réduit.*

Démonstration. Si $a \in \sqrt{A}$ alors, pour tout $b \in A$, on a $ab \in \sqrt{A}$, car $a^n = 0$ implique $(ab)^n = 0$. Vérifions maintenant que la somme de deux éléments nilpotents est nilpotente. Soient $a, b \in A$ et n, m deux entiers positifs tels que $a^n = b^m = 0$. On a

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k};$$

si $k \geq n$ alors $a^k = 0$; d'autre part, si $k < n$ alors $n+m-k > m$ donc $b^{n+m-k} = 0$. Donc tout terme de la somme est nul, et $(a+b)^{n+m} = 0$. On a vérifié que $\sqrt{A}$ est un idéal de A.

Montrons maintenant que $A/\sqrt{A}$ est réduit. Soit $q : A \to A/\sqrt{A}$ la projection. Soit $a \in A$ tel que $q(a)$ est nilpotent : alors $q(a)^n = 0 \in A/\sqrt{A}$ pour un entier positif n, i.e. $a^n \in \sqrt{A}$. Donc a^n est nilpotent, ce qui implique que a est aussi nilpotent, donc $q(a) = 0$. □

Exemple 1.8.
- *Si k est un corps et $A = k[X]/(X^n)$ avec $n \geq 1$ alors $\sqrt{A} = (X)$, et $A/\sqrt{A} \simeq k$.*
- *Soit $n = \prod_{i=1}^{r} p_i^{e_i}$ comme dans l'Exemple 1.6, et $A = \mathbb{Z}/n\mathbb{Z}$. Alors $\sqrt{A} = (p_1 p_2 \cdots p_r)$, et $A/\sqrt{A} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.*

1.3 Idéaux premiers et maximaux

Remarque 1.9. *Un anneau A avec $0 \neq 1$ est un corps si et seulement si les idéaux de A sont $\{0\}$ et A. En effet, si A est un corps alors $A \setminus \{0\} = A^\times$, donc tout idéal $I \neq \{0\}$ contient une unité, donc est égal à A. Réciproquement, soit $a \in A \setminus \{0\}$. On a alors $(a) \supsetneq \{0\}$, donc $(a) = A$, i.e. il existe $b \in A$ tel que $ab = 1$.*

Définition 1.10. *Soit A un anneau.*
- *Un idéal $I \subset A$ est premier si $I \neq A$ et pour tout $a, b \in A$, si $ab \in I$ alors $a \in I$ ou $b \in I$.*
- *Un idéal $I \subset A$ est maximal si $I \neq A$ et pour tout idéal $I \subset J \subset A$ on a $J = I$ ou $J = A$.*

On note $\mathrm{Spec}(A)$ *le spectre de A, i.e. l'ensemble des idéaux premiers de A, et* $\mathrm{MaxSpec}(A)$ *l'ensemble des idéaux maximaux de A.*

Lemme 1.11. *Soit A un anneau et $I \subset A$ un idéal.*
1. *I est premier si et seulement si A/I est un anneau intègre.*
2. *I est maximal si et seulement si A/I est un corps.*

En particulier, tout idéal maximal est premier.

Démonstration. 1. Soit $q : A \to A/I$ la projection. L'anneau A/I est intègre si $A/I \neq \{0\}$ (i.e. $I \neq A$) et, pour tout $a, b \in A$, si $q(a)q(b) = 0$ alors $q(a) = 0$ ou $q(b) = 0$. En d'autres termes, si $ab \in I$ alors $a \in I$ ou $b \in I$, i.e. I est premier.

2. D'après le Lemme 1.3(3) on a que I est maximal si et seulement si $I \neq A$ et les idéaux de A/I sont $\{0\}$ et A/I, ce qui équivaut au fait que A/I soit un corps (Remarque 1.9).

□

Exemple 1.12. — *Pour un entier $n \geq 0$, l'idéal $(n) \subset \mathbb{Z}$ est premier si et seulement si pour tout $a, b \in \mathbb{Z}$, si $n \mid ab$ alors $n \mid a$ ou $n \mid b$. Ceci est le cas si et seulement si $n = 0$ ou n est premier. Pour tout nombre premier p l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc*

$$\mathrm{Spec}(\mathbb{Z}) = \{(0)\} \coprod \{(p), p \text{ premier}\} \supset \mathrm{MaxSpec}(\mathbb{Z}) = \{(p), p \text{ premier}\}.$$

— *Soit k un corps et $A = k[X]$. Les idéaux premiers de A sont de la forme $P(X)$ avec $P(X) = 0$ ou $P(X) \in k[X] \smallsetminus k^\times$ irréductible. Par exemple, $\mathrm{Spec}(\mathbb{C}[X]) = \{(0)\} \coprod \{(X - a), a \in \mathbb{C}\}$. On voit donc que*

$$\begin{aligned} \mathbb{C} &\to \mathrm{MaxSpec}(\mathbb{C}[X]) \\ a &\mapsto (X - a) \end{aligned}$$

est une bijection. Pour tout $P \in \mathbb{C}[X]$, on a $P - P(a) \in (X - a)$, donc l'image de P dans $\mathbb{C}[X]/(X - a)$ est $P(a)$.

Lemme 1.13.

1. *Soit $f : A \to B$ un morphisme d'anneaux. Pour tout $\mathfrak{p} \in \mathrm{Spec}(B)$ on a $f^{-1}(\mathfrak{p}) \in \mathrm{Spec}(A)$. Donc f induit une application*

$$\begin{aligned} f^\sharp : \mathrm{Spec}(B) &\to \mathrm{Spec}(A) \\ \mathfrak{p} &\mapsto f^{-1}(\mathfrak{p}). \end{aligned}$$

2. *Soit A un anneau, $I \subset A$ un idéal et $q : A \to A/I$ la projection. L'application $q^\sharp$ induit une bijection*

$$\mathrm{Spec}(A/I) \to \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supset I\}.$$

3. *Soit A un anneau. L'application $\mathrm{Spec}(A/\sqrt{A}) \to \mathrm{Spec}(A)$ induite par le morphisme $A \to A/\sqrt{A}$ est une bijection.*

Démonstration. 1. Pour $\mathfrak{p} \in \mathrm{Spec}(B)$, l'image réciproque $\mathfrak{q} = f^{-1}(\mathfrak{p})$ est le noyau de la composition $A \to B \to B/\mathfrak{p}$. En particulier, $\mathfrak{q}$ est un idéal différent de A. De plus, $A/\mathfrak{q}$ s'injecte dans l'anneau intègre $B/\mathfrak{p}$, donc $A/\mathfrak{q}$ est intègre et $\mathfrak{q} \in \mathrm{Spec}(B)$ d'après le Lemme 1.11.

2. Découle du Lemme 1.3(3) et du fait que, dans la bijection du lemme, $\bar{J}$ est premier si et seulement si $q^{-1}(\bar{J})$ l'est.

3. Découle de (2) et du fait que tout $\mathfrak{p} \in \mathrm{Spec}(A)$ contient $\sqrt{A}$. En effet, si $a \in A$ est nilpotent il existe $n \geq 0$ tel que $a^n = 0 \in \mathfrak{p}$, donc $a \in \mathfrak{p}$ comme $\mathfrak{p}$ est premier.

□

Remarque 1.14. *Attention : si $f : A \to B$ est un morphisme d'anneaux et $\mathfrak{m} \in \mathrm{MaxSpec}(B)$, il n'est pas vrai en général que $f^{-1}(\mathfrak{m}) \in \mathrm{MaxSpec}(A)$. Un contre-exemple est donné par l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$, avec $\mathfrak{m} = (0)$.*

Exemple 1.15. *(Important) On va montrer en TD que*

$$\mathrm{Spec}(\mathbb{C}[X,Y]) = \{(0)\} \coprod \{(P), P \in \mathbb{C}[X,Y] \text{ unitaire irréductible}\} \coprod \{(X-a, Y-b), (a,b) \in \mathbb{C}^2\},$$

et $\mathrm{SpecMax}(\mathbb{C}[X,Y]) \simeq \mathbb{C}^2$ *via l'application qui envoie* $(a,b) \in \mathbb{C}^2$ *sur* $(X-a, Y-b)$.

Soit $A = \mathbb{C}[X,Y]/(X-Y^2)$. *C'est l'anneau des fonctions polynomiales à valeurs complexes sur la parabole* $C = \{(a,b) \in \mathbb{C}^2 \mid a = b^2\}$. *L'anneau A est intègre, donc (0) est un idéal premier. Les autres idéaux premiers de A, d'après le Lemme 1.13, correspondent aux idéaux* $(X-a, Y-b) \supset (X-Y^2)$. *Donc on a* $\mathrm{Spec}(A) = \{(0)\} \coprod \{(X-a, Y-b), a = b^2\}$, *et l'application qui envoie (a,b) sur $(X-a, Y-b) \subset A$ induit une bijection entre C et* $\mathrm{MaxSpec}(A)$.

Soit $B = \mathbb{C}[X]$; *le morphisme $p : B \to A$ qui envoie X en X induit* $p^\sharp : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$. *On a* $p^\sharp((0)) = (0)$ *et, pour tout* $(a,b) \in C$, $p^\sharp(X-a, Y-b) = (X-a)$. *Donc $p^\sharp$ correspond géométriquement à la projection $\pi : C \to \mathbb{C}$ qui envoie (a,b) sur a.*

Pour tout point $a \in \mathbb{C} \setminus \{0\}$ *la fibre* $\pi^{-1}(a)$ *a deux éléments, mais* $\pi^{-1}(0) = 0$ *(π est un recouvrement de degré 2 ramifié en 0). Reformulons cette observation en langage algébrique. Pour tout $a \in \mathbb{C}$, le Lemme 1.13 donne une bijection entre le spectre du quotient $A/(X-a)$ et l'ensemble des idéaux premiers $\mathfrak{p}$ de A tels que* $p^\sharp(\mathfrak{p}) = (X-a)$. *En d'autres termes,* $\mathrm{Spec}(A/(X-a))$ *est en bijection avec l'image réciproque par* $p^\sharp$ *de* $(X-a) \in \mathrm{Spec}(B)$. *Observons que* $A/(X-a) \simeq \mathbb{C}[Y]/(Y^2-a)$ *est isomorphe à* $\mathbb{C} \times \mathbb{C}$ *si* $a \neq 0$, *et à* $\mathbb{C}[Y]/(Y^2)$ *si* $a = 0$. *Dans les deux cas, $A/(X-a)$ est un $\mathbb{C}$-espace vectoriel de dimension 2 ; pour $a = 0$ le spectre de cet anneau n'a qu'un élément, et l'anneau n'est pas réduit.*

Existence d'idéaux premiers et maximaux Pour terminer, on va traiter deux résultats d'existence d'idéaux premiers et maximaux. La preuve repose sur le lemme de Zorn (donc sur l'axiome du choix), même si l'on verra plus tard qu'on peut s'en passer pour plusieurs anneaux d'intérêt, par exemple les quotients des anneaux de polynômes $k[X_1, \dots, X_n]$ à coefficients dans un corps k.

Proposition 1.16. *Pour tout anneau $A \neq \{0\}$ on a $\mathrm{MaxSpec}(A) \neq \emptyset$ (donc $\mathrm{Spec}(A) \neq \emptyset$).*

Démonstration. L'idée naïve est de choisir un idéal $I_0 \subsetneq A$ (e.g. $I_0 = 0$) ; ensuite, si I_0 n'est pas maximal, il existe un idéal $I_0 \subsetneq I_1 \subsetneq A$; si I_1 n'est pas maximal, on continue...

Pour transformer cette idée en une preuve, notons $\mathcal{I}$ l'ensemble des idéaux $I \subsetneq A$; on remarque que $\mathcal{I}$ est non vide, car $(0) \in \mathcal{I}$. L'inclusion est une relation d'ordre sur $\mathcal{I}$, et si $\{I_\lambda, \lambda \in \Lambda\}$ est totalement ordonné, alors $I = \cup_{\lambda\in\Lambda} I_\lambda$ appartient à $\mathcal{I}$. En effet, il est clair que si $a \in A$ alors $aI \subset I$. De plus, soient $i_1, i_2 \in I$; il existent $\lambda_i, \lambda_2 \in \Lambda$ tels que $i_i \in I_{\lambda_1}$ et $i_2 \in I_{\lambda_2}$. Comme $\mathcal{I}$ est totalement ordonné, on a $I_{\lambda_1} \subset I_{\lambda_2}$ ou $I_{\lambda_2} \subset I_{\lambda_1}$. Sans perte de généralité, supposons que $I_{\lambda_1} \subset I_{\lambda_2}$. Alors $i_1 + i_2 \in I_{\lambda_2} \subset I$. Enfin, $I \neq A$, car pour tout $\lambda \in \Lambda$, 1 n'appartient pas à I_λ.

Comme $I \in \mathcal{I}$ est un majorant de $\{I_\lambda, \lambda \in \Lambda\}$, on peut appliquer le lemme de Zorn, qui nous dit que $\mathcal{I}$ a un élément maximal, qui est donc un idéal maximal de A. □

Proposition 1.17. *Soit A un anneau et $S \subset A$ un sous-ensemble non vide multiplicatif, i.e. tel que, si $s_1, s_2 \in S$, alors $s_1 s_2 \in S$. Soit $I \subset A$ un idéal tel que $I \cap S = \emptyset$. Il existe $\mathfrak{p} \in \mathrm{Spec}(A)$ tel que $\mathfrak{p} \supset I$ et $\mathfrak{p} \cap S = \emptyset$.*

Démonstration. On pose $\mathcal{I}(S) = \{J \text{ idéal}, J \supset I, J \cap S = \emptyset\}$; on a $I \in \mathcal{I}(S)$, donc $\mathcal{I}(S)$ est non vide. L'argument dans la preuve de la proposition précédente montre que $I(S)$ contient un élément $\mathfrak{p}$ maximal par rapport à l'inclusion ; montrons que $\mathfrak{p} \in \mathrm{Spec}(A)$. Tout d'abord, comme $S \neq \emptyset$ et $\mathfrak{p} \cap S = \emptyset$, on a $\mathfrak{p} \neq A$. Ensuite, soient $a_1, a_2 \in A \setminus \mathfrak{p}$. On a $\mathfrak{p} + (a_1) \supsetneq \mathfrak{p}$ et $\mathfrak{p} + (a_2) \supsetneq \mathfrak{p}$, donc $(\mathfrak{p} + (a_i)) \cap S \neq \emptyset$ pour $i = 1, 2$. Soient $p_1, p_2 \in \mathfrak{p}$ et $r_1, r_2 \in A$ tels que $p_1 + a_1 r_1 \in S$ et $p_2 + a_2 r_2 \in S$. Comme S est multiplicatif, il contient $(p_1 + a_1 r_1)(p_2 + a_2 r_2) = p_1 p_2 + p_1 a_2 r_2 + p_2 a_1 r_1 + a_1 a_2 r_1 r_2$. Comme $\mathfrak{p} \cap S = \emptyset$ on a $a_1 a_2 r_1 r_2 \notin \mathfrak{p}$, donc $a_1 a_2 \notin \mathfrak{p}$. □

Corollaire 1.18. *Pour tout anneau A, on a $\sqrt{A} = \cap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}$.*

Démonstration. On a montré que $\sqrt{A} \subset \cap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}$ dans la preuve du Lemme 1.13(3). Réciproquement, soit $a \in A \setminus \sqrt{A}$; soit $I = (0)$, et $S = \{a^n, n \geq 0\}$. Il s'agit d'un ensemble multiplicatif tel que $I \cap S = \emptyset$. Grâce à la Proposition 1.17, il existe $\mathfrak{p} \in \mathrm{Spec}(A)$ tel que $\mathfrak{p} \cap S = \emptyset$. En particulier, $a \notin \mathfrak{p}$. □

2 Algèbres finies et entières

2.1 Modules

Il s'agit de faire de l'algèbre linéaire à partir d'un anneau A quelconque, pas forcement un corps.

Définition 2.1. *Soit A un anneau. Un A-module est un groupe abélien $(M,+)$ muni d'une application*

$$\begin{aligned} A \times M &\to M \\ (a,m) &\mapsto am \end{aligned}$$

telle que

- $\forall m \in M, 1m = m$.
- $\forall a \in A, \forall m,n \in M, a(m+n) = am + an$.
- $\forall a,b \in A, \forall m \in M, (a+b)m = am + bm$.
- $\forall a,b \in A, \forall m \in M, (ab)m = a(bm)$.

Un sous-module d'un A-module M est un sous-groupe $N \subset M$ tel que pour tout $a \in A$ et tout $n \in N$ on a $an \in N$.

Une application $f : M \to M'$ entre $A-$modules est un morphisme de $A-$modules si c'est un morphisme de groupes et, pour tout $a \in A$ et $m \in M$, on a $f(am) = af(m)$.

Exemple 2.2.

- *La multiplication $A \times A \to A$ munit tout anneau A d'une structure de A-module. Les sous-modules de A sont les idéaux de A. Plus généralement, si $f : A \to B$ est un morphisme d'anneaux, alors l'application $A \times B \to B$ qui envoie (a,b) sur $f(a)b$ munit $(B,+)$ d'une structure de A-module.*
- *Si A est un corps, alors un A-module est la même chose qu'un A-espace vectoriel.*
- *Pour $A = \mathbb{Z}$, un A-module est la même chose qu'un groupe abélien.*
- *Si $M_1, \ldots, M_n$ sont des $A-$modules, alors l'application*

$$\begin{aligned} A \times (M_1 \oplus \cdots \oplus M_n) &\to M_1 \oplus \cdots \oplus M_n \\ (a,(m_1,\ldots,m_n)) &\mapsto (am_1,\ldots,am_n) \end{aligned}$$

munit $M_1 \oplus \cdots \oplus M_n$ d'une structure de A-module, appelé somme directe des M_i.

Définition 2.3. *Soit A un anneau.*

— *Un A-module M est dit de type fini s'il existe un entier $n \geq 0$ et un morphisme surjectif de A-modules $A^n \to M$. Concrètement, ceci signifie qu'il existent $m_1, \ldots, m_n \in M$ qui engendrent M, i.e. tels que tout $m \in M$ s'écrit sous la forme $m = \sum_{i=1}^n a_i m_i$ avec $a_1, \ldots, a_n \in A$ (pas nécessairement uniques).*

— *Un A-module M est dit libre de rang $n \geq 0$ s'il est isomorphe à $A^n = A \oplus A \oplus \cdots \oplus A$ (n fois).*

Remarque 2.4. *1. Attention : si A est un corps, alors tout A-module de type fini est libre (tout espace vectoriel de dimension finie admet une base). Ceci n'es pas vrai si A n'est pas un corps. Par exemple, $\mathbb{Z}/2\mathbb{Z}$ est un $\mathbb{Z}$-module de type fini, mais il n'est pas libre.*

2. Si M est libre de rang $n \geq 0$, alors n est unique. En d'autres termes, si $n' \neq n$ alors A^n n'est pas isomorphe à $A^{n'}$. En effet, supposons par l'absurde que $A^n \simeq A^{n'}$. D'après la Proposition 1.16 il existe $\mathfrak{m} \in \mathrm{MaxSpec}(A)$; soit $k = A/\mathfrak{m}$. On obtient $A^n/\mathfrak{m}A^n \simeq A^{n'}/\mathfrak{m}A^{n'}$, i.e. $k^n \simeq k^{n'}$, contradiction.

Comatrice. Rappelons que, si A est une matrice carrée de taille n à coefficients dans un corps k, la comatrice de A, notée $\mathrm{com}\mathsf{A}$, est la matrice carrée de taille n dont le coefficient (i,j) est $(-1)^{i+j}\det(\mathsf{A}_{i,j})$, où $\mathsf{A}_{i,j}$ est la matrice obtenue en supprimant la i-ème ligne et la j-ème colonne de A. La matrice $\mathrm{com}\mathsf{A}$ satisfait

$$\mathsf{A}\,{}^t\mathrm{com}\mathsf{A} = {}^t\mathrm{com}\mathsf{A}\,\mathsf{A} = \det(\mathsf{A})\mathsf{I}_n.$$

La définition de $\mathrm{com}\mathsf{A}$ fait du sens pour des matrices à coefficients dans un anneau quelconque, et l'égalité ci-dessus reste vraie en cette généralité.

Lemme 2.5. *(crucial !) Soit A un anneau et M un A-module de type fini, engendré par $m_1, \ldots, m_n$. Soit $\mathsf{m} = (m_1, \ldots, m_n) \in M^n$. Soit $\mathsf{A} = (a_{ij})_{1 \leq i,j \leq n} \in M_{n \times n}(A)$ une matrice carrée. Si $\mathsf{A}\mathsf{m} = 0$ alors, pour tout $m \in M$, on a $\det(\mathsf{A})m = 0$.*

Démonstration. Comme $\mathsf{A}\mathsf{m} = 0$ on a ${}^t\mathrm{com}\mathsf{A}\,\mathsf{A}\,\mathsf{m} = 0$, donc $\det(\mathsf{A})\mathsf{m} = 0$, i.e. $\det(\mathsf{A})m_i = 0$ pour $1 \leq i \leq n$. Comme $m_1, \ldots, m_n$ engendrent M, on déduit que $\det(\mathsf{A})m = 0$ pour tout $m \in M$. □

2.2 Éléments entiers, algèbres entières et finies

Définition 2.6. *Soit A un anneau.*

— *Une A-algèbre est la donnée d'un anneau B et d'un morphisme d'anneaux $\iota : A \to B$ (on omet souvent ι de la notation).*

— *Une A-algèbre B est finie si B est un A-module de type fini (avec la structure de A-module décrite dans l'Exemple 2.2).*

Exemple 2.7. *(i) Si $K \to L$ est un morphisme de corps, alors L est une K-algèbre finie s'il est un K-espace vectoriel de dimension finie.*

(ii) Soit $D \in \mathbb{Z}$ un entier qui n'est pas un carré. L'anneau $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D}, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ est une $\mathbb{Z}$-algèbre finie.

(iii) Soit k un corps, $A = k[X]$ et $f(X) \in A$. L'anneau

$$B = k[X,Y]/(Y^2 - f(X)) = A[Y]/(Y^2 - f(X))$$

est une A-algèbre finie.

(iv) Si A est un anneau et $I \subset A$ est un idéal, alors A/I est une A-algèbre finie.

(v) Soit k un corps ; l'anneau $k[X]$ est une k-algèbre, pas finie.

(vi) Soit $A = k[X] \to B = k[X,Y]/(XY - 1)$. La A-algèbre B n'est pas finie ; on peut le vérifier directement, et on en donnera une preuve dans la remarque ci-dessous.

Remarque 2.8. *Soit $A \to B$ une A-algèbre finie. Choisissons $b_1, \ldots, b_n \in B$ qui engendrent B comme A-module. Soit $b \in B$; écrivons, pour $1 \leq i \leq n$,*

$$bb_i = \sum_{j=1}^{n} a_{ij} b_j, \ a_{ij} \in A.$$

Soit $\mathsf{A} = (a_{ij})_{1 \leq i,j \leq n} \in M_{n \times n}(A)$, et $\mathsf{b} = (b_1, \ldots, b_n)$. On a $(b\mathsf{I}_n - \mathsf{A})\mathsf{b} = 0$, donc $\det(b\mathsf{I}_n - \mathsf{A})b' = 0$ pour tout $b' \in B$, grâce au Lemme 2.5. Prenant $b' = 1$ on trouve $\det(b\mathsf{I}_n - \mathsf{A}) = 0$. On remarque enfin qu'on peut écrire

$$\det(b\mathsf{I}_n - \mathsf{A}) = b^n + a_{n-1}b^{n-1} + \ldots + a_0, \ \text{avec } a_0, \ldots, a_{n-1} \in A.$$

On a donc montré que tout $b \in B$ est zéro d'un polynôme unitaire dans $A[X]$. On remarque que, dans le dernier exemple ci-dessus, $Y \in k[X,Y]/(XY - 1)$ ne satisfait pas cette propriété.

Définition 2.9. *Soit $A \to B$ une A-algèbre.*

- *Un élément $b \in B$ est entier sur A s'il existe $P(X) \in A[X]$ unitaire tel que $P(b) = 0$.*
- *On dit que B est une A-algèbre entière si tout $b \in B$ est entier sur A.*

Si $\iota : A \to B$ est une A-algèbre et $b \in B$, on note $A[b] \subset B$ la plus petite A-algèbre contenant $\iota(A)$ et b, i.e. l'ensemble des expressions polynomiales en b à coefficients dans $\iota(A)$.

Proposition 2.10. *Soit B une A-algèbre, et soit $b \in B$. Les propriétés suivantes sont équivalentes.*

1. *b est entier sur A.*
2. *$A[b] \subset B$ est une A-algèbre finie.*
3. *Il existe une A-algèbre finie $B' \subset B$ telle que $b \in B'$.*

En particulier, si B est une A-algèbre finie alors elle est entière.

Démonstration. (1) $\Rightarrow$ (2) : supposons que $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$. Alors $b^n = -a_{n-1}b^{n-1} - \ldots - a_0$, donc $b^n \in A + bA = \ldots + b^{n-1}A$, et plus généralement $b^m \in A + bA = \ldots + b^{n-1}A$ pour tout $m \geq n$. Donc $A[b]$ est egendrée par $1, b, \ldots, b^{n-1}$ comme A-module.

(2) $\Rightarrow$ (3) : prendre $B' = A[b]$.

(3) $\Rightarrow$ (1) : même argument que dans la Remarque 2.8. □

Exemple 2.11. *Soit $K \to L$ un morphisme de corps. Un élément $x \in L$ entier sur K s'appelle élément algébrique sur K, et on dit que L/K est algébrique si L est une K-algèbre entière. Le fait que x est algébrique est équivalent à l'existence de $P(X) \in K[X] \setminus \{0\}$ tel que $P(x) = 0$. En effet, si un tel P existe, on peut toujours le rendre unitaire un multipliant par l'inverse du coefficient dominant.*

Par exemple, $L = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}, a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$ est algébrique sur $\mathbb{Q}$, d'après la Proposition 2.10. On remarque que, étant donné $x \in L$ (par exemple $5 + 3\sqrt[3]{2} + \sqrt[3]{4}$), il n'est pas immédiat de trouver un polynôme non nul $P(X) \in \mathbb{Q}[X]$ tel que $P(x) = 0$, dont l'existence et garantie par la Proposition 2.10.

Corollaire 2.12. *Soit A un anneau, B une A-algèbre et C une B-algèbre (on a donc des morphismes $A \to B \to C$).*

1. *Si B est une A-algèbre finie et C est une B-algèbre finie alors C est une A-algèbre finie.*
2. *Si $y_1, \ldots, y_n \in B$ sont entiers sur A, alors $A[y_1, \ldots, y_n]$ est finie sur A.*
3. *Si B est une A-algèbre entière et C est une B-algèbre entière alors C est une A-algèbre entière.*
4. *L'ensemble $\tilde{A} = \{y \in B \mid y \text{ est entier sur } A\}$ est un sous-anneau de B.*

Démonstration.

1. Comme en algèbre linéaire : soient $b_1, \ldots, b_n \in B$ qui engendrent B comme A-module, et $c_1, \ldots, c_m \in C$ qui engendrent C comme B-module. On va montrer que les $b_i c_j, 1 \leq i \leq n, 1 \leq j \leq m$, engendrent C comme A-module. Étant donné $c \in C$, il existent $b_1(c), \ldots, b_m(c) \in B$ tels que $c = \sum_{j=1}^m b_j(c)c_j$. D'autre part, pour $1 \leq j \leq m$ on peut écrire $b_j(c) = \sum_{i=1}^n a_{ij}b_i$. Donc $c = \sum_{i,j} a_{ij}b_i c_j$.
2. Par induction sur n ; si $n = 1$, le résultat découle de la Proposition 2.10. Supposons $n > 1$. Par induction, $B = A[y_1, \ldots, y_{n-1}]$ est finie sur A ; de plus, $A[y_1, \ldots, y_n] = B[y_n]$ est finie sur B d'après la Proposition 2.10, donc elle est finie sur A d'après 1.

3. Soit $c \in C$. Il existent $b_0, \ldots, b_{n-1} \in B$ tels que $c^n + b_{n-1}c^{n-1} + \ldots + c_0 = 0$, donc c est entier sur $B' = A[b_0, \ldots, b_{n-1}]$, donc $B'[c]$ est finie sur B' d'après la Proposition 2.10. D'autre part B' est finie sur A d'après 2., donc $B'[c]$ est finie sur A d'après 1. La Proposition 2.10 implique que c est entier sur A.
4. Soient $y_1, y_2 \in \tilde{A}$. On sait grâce à 2. que $A[y_1, y_2]$ est finie sur A, donc $A[y_1, y_2] \subset \tilde{B}$ d'après la Proposition 2.10. En particulier $y_1 + y_2$ et $y_1 y_2$ appartiennent à $\tilde{A}$.

□

Définition 2.13. *Soit B une A-algèbre. On appelle l'anneau*

$$\tilde{A} = \{y \in B \mid y \text{ est entier sur } A\}$$

la fermeture intégrale de A dans B. Si A est un anneau intègre et $B = \mathrm{Frac}(A)$, on appelle $\tilde{A}$ la clôture intégrale de A. On dit qu'un anneau intègre A est intégralement clos s'il coïncide avec sa clôture intégrale.

Remarque 2.14. *Les arguments dans la preuve du corollaire sont assez indirects, et ne donnent pas de moyen de déterminer $\tilde{A}$. Il ne s'agit pas d'une tâche simple en général, comme l'on verra dans des exemples ci-dessous.*

Exemple 2.15.
— *Soit $A = \mathbb{Z}$ et $B = \mathbb{Q}(\sqrt{5})$. Comme $\sqrt{5}$ est entier sur A (il est une racine de $X^2 - 5$) on a $\mathbb{Z}[\sqrt{5}] \subset \tilde{A}$. Mais l'inclusion n'est pas une égalité. En effet, le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ n'appartient pas à $\mathbb{Z}[\sqrt{5}]$, mais il satisfait $\varphi^2 - \varphi - 1$, donc $\varphi \in \tilde{A}$. En fait, on a $\tilde{A} = \mathbb{Z}[\varphi]$.*

— *Plus généralement, si $D \in \mathbb{Z} \smallsetminus \{0, 1\}$ n'a pas de facteur carré, alors la fermeture intégrale $\tilde{A}$ de $\mathbb{Z}$ dans $\mathbb{Q}(\sqrt{D})$ est (preuve en TD)*

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D}, a, b \in \mathbb{Z}\} \text{ si } D \equiv 2, 3 \pmod 4;$$
$$\mathbb{Z}[(1 + \sqrt{D})/2] = \{a + b(1 + \sqrt{D})/2, a, b \in \mathbb{Z}\} \text{ si } D \equiv 1 \pmod 4.$$

On remarque que, dans les deux cas, la $\mathbb{Z}$-algèbre $\tilde{A}$ est finie. On verra plus tard un généralisation de ce phénomène.

— *La fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(\sqrt[3]{10})$ contient strictement $\mathbb{Z}[\sqrt[3]{10}]$.*

— *Si k est un corps alors $k[X_1, \ldots, X_n]$ est un anneau factoriel, donc il est intégralement clos (TD).*

— *Soit $A = \mathbb{C}[X, Y]/(Y^2 - X^3)$. Il s'agit d'un anneau intègre, qui n'est pas intégralement clos. En effet, $T = \frac{Y}{X} \in \mathrm{Frac}(A)$ satisfait $T^2 - X = 0$, mais il n'appartient pas à A. D'autre part, on a $\mathbb{C}[T] = \tilde{A}$. L'application $\mathrm{Spec}(\tilde{A}) \to \mathrm{Spec}(A)$ induite par l'inclusion $A \to \tilde{A}$ induit une bijection entre idéaux maximaux, qui envoie $(T - t)$ sur $(X - t^2, Y - t^3)$, donc correspond à la paramétrisation $t \mapsto (t^2, t^3)$ des points de la courbe $y^2 = x^3$.*

Algèbres finies et recouvrements. Revenons à l'exemple de l'inclusion

$$p : A = \mathbb{C}[X] \to B = \mathbb{C}[X, Y]/(XY - 1).$$

Il correspond à la projection π de l'hyperbole d'équation $xy = 1$ sur l'axe $y = 0$. Observons que π n'est pas un "recouvrement" de l'axe $y = 0$, car $(0, 0)$ n'est pas dans l'image de π. Du côté algébrique, l'idéal $(X) \subset \mathbb{C}[X]$ n'est pas dans l'image de $p^\sharp$.

D'autre part, on a vu dans l'Exemple 1.15 que l'inclusion $\mathbb{C}[X] \to \mathbb{C}[X, Y]/(Y^2 - X)$ induit une surjection au niveau des spectres ; la prochaine proposition montre qu'il s'agit d'une propriété générale des extensions entières d'anneaux.

Proposition 2.16. *Soit $A \to B$ un morphisme injectif d'anneaux tel que B est une A-algèbre entière. L'application induite* $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *est surjective.*

Démonstration. On identifie A avec un sous-anneau de B. Soit $\mathfrak{p} \in \mathrm{Spec}(A)$, et $S = A \setminus \mathfrak{p}$; c'est un sous-ensemble multiplicatif de B. Soit $I = \{\sum_i p_i b_i, p_i \in \mathfrak{p}, b_i \in B\}$; il s'agit d'un idéal de B. On va montrer que

$$I \cap S = \emptyset. \tag{2.1}$$

En admettant pour l'instant ce fait, terminons la démonstration. La Proposition 1.17 implique qu'il existe $\mathfrak{q} \in \mathrm{Spec}(B)$ tel que $\mathfrak{q} \supset I$ et $\mathfrak{q} \cap S = \emptyset$. Comme $\mathfrak{q} \supset I$ on a $\mathfrak{p} \subset \mathfrak{q} \cap A$, et l'inclusion est une égalité car $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$.

Il reste à montrer (2.1). Supposons par l'absurde qu'il existe $s \in S \cap I$; écrivons $s = b_1 p_1 + \ldots + b_n p_n$ avec $p_1, \ldots, p_n \in \mathfrak{p}$ et $b_1, \ldots, b_n \in B$. Soit $B' = A[b_1, \ldots, b_n]$; il s'agit d'une A-algèbre finie d'après le Corollaire 2.12. Choisissons des générateurs $b'_1, \ldots, b'_m$ de B' comme A-module. Alors $I' = b'_1\mathfrak{p} + \ldots + b'_m\mathfrak{p} \subset B'$ est un idéal, et $s \in I'$. Donc $b'_i s \in I'$ pour $1 \leq i \leq m$, et on peut écrire :

$$b'_i s = \sum_{j=1}^{m} p_{ij} b'_j \text{ avec } p_{ij} \in \mathfrak{p}.$$

Soit $\mathsf{P} = (p_{ij})_{1 \leq i,j \leq m}$ et $\mathsf{b}' = (b'_1, \ldots, b'_m)$. On déduit que $(s\mathsf{I_m} - \mathsf{P})\mathsf{b}' = 0$, donc $\det(s\mathsf{I_m} - \mathsf{P})b' = 0$ pour tout $b' \in B'$, d'après le Lemme 2.5. En prenant $b' = 1$ on trouve que

$$0 = \det(s\mathsf{I_m} - \mathsf{P}) = s^m + p_{m-1}s^{m-1} + \ldots + p_0, \text{ avec } p_0, \ldots, p_{m-1} \in \mathfrak{p}.$$

Ceci implique que s^m appartient à $\mathfrak{p}$, donc s aussi car $\mathfrak{p}$ est premier ; mais s appartient à S, contradiction. □

Remarque 2.17. *L'injectivité du morphisme est une hypothèse nécessaire : si I est un idéal de A, alors A/I est une A-algèbre finie, mais l'application* $\mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ *est injective et pas surjective en général.*

Algèbres finies sur un corps

Lemme 2.18. *Soit $A \to B$ un morphisme injectif d'anneaux tel que B est entière sur A.*

1. *Si B est un corps alors A est un corps.*
2. *Si A est un corps et B est un anneau intègre alors B est un corps.*

Démonstration.

1. C'est un cas particulier de la Proposition 2.16, mais on peut aussi le vérifier à la main : soit $a \in A \setminus \{0\}$ et $b = a^{-1} \in B$. Il existent $a_0, \ldots, a_{n-1} \in A$ tels que $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$, donc
$$b = -(a_{n-1} + aa_{n-2} + \ldots + a^{n-1}a_0) \in A.$$
2. Soit $b \in B \setminus \{0\}$, et soient $a_0, \ldots, a_{n-1} \in A$ tels que $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$. Comme b n'est pas un diviseur de zéro, on peut supposer que $a_0 \neq 0$, donc $c = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1)$ satisfait $bc = 1$.

□

Proposition 2.19. *Soit k un corps et A une k-algèbre finie.*

1. $\mathrm{Spec}(A) = \mathrm{MaxSpec}(A)$, *et pour tout $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ le quotient $A/\mathfrak{m}$ est une extension finie de k.*
2. $\mathrm{Spec}(A)$ *est fini.*
3. $A/\sqrt{A} \simeq \prod_{\mathfrak{m} \in \mathrm{MaxSpec}(A)} A/\mathfrak{m}$.

En particulier, A est réduite si et seulement si A est un produit de corps.

Démonstration.

1. Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. D'après le Corollaire 2.12 la composée $k \to A \to A/\mathfrak{p}$ munit $A/\mathfrak{p}$ d'une structure de k-algèbre finie, donc $A/\mathfrak{m}$ est un corps (et une extension finie de k) d'après le Lemme 2.18.
2. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_l \in \mathrm{Spec}(A)$. D'après 1. on a $\mathfrak{p}_i + \mathfrak{p}_j = A$ si $i \neq j$. Le Lemme 1.5 implique que $A/\mathfrak{p}_1 \ldots \mathfrak{p}_k \simeq A/\mathfrak{p}_1 \times \cdots \times A/\mathfrak{p}_l$. On a donc
$$l \leq \dim_k(A/\mathfrak{p}_1 \ldots \mathfrak{p}_l) \leq \dim_k(A).$$
3. Même argument qu'au point précédent, en utilisant le Corollaire 1.18.

□

Exemple 2.20. — *Toute $\mathbb{C}$-algèbre finie réduite est un produit (fini) de copies de $\mathbb{C}$.*

— *Soit A un anneau et B une A-algèbre, libre de rang n comme A-module. Soit $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ et $k(\mathfrak{m}) = A/\mathfrak{m}$. Le quotient $B/\mathfrak{m}B$ est libre de rang n sur $k(\mathfrak{m})$, donc il contient au plus n idéaux premiers d'après la preuve de la Proposition 2.19.*

Par exemple, pour $A = \mathbb{Z}$ et $B = \mathbb{Z}[\sqrt[n]{2}]$, le spectre de $B/(p)$ où p est un nombre premier contient au plus n éléments. Pouvez-vous donner des conditions qui impliquent que $\mathrm{Spec}(B/(p))$ a cardinal n ?

3 Modules et anneaux noethériens

3.1 Propriétés de base et théorème de la base de Hilbert

Définition 3.1. *Soit A un anneau. Un A-module M est noethérien si tout sous-module $N \subset M$ est de type fini. On dit que A est un anneau noethérien s'il est noethérien comme A-module, i.e. si tout idéal $I \subset A$ est de la forme $(a_1, \ldots, a_k)$, avec $k \geq 0$ et $a_1 \ldots, a_k \in A$.*

Lemme 3.2. *Soit A un anneau et M un A-module. Les conditions suivantes sont équivalentes.*

1. *M est noethérien.*
2. *Toute chaîne $N_1 \subset N_2 \subset \ldots \subset M$ de sous-modules de M est stationnaire (i.e. il existe $k \geq 1$ tel que $N_j = N_k$ pour tout $j \geq k$).*
3. *Tout ensemble non vide de sous-modules de M possède un élément maximal par rapport à l'inclusion.*

Démonstration. (1) $\Rightarrow$ (2). Soit $N_\infty = \cup_{i \geq 1} N_i$; il s'agit d'un sous-module de M, donc il existent $m_1, \ldots, m_r \in N_\infty$ tels que $N_\infty = Am_1 + \ldots + Am_r$. Il existe $k \geq 1$ tel que $m_i \in N_k$ pour tout $1 \leq i \leq r$. Donc $N_\infty \subset N_k$, et $N_j = N_k$ si $j \geq k$.

(2) $\Rightarrow$ (3). Soit S un ensemble non vide de sous-modules de M ; choisissons $N_1 \in S$. Pour $i \geq 1$, si N_i n'est pas maximal alors il existe $N_{i+1} \in S$ tel que $N_{i+1} \supsetneq N_i$. La chaîne $N_1 \subsetneq N_2 \subsetneq \ldots$ est stationnaire, donc il existe $k \geq 1$ tel que N_k est maximal.

(3) $\Rightarrow$ (1). Soit $N \subset M$ un sous-module, et S l'ensemble des sous-modules de type fini de N. On a $(0) \in S$, donc S et non vide et contient un élément maximal N'. Montrons par l'absurde que $N' = N$. Si $N' \subsetneq N$, soit $n \in N \smallsetminus N'$. Le module $N' + An$ appartient à S et contient proprement N', contradiction. □

Remarque 3.3. *En particulier, dans un anneau noethérien tout ensemble non vide d'idéaux a un élément maximal, ce qui rend plus simple les preuves des Propositions 1.16 et 1.17.*

Lemme 3.4. *Soit A un anneau.*

1. *Si $M_1, \ldots, M_r$ sont des A-modules noethériens, alors $M_1 \oplus \ldots \oplus M_r$ est noethérien.*
2. *Si $f : M \to M'$ est un morphisme surjectif de A-modules et M est noethérien alors M' est noethérien.*
3. *Supposons A noethérien. Alors un A-module est noethérien si et seulement si il est de type fini.*
4. *Si A est un anneau noethérien et $A \to B$ est une A-algèbre finie alors B est un anneau noethérien.*

Démonstration. 1. Par induction sur r ; si $r = 1$ l'énoncé est tautologique. Pour $r \geq 2$, soit $N \subset M_1 \oplus \ldots \oplus M_r$ un sous-module, $N_r = N \cap M_r$ et $N^{(r)} = N/N_r$. La projection sur $M_1 \oplus \cdots \oplus M_{r-1}$ induit une injection $N^{(r)} \to M_1 \oplus \cdots \oplus M_{r-1}$, donc $N^{(r)}$ est un A-module de type fini, par hypothèse inductive. Soient $n_1, \ldots, n_k \in N$ dont les images dans $N^{(r)}$ engendrent $N^{(r)}$. Alors $N = N_r + An_1 + \ldots + An_k$ est de type fini, car N_r est un A-module de type fini.

2. Soit $N' \subset M'$ un sous-module et $N = f^{-1}(N')$. Il existent $n_1, \ldots, n_r$ qui engendrent N, donc $f(n_1), \ldots, f(n_r)$ engendrent $f(N) = N'$.
3. Par définition tout A-module noethérien est de type fini. Réciproquement, s'il existe une surjection $A^r \to M$ alors A^r est noethérien d'après 1., donc M l'est d'après 2.
4. B est un A-module noethérien d'après 3., donc tout idéal $I \subset B$ est un A-module de type fini, donc un B-module de type fini.

□

Exemple 3.5. — *Tout anneau principal (e.g. $\mathbb{Z}$ ou $k[X]$ pour un corps k) est noethérien.*

— *Soit k un corps. L'anneau $k[X_1, X_2, \ldots, X_n, \ldots]$ n'est pas noethérien, car $(X_1) \subset (X_1, X_2) \subset \cdots$ est une chaîne d'idéaux non stationnaire.*

— *Soit k un corps. L'anneau $\{a + XP(X, Y), a \in k\} = k[X, XY, XY^2, \ldots] \subset k[X, Y]$ n'est pas noethérien. En effet, l'idéal $(X, XY, XY^2, \ldots)$ n'est pas de type fini.*

Théorème 3.6. *(Théorème de la base de Hilbert) Si A est un anneau noethérien, alors $A[X]$ est noethérien.*

Corollaire 3.7. *Soit k un corps.*

1. *Pour tout $n \geq 0$, l'anneau $k[X_1, \ldots, X_n]$ est noethérien.*

2. *Pour tout $n \geq 0$ et tout idéal $I \subset k[X_1, \ldots, X_n]$ l'anneau $k[X_1, \ldots, X_n]/I$ est noethérien.*

Démonstration. 1. Théorème 3.6 + induction sur n.

2. 1.+ Lemme 3.4.

□

Preuve du Théorème 3.6. Soit $I \subset A[X]$ un idéal. Soit

$$J = \{0\} \cup \{a \in A \mid \exists P(X) \in I : a \text{ est le coefficient dominant de } P(X)\}.$$

Vérifions que J est un idéal de A. Si $P(X) \in I$ a coefficient dominant $a \in A$, alors pour tout $b \in A$ soit $ab = 0$ soit ab est le coefficient dominant de $bP(X)$, donc $bJ \subset J$. De plus, soient $P(X) = a_nX^n + \ldots + a_0 \in I$ et $Q(X) = b_mX^m + \ldots + b_0 \in I$, donc $a_n, b_m \in J$. Sans perte de généralité, supposons que $n \geq m$. Alors $P(X) + X^{n-m}Q(X) = (a_n + b_m)X^{n+m} + \ldots$ appartient à I, donc $a_n + b_m$ appartient à J.

Comme A est noethérien, il existent $a_1, \ldots, a_r$ qui engendrent J. Pour $1 \leq i \leq r$ choisissons $P_i(X) \in I$ avec coefficient dominant a_i, et notons k_i le degré de $P(X)$. Soit $k = \max\{k_i, 1 \leq i \leq r\}$. On va montrer que

$$I = \{P(X) \in I \mid \deg(P(X)) \leq k\} + A[X]P_1 + \ldots + A[X]P_r$$

ce qui implique (grâce au Lemme 3.4(3)) que I est de type fini comme $A[X]$-module. Soit $P(X) = aX^d + \ldots \in I$ de degré $d > k$. Écrivons $a = a_1b_1 + \ldots + a_rb_r$ avec $b_1, \ldots b_r \in A$. Considérons

$$Q(X) = P(X) - (b_1X^{d-k_1}P_1(X) + \ldots + b_rX^{d-k_r}P_r(X)) = (a - \sum_{i=1}^{r} a_ib_i)X^d + \ldots$$

C'est un polynôme de degré au plus $d-1$. Si $\deg(Q(X)) \leq k$ on a terminé, sinon on repète l'argument.

Remarque 3.8. — *La démonstration n'est pas constructive, i.e. ne donne pas un ensemble de générateurs "explicite" de I, ce qui avait étonné les collègues de Hilbert.*

— *Pour $A = \mathbb{C}[X_1, \ldots, X_n]$, soit $(P_k(X))_{k\geq 1}$ une suite de polynômes dans A. Soit $V = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid P_k(x_1, \ldots, x_n) = 0 \text{ pour tout } k \geq 1\}$. Le Théorème de la base de Hilbert nous dit qu'on peut définir V comme lieu des zéros d'un nombre fini de polynômes.*

3.2 Finitude de la fermeture intégrale

On s'intéresse à la question suivante : soit A un anneau intègre de corps des fractions K, et soit L/K une extension finie de corps. Soit B la fermeture intégrale de A dans L. Si A est noethérien, que peut-on dire de B ?

Exemple 3.9. *Soit $A = \mathbb{Z}$ et L une extension finie de $\mathbb{Q}$, qu'on appelle un corps de nombres. La fermeture intégrale de A dans L est notée O_L, et est appelée l'anneau des entiers de L. Il s'agit d'un objet central en théorie des nombres. Par exemple, lorsque $L = \mathbb{Q}(e^{2\pi i/p})$, le propriétés arithmétiques de O_L ont été étudiées par Kummer dans ses travaux sur l'équation de Fermat $X^p + Y^p = Z^p$.*

Lemme 3.10. *Soit A un anneau intègre, K son corps des fractions, et L/K une extension finie de corps de degré n.*

1. *Pour tout $x \in L$ il existe $d \in A$ tel que dx est entier sur A.*
2. *Il existe une base $x_1, \ldots, x_n$ de L comme K-espace vectoriel tel que x_i est entier sur A pour $1 \leq i \leq n$.*

Démonstration. 1. Soit $x \in L$ et soient $c_0, \ldots, c_{k-1} \in K$ tels que $x^k + c_{k-1}x^{k-1} + \ldots + c_0 = 0$. Écrivons $c_i = \frac{a_i}{d}$, avec $a_i, d \in A$. On a donc

$$d^k x^k + a_{k-1}d^{k-1}x^{k-1} + a_{k-2}dd^{k-2}x^{k-2} + \ldots + a_0 d^{k-1} = 0,$$

ce qui montre que dx est entier sur A.

2. Appliquer 1. à une base de L comme K-espace vectoriel.

□

Théorème 3.11. *Soit A un anneau intègre, de corps des fractions K de caractéristique zéro. Soit L/K une extension finie de corps, et B la fermeture intégrale de A dans L. Si A est noethérien et intégralement clos, alors B est une A-algèbre finie, donc un anneau noethérien.*

Avant de démontrer le théorème, voici une application importante en théorie des nombres et géométrie.

Proposition 3.12. *Soit $A = \mathbb{Z}$ ou $k[T]$, où k est un corps de caractéristique zéro. Soit L une extension finie de $K = \mathrm{Frac}(A)$. La fermeture intégrale B de A dans L a les propriétés suivantes :*

1. *B est un A-module libre de rang $[L : K]$;*
2. *B est noethérien ;*
3. *B est intégralement clos ;*
4. *Tout idéal premier de B différent de (0) est maximal.*

Démonstration. 1. B est un A-module de type fini et sans torsion, donc libre, car A est un anneau principal. De plus, d'après le Lemme 3.10 B contient un A-module libre de rang $[L : K]$, donc il a rang au moins $[L : K]$. En fait, le rang de B est exactement $[L : K]$, car des éléments A-linéairement indépendants dans L sont aussi K-linéairement indépendants.

2. =1+Lemme 3.4.

3. On a $\mathrm{Frac}(B) = L$ d'après le Lemme 3.10. Si $x \in L$ est entier sur B alors il est entier sur A grâce au Corollaire 2.12, donc $x \in B$.

4. Soit $\mathfrak{p} \in \mathrm{Spec}(B)$ différent de (0). Choisissons $x \in B$; il existent $a_0, \ldots, a_{k-1} \in A$ avec $a_0 \neq 0$ tels que $x^k + a_{k-1}x^{k-1} + \ldots + a_0 = 0$, donc $a_0 \in \mathfrak{q} = \mathfrak{p} \cap A$. On en déduit que $\mathfrak{q}$ est un idéal premier non nul de A, donc il est maximal. Le morphisme $A/\mathfrak{q} \to B/\mathfrak{p}$ est injectif et $B/\mathfrak{p}$ est entier sur $A/\mathfrak{q}$. Comme $A/\mathfrak{q}$ est un corps, le Lemme 2.18 implique que $B/\mathfrak{p}$ est aussi un corps.

□

Trace. Fixons désormais les notations et hypothèses du Théorème 3.11, et notons $n = [L : K]$. L'outil principal dans la preuve du Théorème est une forme K-bilinéaire $\langle \cdot, \cdot \rangle : L \times L \to K$, qu'on va maintenant définir. Pour tout $x \in L$, la multiplication par x est une application K-linéaire $m_x : L \to L$, $m_x(y) = xy$. On appelle trace de x la trace de m_x, notée $Tr(x)$. On définit

$$\begin{aligned} \langle \cdot, \cdot \rangle : L \times L &\to K \\ (x, y) &\mapsto Tr(xy). \end{aligned}$$

Les propriétés de la trace qui seront fondamentales pour nous sont données par le lemme suivant.

Lemme 3.13.

1. *Si $b \in B$ alors $Tr(b) \in A$.*
2. *La forme bilinéaire $\langle \cdot, \cdot \rangle$ est non dégénérée.*

Démonstration. 1. Soit $P(X) \in A[X]$ un polynôme unitaire tel que $P(b) = 0$. Soit $M(X) \in K[X]$ le polynôme unitaire de degré minimal tel que $M(b) = 0$. On montrera les deux faits suivants en TD :

— $M(X) \mid P(X)$;

— le polynôme caractéristique de m_b est une puissance de $M(X)$.

Comme $Tr(b)$ est un coefficient du polynôme caractéristique de m_b, il suffit de montrer que $M(X) \in A[X]$. Dans une extension finie du corps K, on

peut écrire $M(X) = (X - \beta_1) \cdots (X - \beta_t)$ avec $b = \beta_1$, ce qui implique que $P(\beta_i) = 0$ pour $1 \leq i \leq t$. Donc

$$M(X) = X^t - (\beta_1 + \ldots + \beta_t)X^{t-1} + (\sum_{1 \leq i < j \leq t} \beta_i \beta_j)X^{t-2} - \ldots \pm \beta_1 \cdots \beta_t$$

a coefficients entiers sur A. Comme $M(X) \in K[X]$ et A est intégralement clos, on déduit que $M(X)$ appartient à $A[X]$.

2. Pour tout $x \in L^\times$, on a $\langle x, x^{-1} \rangle = Tr(1) = n \neq 0$.

□

Preuve du Théorème 3.11. Choisissons, grâce au Lemme 3.10, $b_1, \ldots, b_n \in B$ qui forment un base de L comme $K-$espace vectoriel. Soit $b \in B$; écrivons $b = x_1 b_1 + \ldots + x_n b_n$ avec $x_1, \ldots, x_n \in K$. Pour montrer le théorème, il faut borner les dénominateurs des x_i de façon indépendante de b. Pour $1 \leq j \leq n$, on a

$$bb_j = \sum_{i=1}^{n} x_i b_i b_j, \text{ donc } Tr(bb_j) = \sum_{i=1}^{n} x_i Tr(b_i b_j).$$

De plus, $bb_j \in B$ donc $Tr(bb_j) \in A$ grâce au Lemme 3.13. Soit $\mathsf{T} \in M_{n \times n}(A)$ la matrice dont l'entrée (i, j) est $Tr(b_i b_j)$, et $\mathsf{x} = (x_1, \ldots, x_n)$. La discussion ci-dessus implique que $\mathsf{x}\mathsf{T}$ appartient à A^n, donc

$$\mathsf{x}\mathsf{T}\, {}^t\mathrm{com}\mathsf{T} = \mathsf{x} \det(\mathsf{T}) \in A^n.$$

Le Lemme 3.13 implique que $d = \det(\mathsf{T}) \neq 0$, donc $x_i \in \frac{1}{d}A$ pour $1 \leq i \leq n$. On a donc montré que $B \subset \frac{b_1}{d}A + \ldots + \frac{b_1}{d}A$, donc le Lemme 3.4 implique que B est un A-module de type fini.

Remarque 3.14. *L'argument ci-dessus marche si la caractéristique de K ne divise pas $[L : K]$. En fait, le théorème est vrai si L/K est séparable, ce qui implique que le Lemme 3.13(2) reste vrai.*

Définition 3.15. *Un anneau de Dedekind est un anneau noethérien, intégralement clos, et tel que tout idéal premier non nul est maximal.*

Exemple 3.16.

— *L'anneau des entiers O_L d'un corps de nombres L est un anneau de Dedekind, d'après la Proposition 3.12. Par contre, $\mathbb{Z}[2i]$ n'est pas un anneau de Dedekind, car il n'est pas intégralement clos.*

— *Pour $t \in \mathbb{C}$, l'anneau $\mathbb{C}[X, Y]/(Y^2 - X(X-1)(X-t))$ est de Dedekind si et seulement si $t \neq 0, 1$. On voit dans cet exemple - et on comprendra mieux dans la suite du cours - que la notion d'anneau de Dedekind correspond à la notion géométrique de courbe lisse. Donc, étant donné un anneau intègre $B = \mathbb{C}[X, Y]/(P(X, Y))$, remplacer B par sa clôture intégrale correspond géométriquement à transformer la courbe $\{(x, y) \in \mathbb{C}^2 \mid P(x, y) = 0\}$ en une courbe lisse (résolution des singularités).*

4 Théorème de normalisation de Noether et Nullstellensatz

On fixe un corps k ; si A et B sont des k-algèbres, un morphismes d'anneaux $f : A \to B$ est appelé morphisme de k-algèbres si $f(x) = x$ pour tout $x \in k$. On s'intéresse aux algèbres A de type fini sur k, i.e. telles qu'il existe un morphisme surjectif de k-algèbres $k[X_1, \dots, X_n] \to A$ pour un entier $n \geq 1$. En d'autres termes, on peut écrire $A = k[X_1, \dots, X_n]/I$ pour un idéal $I \subset k[X_1, \dots, X_n]$. On sait d'après le Corollaire 3.7 qu'il existent $P_1, \dots, P_m \in k[X_1, \dots X_n]$ qui engendrent l'idéal I. On note

$$Z_k(I) = \{(x_1, \dots, x_n) \in k^n \mid P_i(x_1, \dots, x_n) = 0 \text{ pour } 1 \leq i \leq m\}.$$

On va montrer deux propriétés clé des "variétés algébriques" $Z_k(I)$, lorsque k est algébriquement clos :

1. Il existe un entier $d \geq 1$ (qui dépend de I) et un "recouvrement fini" $Z_k(I) \to k^d$. Intuitivement, d est la dimension de l'espace $Z_k(I)$.
2. $Z_k(I)$ est déterminé par A : l'application $Z_k(I) \to \mathrm{MaxSpec}(A)$ qui envoie $(x_1, \dots, x_n)$ sur $(X - x_1, \dots, X - x_n)$ est une bijection.

4.1 Théorème de normalisation de Noether

Exemple 4.1. *Soit k un corps et $A = k[X, Y]/(XY - 1)$. On veut munir A d'une structure de $k[T]$-algèbre finie. On a vu que l'application qui envoie T sur X - qui correspond à la projection de l'hyperbole $xy = 1$ sur l'axe $y = 0$ - ne marche pas. On va essayer de projeter l'hyperbole sur une autre droite par l'origine. Algébriquement, posons $X' = X + aY$ avec $a \in k^\times$. On a donc $A = k[X', Y]/((X' - aY)Y - 1)$, ce qui donne l'égalité suivante dans A :*

$$-aY^2 + X'Y - 1 = 0 \Rightarrow Y^2 - \frac{X'}{a}Y + \frac{1}{a} = 0.$$

Donc le morphisme $k[T] \to A$ qui envoie T sur $X + aY$ avec $a \in k^\times$ donne à A la structure d'une $k[T]$-algèbre finie.

Définition 4.2. *Soit k un corps, A une k-algèbre et $x_1, \dots, x_n \in A$. On dit que $x_1, \dots, x_n$ sont algébriquement indépendants sur k si pour tout $P \in k[X_1, \dots, X_n] \setminus \{0\}$ on a $P(x_1, \dots, x_n) \neq 0$. En d'autre termes, l'application*

$$\begin{aligned} ev_{x_1,\dots,x_n} : k[X_1, \dots, X_n] &\to A \\ P &\mapsto P(x_1, \dots, x_n) \end{aligned}$$

est injective.

Théorème 4.3. *(Normalisation de Noether) Soit k un corps et A une k-algèbre de type fini. Il existent un entier $d \geq 0$ et $x_1, \ldots, x_d \in A$ algébriquement indépendants sur k tels que*

$$ev_{x_1,\ldots,x_d} : k[X_1, \ldots, X_d] \to A$$

est une $k[X_1, \ldots, X_d]-$algèbre finie.

Démonstration. On va donner la preuve pour k infini, généralisant la technique dans l'Exemple 4.1. Pour le cas général, cf. [1, Theorem 2.1, p. 357].

Par hypothèse, il existe un morphisme surjectif $f : k[X_1, \ldots, X_n] \to A$ pour un entier $n \geq 0$. Notons $a_i = f(X_i)$ pour $1 \leq i \leq n$. On va montrer l'énoncé par induction sur n ; pour $n = 0$, f est un isomorphisme et l'énoncé est vrai avec $d = 0$. Pour n arbitraire, si f est un isomorphisme alors $f = ev_{a_1,\ldots,a_n}$ satisfait la conclusion du théorème. Sinon, soit $P(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n] \setminus \{0\}$ tel que $P(a_1, \ldots, a_n) = 0$. On va montrer qu'il existent $b_1, \ldots, b_n \in A$ tels que $A = k[b_1, \ldots, b_n]$ et A est une $k[b_1, \ldots, b_{n-1}]-$algèbre finie. Par induction, il existent $x_1, \ldots, x_d \in k[b_1, \ldots, b_{n-1}]$ algébriquement indépendants sur k et tels que $k[b_1, \ldots, b_{n-1}]$ soit une $k[x_1, \ldots, x_d]$-algèbre finie. Le Corollaire 2.12 implique que A est une $k[x_1, \ldots, x_d]$-algèbre finie, donc $ev_{x_1,\ldots,x_d}$ satisfait la conclusion du théorème.

On pose $b_n = a_n$, et on cherche $b_1, \ldots, b_{n-1}$ de la forme $b_i = a_i - \alpha_i a_n$, avec $\alpha_1, \ldots, \alpha_{n-1} \in k$ à déterminer. Écrivons

$$P(X_1, \ldots, X_n) = P_r(X_1, \ldots, X_n) + P_{r-1}(X_1, \ldots, X_n) + \ldots + P_0,$$

avec $P_i(X_1, \ldots, X_n)$ homogène de degré i et $P_r \neq 0$. En particulier,

$$P_r(X_1, \ldots, X_n) = \sum_{i_1+\ldots+i_n=r} c_{i_1,\ldots,i_r} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n},$$

donc

$$P(a_1, \ldots, a_n) = \sum_{i_1+\ldots+i_n=r} c_{i_1,\ldots,i_r} (b_1+\alpha_1 b_n)^{i_1} \cdots (b_{n-1}+\alpha_{n-1} b_n)^{i_{n-1}} b_n^{i_n} + Q(b_1, \ldots, b_n)$$

où $\deg(Q) < r$. Comme $P(a_1, \ldots, a_n) = 0$, on trouve

$$\begin{aligned} 0 &= \left(\sum_{i_1+\ldots+i_n=r} c_{i_1,\ldots,i_r} \alpha_1^{i_1} \cdots \alpha_{n-1}^{i_{n-1}} \right) b_n^r + \text{ termes où } b_n \text{ apparaît avec degré } < r \\ &= P_r(\alpha_1, \ldots, \alpha_{n-1}, 1) b_n^r + \text{ termes où } b_n \text{ apparaît avec degré } < r. \end{aligned}$$

Il reste à montrer qu'il existent $\alpha_1, \ldots, \alpha_{n-1} \in k$ tels que $P_r(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$. Supposons le contraire ; le polynôme P_r étant homogène et non nul, on a

$P_r(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = 0$ pour tout $\alpha_1, \ldots, \alpha_{n-1} \in k$ et $\alpha_n \in k^\times$. On va montrer que ceci n'est pas possible. Écrivons

$$P_r(X_1, \ldots, X_n) = \sum_{i=0}^{t} Q_i(X_1, \ldots, X_{n-1}) X_n^i.$$

Pour tout $\alpha_1, \ldots, \alpha_{n-1} \in k$ le polynôme $P_r(\alpha_1, \ldots, \alpha_{n-1}, X_n) \in k[X_n]$ s'annule sur $k^\times$, donc, comme k est infini, il est nul. On en déduit que $Q_i(X_1, \ldots, X_{n-1}) = 0$ pour $0 \leq i \leq t$, donc $P_r = 0$, contradiction. □

Théorème 4.4. *(Nullstellensatz de Hilbert) Soit k un corps et $n \geq 0$ un entier.*

1. *Soit $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ un idéal maximal. Le quotient $k[X_1, \ldots, X_n]/\mathfrak{m}$ est une extension finie de k.*
2. *Si k est algébriquement clos, alors tout idéal maximal de $k[X_1, \ldots, X_n]$ est de la forme $(X_1 - a_1, \ldots, X_n - a_n)$ avec $(a_1, \ldots, a_n) \in k^n$.*

Démonstration.

1. Le quotient $A = k[X_1, \ldots, X_n]/\mathfrak{m}$ est une k-algèbre de type fini, donc d'après le Théorème 4.3 il existe $d \geq 0$ et un morphisme injectif $k[X_1, \ldots, X_d] \to A$ tel que A soit une $k[X_1, \ldots, X_d]$-algèbre finie. D'après le Lemme 2.18 $k[X_1, \ldots, X_d]$ est un corps, donc $d = 0$.
2. Comme k est algébriquement clos, le point 1. implique que $k[X_1, \ldots, X_n]/\mathfrak{m} \simeq k$. Si $a_i \in k$ dénote l'image de X_i, alors $(X_1 - a_1, \ldots, X_n - a_n) \subset \mathfrak{m}$, donc on a égalité car les deux idéaux sont maximaux.

□

4.2 Dictionnaire algèbre-géométrie

Définition 4.5.

1. *Soit A un anneau et $I \subset A$ un idéal. On appelle radical de I l'ensemble $\sqrt{I} = \{a \in A \mid \exists k \geq 1 : a^k \in I\}$.*
2. *Soit k un corps algébriquement clos. On appelle ensemble algébrique dans k^n un sous-ensemble de la forme $Z_k(I) = \{x \in k^n \mid \forall P \in I, P(x) = 0\}$ pour un idéal $I \subset k[X_1, \ldots, X_n]$.*

Remarque 4.6. *Le radical d'un idéal I est l'image réciproque du radical de l'anneau quotient A/I, donc il est un idéal.*

Géométriquement, le Nullstellensatz de Hilbert nous dit que les idéaux maximaux de $k[X_1, \ldots, X_n]$ avec k algébriquement clos correspondent aux ensembles algébriques les plus simples dans k^n, i.e. les points. Plus en général, il y a un lien étroit entre les idéaux de $k[X_1, \ldots, X_n]$ et les ensembles algébriques dans k^n.

Corollaire 4.7. *Soit k un corps algébriquement clos, $I \subset k[X_1, \ldots, X_n]$ un idéal et $A = k[X_1, \ldots, X_n]/I$. L'application*

$$Z_k(I) \to \mathrm{MaxSpec}(A)$$
$$(x_1, \ldots, x_n) \mapsto (X_1 - x_1, \ldots, X_n - x_n)$$

est bijective.

Démonstration. La bijection du Lemme 1.3(3) induit une bijection entre $\mathrm{SpecMax}(A)$ et l'ensemble $\{\mathfrak{m} \in \mathrm{MaxSpec}(k[X_1, \ldots, X_n]) \mid \mathfrak{m} \supset I\}$. Pour $(x_1, \ldots, x_n) \in k^n$, on a $(X - x_1, \ldots, X - x_n) \supset I$ si et seulement si $P(x_1, \ldots, x_n) = 0$ pour tout $P \in I$, i.e. si et seulement si $(x_1, \ldots, x_n) \in Z_k(I)$. Le corollaire découle donc du Théorème 4.4. □

Dans la preuve du théorème 4.9 ci-dessous on va se servir du fait suivant, qu'on pourra comprendre de façon plus conceptuelle plus tard en termes de localisation des anneaux.

Lemme 4.8. *Soit A un anneau, $a \in A$ et $B = A[X]/(aX - 1)$. Si $a \in A$ n'est pas nilpotent alors B n'est pas l'anneau nul.*

Démonstration. Supposons par l'absurde que $1 = (aX - 1)Q(X) \in A[X]$ avec $Q(X) = a_d X^d + \ldots + a_0 \in A[X]$. La comparaison des termes constants donne $1 = -a_0$. En regardant les coefficients de X on trouve $0 = aa_0 - a_1$ donc $a_1 = -a$. De la même façon, la comparaison des coefficients de $X^2, X^3, \ldots, X^d$ montre que $aa_{i-1} - a_i = 0$ donc $a_i = -a^i$ pour $2 \leq i \leq d$. Mais le terme de degré $d + 1$ de $(aX - 1)Q(X)$ est alors $-a^{d+1}X^{d+1}$, qui est non nul car a n'est pas nilpotent. □

Théorème 4.9. *(Nullstellensatz, version forte) Soit k un corps algébriquement clos et $A = k[X_1, \ldots, X_n]$.*

1. *Soit I un idéal et $P \in A$ tel que $P(x) = 0$ pour tout $x \in Z_k(I)$. Alors $P \in \sqrt{I}$.*
2. *L'application $I \mapsto Z_k(I)$ induit une bijection entre idéaux $I \subset A$ tels que $\sqrt{I} = I$ (i.e. l'anneau A/I est réduit) et ensembles algébriques dans k^n.*

Démonstration. 1. Soit $B = A/I$. Si $P \notin \sqrt{I}$ alors P n'est pas nilpotent dans B, donc $B[Y]/(PY - 1)$ n'est pas l'anneau nul d'après le Lemme 4.8. Il s'agit d'une k-algèbre de type fini, qui possède un idéal maximal d'après la Proposition 1.16. Grâce au Théorème 4.4, un tel idéal nous donne un morphisme de k-algèbres $\varphi : B[Y]/(PY - 1) \to k$. On regarde le morphisme composé

$$A \to A/I = B \to B[Y]/(PY - 1) \xrightarrow{\varphi} k. \tag{4.1}$$

D'après le Théorème 4.4 sont noyau $\mathfrak{m}$ est de la forme $(X - x_1, \ldots, X - x_n)$ pour $x = (x_1, \ldots, x_n) \in k^n$. On a $I \subset \mathfrak{m}$ donc $x \in Z_k(I)$. D'autre part, l'image de $P \in A$ par la composition des morphismes dans (4.1) est une unité dans k, donc $P(x) \neq 0$.

2. On a $Z_k(I) = Z_k(\sqrt{I})$, donc l'application est surjective. Soient I, J deux idéaux tels que $Z_k(I) = Z_k(J)$ et $\sqrt{I} = I, \sqrt{J} = J$. Pour tout $P \in J$ on a $P \in \sqrt{I}$ d'après 1., donc $J \subset \sqrt{I} = I$. Échangeant les rôles de I et J on trouve que $I \subset J$, donc $I = J$.

□

Remarque 4.10. *Les résultats de cette section nous disent que l'anneau $k[X_1, \ldots, X_n]$ contient assez d'information pour retrouver l'ensemble des points de n'importe quel ensemble algébrique. Ceci n'est que le début de l'histoire :*

- *on aurait envie de donner plus de structure - par exemple une topologie - aux ensembles algébriques ;*
- *Dans le passage des idéaux aux ensembles algébriques on perd de l'information - en gros, on "oublie les nilpotents". Cependant, même si l'on s'intéresse uniquement aux ensembles algébriques, des anneaux comme $k[T]/(T^2)$ peuvent être très utiles : par exemple, quels sont les morphismes de k-algèbres $k[X, Y]/(Y^2 - X) \to k[T]/(T^2)$?*

Extensions finies de k-algèbres de type fini. Soit k un corps algébriquement clos, et soient $A = k[X_1, \ldots, X_n]/I$ et $B = k[X_1, \ldots, X_m]/J$ deux k-algèbres de type fini. Soit $f : A \to B$ un morphisme de k-algèbres. Tout d'abord, pour tout $\mathfrak{m} \in \mathrm{MaxSpec}(B)$ on a $f^{-1}(\mathfrak{m}) \in \mathrm{MaxSpec}(A)$. En effet, on a

$$k \to A/f^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m} \simeq k$$

donc tout morphisme ci-dessus est un isomorphisme. En conséquence, le morphisme f induit une application $f^* : \mathrm{MaxSpec}(B) \to \mathrm{MaxSpec}(A)$ qui, via la bijection du Corollaire 4.7, donne une application

$$\tilde{f} : Z_k(J) \to Z_k(I).$$

Corollaire 4.11. *Si $f : A \to B$ est injective et B est une A-algèbre finie, alors pour tout $(x_1, \ldots, x_n) \in Z_k(I)$ l'image réciproque $\tilde{f}^{-1}(x_1, \ldots, x_n)$ est finie et non vide.*

Démonstration. On identifie A avec son image dans B. Soit $\mathfrak{m} = (X - x_1, \ldots, X - x_n) \in \mathrm{MaxSpec}(A)$. Alors

$$(f^*)^{-1}(\mathfrak{m}) = \{\mathfrak{m}' \in \mathrm{MaxSpec}(B) \mid \mathfrak{m}' \supset \mathfrak{m}\} \simeq \mathrm{MaxSpec}(B/\mathfrak{m}B).$$

Comme $B/\mathfrak{m}B$ est une $A/\mathfrak{m}A \simeq k-$algèbre finie, la Proposition 2.19 implique que $(f^*)^{-1}(\mathfrak{m})$ est fini. Le fait qu'il soit non vide est une conséquence de la Proposition 2.16. □

5 Rappels de topologie générale

Définition 5.1. *Un espace topologique est un couple $(X, \mathcal{T})$ où X est un ensemble non-vide et $\mathcal{T}$ est un ensemble de parties de X telles que*

1. $(\emptyset, X) \in \mathcal{T}^2$;
2. $\mathcal{T}$ *est stable par union quelconque ;*
3. $\mathcal{T}$ *est stable par intersection finie.*

Les éléments de $\mathcal{T}$ sont appelés les ouverts de la topologie $\mathcal{T}$ et les complémentaires des ouverts dans X sont les fermés de la topologie $\mathcal{T}$.

Exemple 5.2. *On dispose toujours sur un ensemble X non-vide de deux topologies extrêmes :*

1. *la topologie grossière, pour laquelle $\mathcal{T} = \{\emptyset, X\}$;*
2. *la topologie discrète, pour laquelle $\mathcal{T} = \mathcal{P}(X)$.*

La topologie discrète est la topologie la plus fine (tout sous-ensemble de X est un ouvert) tandis que la topologie grossière l'est le moins possible. On a présenté ici le point de vue le plus classique, où la topologie $\mathcal{T}$ est constituée par les ouverts. On peut définir une topologie -nous le feront plus tard- en construisant un ensemble $\mathcal{F}$ de fermés, qui vérifient la condition 1. précédente, tel que $\mathcal{F}$ est stable par intersection quelconque et par union finie, et en prenant pour $\mathcal{T}$ les complémentaires des éléments de $\mathcal{F}$.

Définition 5.3. *Si $(X, \mathcal{T})$ est un espace topologique et $Y \subset X$ est un sous-ensemble, l'ensemble*

$$\mathcal{T}_Y := \{U \cap Y,\ U \in \mathcal{T}\}$$

définit une topologie sur Y, qu'on appelle la topologie induite.

Définition 5.4. *Si $(X, \mathcal{T})$ est un espace topologique $Y \subset X$ est un sous-ensemble, l'adhérence de Y, notée $\overline{Y}$, est le plus petit fermé qui contient Y. On dit que $Y \subset X$ est une partie dense si $\overline{Y} = X$.*

Définition 5.5. *Si $(X, \mathcal{T})$ est un espace topologique, un sous-ensemble $\mathcal{B} \subset \mathcal{T}$ est une base d'ouverts si tout élément de $\mathcal{T}$ est une union d'éléments de $\mathcal{B}$.*

Exemple 5.6. *Dans le cadre d'un espace métrique (X, d), on a par définition que la topologie associée à d est donnée par*

$$\mathcal{T}_d = \{U \in \mathcal{P}(X),\ \forall x \in U, \exists r > 0,\ B_d(x, r) \subset U\}$$

où $B_d(x, r)$ désigne la boule ouverte de centre x et de rayon r. On montre sans peine que les boules ouvertes forment une base de la topologie $\mathcal{T}_d$.

Définition 5.7. *Un espace topologique $(X, \mathcal{T})$ est séparé (ou de Hausdorff) si*

$$\forall (x, y) \in X^2,\ x \neq y,\ \exists (U_1, U_2) \in \mathcal{T}^2,\ (x \in U_1,\ y \in U_2 \text{ et } U_1 \cap U_2 = \emptyset)$$

Les espaces métriques vérifient toujours cette propriété puisqu'on peut séparer les points avec des boules ouvertes. Les topologies que nous rencontreront par la suite ne la satisferont que rarement (les espaces auxquels nous auront affaire ne seront donc pas «métrisables»).

Définition 5.8. *Un espace topologique $(X, \mathcal{T})$ est quasi-compact, si de tout recouvrement*

$$E = \bigcup_{i \in \mathcal{I}} U_x$$

par des ouverts, on peut extraire un sous-recouvrement fini $E = \bigcup_{j=1}^{n} U_j$.

Un espace topologique $(X, \mathcal{T})$ est compact s'il est à la fois quasi-compact et séparé. On peut bien sûr définir de manière équivalente la quasi-compacité grâce aux fermés, par passage au complémentaire : un espace topologique $(X, \mathcal{T})$ est quasi-compact si de toute famille de fermés d'intersection vide, on peut extraire une famille *finie* de fermés d'intersection vide.

Définition 5.9. *Un espace topologique $(X, \mathcal{T})$ est connexe si X ne s'écrit pas comme la réunion disjointe de deux ouverts non-vides (ou de manière équivalente celle de deux fermés non-vides).*

Définition 5.10. *Soient $(X, \mathcal{T})$ et $(X, \mathcal{T}')$ deux espaces topologiques. Une application $f : X \longrightarrow X'$ est continue si pour tout ouvert $U \in \mathcal{T}'$, on a $f^{-1}(U) \in \mathcal{T}$.*

Un homéomorphisme entre les espace $(X, \mathcal{T})$ et $(X, \mathcal{T}')$ est une application continue $f : X \longrightarrow X'$ bijective et d'inverse $f^{-1} : X' \longrightarrow X$ continue.

6 Topologies de Zariski

Étant donné un anneau A, on note $\mathrm{MaxSpec}(A)$ l'ensemble de ses idéaux maximaux. Comme vous l'avez vu en première partie du cours, on dispose en vertu du théorème des zéros de Hilbert d'une identification

$$\mathbb{C}^n \simeq \mathrm{MaxSpec}(\mathbb{C}[X_1, ..., X_n])$$

entre « l'espace affine » $\mathbb{C}^n$ et les idéaux maximaux de l'anneau $\mathbb{C}[X_1, .., X_n]$. Le Corollaire 4.7 pousse plus loin l'analogie pour les sous-ensembles de $\mathbb{C}^n$ solutions d'un système d'équations algébriques $\mathcal{S}$: l'ensemble

$$Z(\mathcal{S}) = \{(x_1, ..., x_n) \in \mathbb{C}^n, \forall P \in \mathcal{S},\ P(x_1, ..., x_n) = 0\}$$

correspond alors à $\mathrm{MaxSpec}(\mathbb{C}[X_1, ..., X_n]/I)$, où I est l'idéal de $\mathbb{C}[X_1, ..., X_n]$ engendré par les éléments de $\mathcal{S}$.

Le résultat vaut toujours pour n'importe quel corps algébriquement clos, et dresse un pont entre les problèmes algébriques (idéaux dans un anneau) et une intuition géométrique (points dans un espace). La généralisation de cette philosophie à n'importe quel anneau est un grand défi réalisé par la géométrie algébrique, que nous allons aborder dans cette seconde partie du cours.

Une première différence, dès lors qu'on considère des anneaux quelconques, est le défaut de fonctorialité de MaxSpec : si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux, l'image réciproque d'un idéal maximal de B n'est pas toujours un idéal maximal de A. À défaut de considérer dans la suite l'ensemble MaxSpec, on associera plutôt à un anneau A son spectre, c'est à dire l'ensemble de ses idéaux *premiers*.

Exercice 6.1. *Montrer que si A et B sont deux anneaux, on a*

$$\mathrm{Spec}(A \times B) = \mathrm{Spec}(A) \sqcup \mathrm{Spec}(B).$$

Définition 6.2. *Si A est un anneau, on associe à tout idéal I de A l'ensemble*

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A),\ I \subset \mathfrak{p}\}$$

des idéaux premiers de A qui le contiennent.

Théorème 6.3 (Krull)**.** *Tout idéal propre d'un anneau A est contenu dans un idéal maximal. En particulier, $V(I)$ est vide si et seulement si $I = A$.*

Démonstration. C'est la Proposition 1.16 appliquée à l'anneau A/I (on peut aussi faire la preuve de manière similaire à la preuve de la Proposition 1.16, en choisissant pour $\mathcal{I}$ l'ensemble des idéaux propres qui contiennent I). Ainsi si $I \neq A$, l'idéal I est contenu dans un idéal maximal et $V(I) \neq \emptyset$. □

Nous verrons que les ensembles $V(I)$, où I parcoure les idéaux de A, jouent le rôle des ensembles algébriques donnés par des équations polynomiales.

Proposition 6.4. *Soit A un anneau. Les ensembles $V(I)$, où I parcoure tous les idéaux de A, sont les fermés d'une topologie sur* $\mathrm{Spec}(A)$.

Démonstration. D'une part, les deux ensembles $\mathrm{Spec}(A) = V(\{0\})$ et $\emptyset = V(A)$ s'écrivent bien de cette manière. De plus, si $\{V(I_x)\}_{x\in\mathfrak{X}}$ est une famille de tels sous-ensembles, on a

$$\bigcap_{x\in\mathfrak{X}} V(I_x) = V(< I_x >_{x\in\mathfrak{X}}).$$

En effet si $\mathfrak{p}$ contient l'idéal engendré par les I_x, alors $I_x \subset \mathfrak{p}$ pour tout $x \in \mathfrak{X}$. Réciproquement si $\mathfrak{p}$ est un idéal premier qui contient les I_x, pour tout $x \in \mathfrak{X}$, alors il contient l'idéal qu'ils engendrent.

Enfin, montrons que si I et J sont deux idéaux de A, on a

$$V(I) \cup V(J) = V(IJ).$$

$\boxed{\subset}$ Si $\mathfrak{p}$ est un idéal premier qui contient disons I, alors il contient $I \cap J$. Comme on a $IJ \subset I \cap J$, on a bien $\mathfrak{p} \in V(IJ)$.
$\boxed{\supset}$ Soit $\mathfrak{p}$ un idéal premier qui contient IJ. Si I n'est pas contenu dans $\mathfrak{p}$, alors en prenant un élément $i \in I \setminus \mathfrak{p}$, on a $ij \in \mathfrak{p}$ pour tout $j \in J$. L'idéal $\mathfrak{p}$ étant premier on a donc $J \subset \mathfrak{p}$. □

Définition 6.5. *La topologie définie par les fermés $V(I)$ sur* $\mathrm{Spec}(A)$ *est la topologie de Zariski. On dit qu'un espace topologique $(X, \mathcal{T})$ est spectral s'il est homéomorphe au spectre d'un anneau, muni de la topologie de Zariski.*

Les ouverts pour la topologie de Zariski sur $\mathrm{Spec}(A)$ sont donc de la forme $\mathrm{Spec}(A) \setminus V(I)$, pour un idéal $I \subset A$. Si a est un élément de A, on pose

$$D(a) = \{\mathfrak{p} \in \mathrm{Spec}(A),\ a \notin \mathfrak{p}\} = \mathrm{Spec}(A) \setminus V(< a >).$$

Les ouverts de cette forme sont appelés les *ouverts standards*. Les ouverts standards sont une base pour la topologie de Zariski puisqu'on a l'égalité

$$V(I) = \bigcap_{i\in I} V(< i >),$$

pour tout idéal I de A.

Remarque 6.6. *Pour la topologie de Zariski, $V(\mathfrak{p})$ est naturellement l'adhérence de l'idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$.*

Exemple 6.7. *La topologie de Zariski sur le spectre* $\mathrm{Spec}(A \times B)$ *d'un produit d'anneaux est la topologie naturelle sur l'union disjointe de* $\mathrm{Spec}(A)$ *et* $\mathrm{Spec}(B)$.

Proposition 6.8. *Pour tout idéal I d'un anneau A, on a*

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

Démonstration. D'un part l'inclusion $I \subset \sqrt{I}$ implique que $V(\sqrt{I}) \subset V(I)$.

Réciproquement, soit $\mathfrak{p}$ un idéal premier qui contient I. Si $x \in \sqrt{I}$, on a pour un certain $n \in \mathbb{N}^*$, $x^n \in I \subset \mathfrak{p}$. En particulier $x \in \mathfrak{p}$ car $\mathfrak{p}$ est premier et $\sqrt{I} \subset \mathfrak{p}$. □

6.1 Propriétés topologiques

La topologie de Zariski apparait naturellement pour étudier les ensembles algébriques, mais elle s'éloigne des topologies que vous avez rencontrées pour l'instant, notamment des espaces métriques, à bien des égards.

Proposition 6.9. *Le spectre de tout anneau A est quasi-compact.*

Démonstration. Soit $(I_x)_{x\in\mathfrak{X}}$ une famille d'idéaux tel que $\bigcap_{x\in\mathfrak{X}} V(I_x) = \emptyset$. On a donc par le lemme 6.3 et la proposition 6.4

$$< (I_x)_{x\in\mathfrak{X}} >= A.$$

Il existe ainsi une famille finie d'indices $x_1, ..., x_n$ de $\mathfrak{X}$ et des éléments $i_1, ..., i_n$ de $I_{x_1}, ..., I_{x_n}$ tels que $i_1 + i_2 + ... + i_n = 1$. On a donc $\bigcap_{i=1}^{n} V(I_x) = V(A) = \emptyset$, ce qui permet d'extraire un recouvrement fini du recouvrement ouvert

$$A = \bigcup_{x\in\mathfrak{X}} \mathrm{Spec}(A) \setminus V(I_x).$$

□

Définition 0.1. Un espace topologique $(X, \mathcal{T})$ est noethérien si toute chaîne décroissante de fermés

$$X \supset F_1 \supset F_2 \supset F_3 \supset ...$$

est stationnaire.

Proposition 6.10. *Muni de la topologie de Zariski, le spectre d'un anneau noétherien est un espace noethérien.*

Démonstration. L'assignation $I \mapsto V(I)$ renverse le sens des inclusions. □

Exemple 6.11. *La réciproque à la proposition 6.10 est fausse, en considérant*

$$A = \mathbb{C}[x_1, x_2, x_3, ...]/ < x_1^2, x_2^2, x_3^2, ... > .$$

On verra en effet par la suite (proposition 6.20) qu'ici $\mathrm{Spec}(A)$ *est réduit à* 1 *point. Pourtant, A n'est pas noethérien puisque la chaine d'idéaux*

$$< x_1 > \subset < x_1, x_2 > \subset < x_1, x_2, x_3 > \subset ...$$

n'est pas stationnaire.

Le résultat suivant montre que la topologie de Zariski sur le spectre d'un anneau n'est que rarement métrisable.

Proposition 6.12. *Muni de la topologie de Zariski,* $\mathrm{Spec}(A)$ *est séparé si et seulement si tout idéal premier de* A *est maximal.*

Démonstration. Supposons que tout idéal premier $\mathfrak{p}$ de A est maximal. Si $\mathfrak{q}$ est un autre idéal premier de A, on prend un élément $a \in \mathfrak{p}$ tel que $a \notin \mathfrak{q}$. On verra en exercice de TD qu'on a alors un élément $s \in A \setminus \mathfrak{p}$ et un entier $n \in \mathbb{N}^*$ tel que $sa^n = 0$. On a alors bien $\mathfrak{q} \in D(a)$, $\mathfrak{p} \in D(s)$, et

$$D(a) \cap D(s) = D(sa) = D(sa^n) = D(0) = \emptyset.$$

On a en effet $D(sa) = D(sa^n)$: si un idéal premier $\mathfrak{r}$ contient sa, il contient sa^n donc $D(sa^n) \subset D(sa)$. Réciproquement si $\mathfrak{r}$ idéal premier contient sa^n, alors il contient s ou a, donc dans les deux cas il contient sa et $D(sa) \subset D(sa^n)$. L'espace spectral $\mathrm{Spec}(A)$ est donc séparé.

Réciproquement, supposons que A contienne un idéal $\mathfrak{p}$ premier qui n'est pas maximal, et notons $\mathfrak{m}$ un idéal maximal qui le contient. Si $U \subset \mathrm{Spec}(A)$ est un ouvert ne contenant pas $\mathfrak{p}$, alors son complémentaire U^c contient $\mathfrak{p}$, donc son adhérence $V(\mathfrak{p})$ qui contient elle même $\mathfrak{m}$. En particulier $\mathfrak{m}$ n'est pas non plus un élément de U et $\mathrm{Spec}(A)$ n'est pas séparé. □

On rappelle que si A est un anneau, un élément $a \in A$ est un idempotent s'il vérifie $a^2 = a$. La définition suivante permet de caractériser la connexité de l'espace topologique $\mathrm{Spec}(A)$ en fonction des propriétés algébriques de A.

Définition 6.13. *Un anneau* A *est connexe si les seuls idempotents de* A *sont les idempotents triviaux* 0 *et* 1.

Remarque 6.14. *Si* a *idempotent dans* A, $1 - a$ *est lui aussi idempotent.*

Proposition 6.15. *Un anneau* A *est connexe si et seulement s'il n'est pas isomorphe au produit* $B \times C$ *de deux anneaux non triviaux.*

Démonstration. vue en TD.

□

Théorème 6.16. *Soit* A *un anneau. Les assertions suivantes sont équivalentes :*

1. *muni de la topologie de Zariski,* $\mathrm{Spec}(A)$ *est connexe ;*
2. A *est connexe*
3. A *ne se décompose pas en un produit* $B \times C$ *d'anneaux non-triviaux.*

Démonstration. vue en TD. □

6.2 Spectres et quotients

Le choix des idéaux premiers au début de ce cours permet notamment de rendre l'association $A \mapsto \mathrm{Spec}(A)$ fonctorielle.

Proposition 6.17. *Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux, alors l'application $\varphi^\sharp : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ induite donnée par $\varphi^\sharp(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ est continue pour la topologie de Zariski.*

Démonstration. L'image réciproque d'un idéal premier demeure un idéal premier, donc l'application $\varphi^\sharp$ est bien définie.

Si I est un idéal de A, on a

$$\begin{aligned}(\varphi^\sharp)^{-1}(V(I)) &= \{\mathfrak{p} \in \mathrm{Spec}(B),\ \varphi^\sharp(\mathfrak{p}) \in V(I)\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(B),\ I \subset \varphi^{-1}(\mathfrak{p})\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(B),\ \varphi(I) \subset \mathfrak{p}\} \\ &= V(< \varphi(I) >)\end{aligned}$$

L'image réciproque d'un fermé est donc fermée et $\varphi^\sharp$ est continue. □

Théorème 6.18. *Si A est un anneau et I un idéal de A, alors $V(I)$ muni de la topologie induite par celle de Zariski sur $\mathrm{Spec}(A)$ est un espace spectral, homéomorphe à $\mathrm{Spec}(A/I)$.*

Démonstration. En notant $\pi : A \longrightarrow A/I$ la projection canonique, le Lemme 1.13 (2) assure que les applications $\mathfrak{p} \mapsto \pi(\mathfrak{p})$ et $\pi^\sharp$ sont des bijections réciproques, continues par la Proposition 6.17. □

Remarque 6.19. *On montrera par la suite que les ouverts standards $D(a)$ de $\mathrm{Spec}(A)$ sont aussi des espaces spectraux.*

On en déduit que la topologie de Zariski ne «voit pas» les éléments nilpotents... Nous n'aborderons pas ce sujet dans le cours plus en détails, il faudra pour en savoir plus continuer à étudier la géométrie algébrique.

Corollaire 6.20. *Si A est un anneau, alors $\mathrm{Spec}(A)$ et $\mathrm{Spec}(A/\sqrt{0})$ sont homéomorphes.*

Démonstration. Comme vu en première partie du cours, le nilradical $\sqrt{0}$ de A est l'intersection de tous ses idéaux premiers. Tout idéal premier $\mathfrak{p}$ contient $\sqrt{0}$ et l'application induite par le quotient $A \longrightarrow A/\sqrt{0}$ est un homéomorphisme. □

Exercice 6.21. *Soit k un corps. On considère l'algèbre des nombres duaux*

$$k[\varepsilon] := \{a + b\varepsilon,\ (a, b) \in k^2\}$$

obtenue en adjoignant l'élément ε sujet à la relation $\varepsilon^2 = 0$.

1. *Donner la structure d'anneau de $k[\varepsilon]$. Est-ce un corps ?*
2. *Déterminer les inversibles de $k[\varepsilon]$.*
3. *Décrire* $\mathrm{Spec}(k[\varepsilon])$ *et sa topologie de Zariski.*

6.3 Spectres irréductibles, composantes

Définition 6.22. *Un espace topologique $(X, \mathcal{T})$ est irréductible si X ne se décompose pas en une union de deux fermés stricts et non-vides.*

Un espace topologique irréductible est donc nécessairement connexe car l'union dans la définition 6.22 n'est pas disjointe.

Définition 0.2. Une composante irréductible d'un espace topologique X est un fermé irréductible (pour la topologie induite) maximal pour l'inclusion.

Proposition 6.23. *Tout espace topologique est recouvert par ses composantes irréductibles.*

Démonstration. Pour $x \in X$, on applique le lemme de Zorn à l'ensemble $\mathfrak{I}_x$ des sous-ensembles irréductibles (pour la topologie induite) de X qui contiennent x. D'une part $\mathfrak{I}_x$ contient le singleton $\{x\}$, donc est non-vide. Soit $(X_j)_{j\in J}$ une famille totalement ordonnée de $\mathfrak{I}_x$; posons

$$X' = \bigcup_{j\in J} X_j.$$

Soit $X' = Y \cup Z$ une décomposition de X' en deux fermés. Un élément $j_0 \in J$ étant fixé on a soit $X_{j_0} \subset Y$, soit $X_{j_0} \subset Z$ car X_{j_0} est irréductible. Dès lors comme tous les X_j satisfont cette propriété, si l'on a disons $X_{j_0} \subset Y$, alors $X_j \in Y$ pour tout $j \in J$ car la famille $(X_j)_{j\in J}$ est totalement ordonnée et tous ses éléments intersectent Y. On a donc $X' = Y$ et l'espace X' est irréductible. La famille $\mathfrak{I}_x$ contient donc un élement maximal et x est contenu dans une composante irréductible. □

Lemme 6.24. *Soit X un espace topologique.*

1. *Si Y est un sous-ensemble irréductible de X, son adhérence est irréductible.*
2. *Les composantes irréductibles de X sont fermées.*
3. *Si X est irréductible, tout ouvert non-vide de X est dense.*

Démonstration.

1. Considérons une décomposition $\overline{Y} = Y_1 \cup Y_2$ de l'adhérence de Y en deux fermés. On a $Y = (Y \cap Y_1) \cup (Y \cap Y_2)$ donc par irréductibilité, disons $Y = Y \cap Y_1$, et ainsi $\overline{Y} = \overline{Y \cap Y_1} \subset Y_1$.
2. Immédiat d'après 1. par maximalité.

3. Si O soit un ouvert non-vide et non-dense de X, le complémentaire O' de son adhérence est un ouvert non-vide, car $\overline{O} \neq X$. On voit alors que $O \cap O' = \emptyset$, c'est à dire que $O^c \cup O'^c = X$, ce qui contredit l'irréductibilité de X.

□

Proposition 6.25. *Soit A un anneau et I un idéal de A.*

1. *Les points fermés de* $\mathrm{Spec}(A)$ *correspondent aux idéaux maximaux.*
2. *$V(I) \subset \mathrm{Spec}(A)$ est irréductible si et seulement si I est premier.*

Démonstration. 1. L'adhérence d'un idéal $\mathfrak{p} \in \mathrm{Spec}(A)$ est $V(\mathfrak{p})$. Il est donc clair que $\mathfrak{p}$ est un point fermé fermé si et seulement si $V(\mathfrak{p}) = \{\mathfrak{p}\}$, c'est à dire si l'idéal $\mathfrak{p}$ est maximal.

2. Si $\mathfrak{p}$ est un idéal premier, on a $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$ irréductible, par le lemme 6.24. Considérons maintenant $V(I)$ irréductible. En vertu de la proposition 6.8, on peut supposer que I est radical (c'est à dire $\sqrt{I} = I$).

   Supposons que I n'est pas premier et prenons a, b de A n'appartenant pas à I, mais tels que $ab \in I$. On a

   $$V(I) = V(< I, a >) \cup V(< I, b >)$$

   (si $\mathfrak{p}$ contient I, il contient alors ab, donc soit a, soit b).

   En outre on $V(< I, a >) \subsetneq V(I)$, car sinon a appartient à tout idéal premier contenant I et a est un élément de

   $$\bigcap_{I \subset \mathfrak{p}} \mathfrak{p} = \sqrt{I} = I,$$

   ce qui contredit l'irréductibilité de $V(I)$. L'idéal I est donc premier.

□

On peut ainsi obtenir une caractérisation purement algébrique des composantes irréductibles pour la topologie de Zariski.

Théorème 6.26. *Tout fermé irréductible de* $\mathrm{Spec}(A)$ *est l'adhérence d'un unique idéal premier $\mathfrak{p}$ de A. On obtient ainsi une bijection*

$$\{\textit{idéaux premiers de } A\} \simeq \{\textit{fermés irréductibles de } \mathrm{Spec}(A)\}.$$

Les composantes irréductibles de $\mathrm{Spec}(A)$ *sont de la forme $V(\mathfrak{p})$, où $\mathfrak{p}$ est un idéal premier minimal de A.*

Démonstration. D'après la proposition 6.25, tout fermé irréductible de $\mathrm{Spec}(A)$ est de la forme $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, où $\mathfrak{p}$ est un idéal premier. L'unicité de $\mathfrak{p}$ est claire puisque $V(\mathfrak{p}) = V(\mathfrak{q})$ implique $\mathfrak{p} = \mathfrak{q}$ (les deux sont premiers).

La bijection obtenue est décroissante, les composantes irréductibles de $\mathrm{Spec}(A)$ correspondent donc aux idéaux premiers minimaux de A. □

Corollaire 6.27. *Le spectre* $\mathrm{Spec}(A)$ *d'un anneau* A *est irréductible si et seulement si le nilradical de* A *est un idéal premier.*

Démonstration. En vertu du théorème 6.26, $\mathrm{Spec}(A)$ est irréductible si et seulement s'il possède un unique idéal premier minimal. L'égalité

$$\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} = \sqrt{0}$$

indique que cette situation correspond au cas où le nilradical de A est premier. □

7 Localisation

Le corps des nombres rationnels est construit formellement à partir $\mathbb{Z}$, en inversant tous les entiers non-nuls. La construction que vous connaissez se généralise à n'importe quel anneau intègre A et mène à son *corps des fractions*.

La généralisation de ce processus pour les anneaux quelconques est la *localisation*. Dans cette partie nous définissons les localisés d'un anneau vis-à-vis d'une partie multiplicative. Cette description nous permet de montrer que munis de la topologie de Zariski, les ouverts standards sont des espaces spectraux.

7.1 Définition et propriété universelle

Définition 7.1. *Un sous-ensemble* S *d'un anneau* A *est une partie multiplicative si* S *est stable par multiplication, contient* 1 *mais ne contient pas* 0.

Exemple 7.2.
1. *L'ensemble* $A^\times$ *des éléments inversibles de* A *est une partie multiplicative (qui s'avère peu intéressante pour la localisation).*
2. *Si* $a \in A$ *n'est pas nilpotent, le sous ensemble* $S_a = \{1, a, a^2, ...\}$ *des puissances de* a *est une partie multiplicative.*

Si A est un anneau et S est une partie multiplicative de A, on veut mimer la construction du corps des fractions. On voudrait donc considérer l'ensemble $S^{-1}A$ des «fractions» $\frac{a}{s} = (a, s) \in A \times S$ avec dénominateur dans S, munies des additions et multiplications habituelles, telles que $(a, s) = (b, t)$ dès lors que $at = bs$.

On remarque cependant qu'il faut faire attention : si s et a sont des éléments respectifs de S et A tels que $sa = 0$, alors on veut que a soit nul dans tout anneau où s est inversible, c'est à dire

$$(a, 1) = (0, 1)$$

sans pour autant avoir $a = 0$, qui est pourtant immédiat avec la relation classique des fractions. Pour éviter cet écueil, on définit donc $S^{-1}A$, la localisation de A par

S, en posant $S^{-1}A = A \times S$, avec les additions et multiplications habituelles, mais modulo la relation

$$(a, s) \sim (b, t) \Leftrightarrow \text{il existe } x \in S \text{ tel que } x(at - bs) = 0.$$

Lemme 7.3. *La relation $\sim$ précédente sur $A \times S$ une relation d'équivalence.*

Démonstration. La relation est clairement réflexive et symétrique. Si on a

$$(a, s) \sim (b, t) \sim (c, u),$$

avec donc x et y dans A tels que $x(at - bs) = 0 = y(bu - ct)$, alors en focalisant autour de l'élément b et en saturant par des éléments de S, on voit que

$$bsxyu = atxyu \text{ et } bsxyu = ctysx,$$

on a donc bien $txy(au - sc) = 0$, avec $txy \in S$ car cette dernière est multiplicative. □

Définition 7.4. *L'ensemble quotient de $A \times S$ par la relation d'équivalence précédente est noté $S^{-1}A$, et appelé le localisé de A en la partie multiplicative S.*

Pour tout $(a, s) \in A \times S$, on note dans la suite $[a, s]$ la classe d'équivalence associée dans $S^{-1}A$. On a loisir d'écrire aussi ces classes sous formes de fractions, ce qui s'avère parfois pratique pour les calculs.

Proposition 7.5. *Muni des lois*

$$[a, s] \cdot [b, t] = [ab, st] \text{ et } [a, s] + [b, t] = [at + bs, st]$$

l'ensemble $S^{-1}A$ est muni d'une structure d'anneau. L'application

$$\begin{array}{rccc} \iota : & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & [a, 1] \end{array}$$

est un morphisme d'anneaux.

Démonstration. Il faut vérifier que ces lois sont bien définies. Si on a $[a, s] = [a', s']$, c'est à dire $x(as' - a's) = 0$ pour un $x \in S$, alors on a

$$abs'tx = a'bstx$$

et donc $[a'b, s't] = [ab, st]$. En outre l'égalité

$$(at + bs)s'x = ats'x + bss'x = ta'sx + bss'x = (at' + bs')sx$$

indique que $(at+bs)s'tx = (at'+bs')stx$, c'est à dire

$$[at+bs, st] = [at'+bs', s't].$$

Le même raisonnement en choisissant un autre représentant à $[b,t]$ montre que ces opérations sont bien définies. De la même manière que pour la construction de $\mathbb{Q}$ ou des corps de fractions, on voit facilement que muni de ces lois, $S^{-1}A$ est un anneau, dont le 0 est la classe $[0,1]$ et dont l'unité est la classe $[1,1]$. L'application ι est ainsi naturellement un morphisme d'anneaux. □

Remarque 7.6. *L'anneau $S^{-1}A$ ne peut être l'anneau nul sous nos hypothèses, car $[1,1] \neq 0$ (sinon 0 appartiendrait à S).*

Lemme 7.7. *Soit A un anneau et S une partie multiplicative de A. Alors*

$$\ker(\iota) = \{a \in A,\ \exists s \in S, sa = 0\}.$$

En particulier si A est intègre, le morphisme ι est injectif.

Démonstration. On a que $a \in \ker(\iota)$ si et seulement si $[a,1] = [0,1]$, c'est à dire qu'il existe un élément $s \in S$ tel que $sa = 0$. Lorsque A est intègre, sachant que S ne contient pas 0, on obtient que a est nul. □

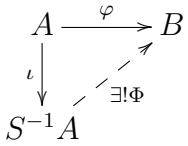
Exemples 7.8. *1. Si $A = \mathbb{Z}$ et $S = A^*$, on obtient $S^{-1}A = \mathbb{Q}$.*

2. *Si la partie multiplicative de A choisie est l'ensemble $S = A^\times$ des inversibles de A, l'application*
$$\iota : A \longrightarrow S^{-1}A$$
est un isomorphisme d'anneaux.

3. *un exemple $\mathbb{Z}$ localisé en un nombre premier.*

4. *Si k est un corps, alors $A = k[X]$ est intègre et en posant $S = k[X]^*$, on obtient pour $S^{-1}A$ le corps $k(X)$ des fractions rationnelles.*

Théorème 7.9 (Propriété universelle de la localisation)**.** *Soit $\varphi : A \longrightarrow B$ un morphisme d'anneaux et $S \subset A$ une partice multiplicative. Si $\varphi(s)$ est inversible pour tout $s \in S$, alors il existe un unique morphisme d'anneaux $\Phi : S^{-1}A \longrightarrow B$ tel que $\Phi \circ \iota = \varphi$, c'est à dire qui complète le diagramme*



Démonstration. (Unicité) Si un tel Φ existe alors pour $a \in A$, on a $\varphi(a) = \Phi([a,1])$. En particulier pour tout $(a,s) \in A \times S$ on a

$$\varphi(a) = \Phi([a,1]) = \Phi([s,1])\Phi([a,s]) = \varphi(s)\Phi([a,s])$$

et $\varphi(s)$ étant inversible l'élément $\Phi([a,s]) = \varphi(a)\varphi(s)^{-1}$ est uniquement déterminé.

(Existence) On montre que la formule

$$\Phi([a,s]) = \varphi(a)\varphi(s)^{-1}$$

définit bien un morpshime d'anneaux $\Phi : S^{-1}A \longrightarrow B$. Supposons que $[a,s] = [b,t]$, c'est à dire qu'il existe $x \in S$ tel que $x(at - bs) = 0$. On a alors

$$\varphi(x)\varphi(a)\varphi(t) = \varphi(x)\varphi(b)\varphi(s),$$

donc $\varphi(a)\varphi(s)^{-1} = \varphi(b)\varphi(t)^{-1}$. Le fait qu'on définisse ainsi un morphisme d'anneaux découle directement des propriétés de φ. □

La dénomination «propriété universelle» provient du fait que cette propriété caractérise l'anneau $S^{-1}A$ comme solution d'un problème universel.

Corollaire 7.10. *Soit $S \subset A$ une partie multiplicative d'un anneau A et un morphisme d'anneaux $\tilde{\iota} : A \longrightarrow \tilde{A}$ tel que pour tout $s \in S$, $\tilde{\iota}(s)$ est inversible, et vérifiant la propriété universelle précédente. Alors il existe une unique morphisme d'anneaux*

$$\Phi : S^{-1}A \longrightarrow \tilde{A}$$

tel que $\Phi \circ \iota = \iota'$, et Φ est un isomorphisme.

Démonstration. Par le théorème 7.9 pour $\varphi = \tilde{\iota}$ et $B = \tilde{A}$, on obtient un unique morphisme $\Phi : S^{-1}A \longrightarrow \tilde{A}$ tel que $\tilde{\iota} = \Phi \circ \iota$ (propriété universelle de $S^{-1}A$).

De même par hypothèse, $\tilde{A}$ vérifiant la propriété universelle, il existe un morphisme $\Psi : \tilde{A} \longrightarrow S^{-1}(A)$ tel que $\iota = \Psi \circ \tilde{\iota}$. Le diagramme (trivial)

$$\begin{array}{ccc} A & \xrightarrow{\iota} & S^{-1}A \\ {\scriptstyle \iota}\downarrow & & \\ S^{-1}A & & \end{array}$$

est évidemment complété par l'application identité $S^{-1}A \longrightarrow S^{-1}A$, mais aussi par $\Psi \circ \Phi$, puisque

$$\Psi \circ \Phi \circ \iota = \Psi \circ \tilde{\iota} = \iota.$$

L'unicité pour la propriété universelle de $S^{-1}A$ indique donc que $\Psi \circ \Phi = \mathrm{id}_{S^{-1}A}$.

Le même raisonnement en remplaçant $S^{-1}A$ par $\tilde{A}$, ι par $\tilde{\iota}$ et en invoquant la propriété universelle de $\tilde{A}$ montre que $\Phi \circ \Psi = \mathrm{id}_{\tilde{A}}$. □

L'unicité dans la propriété universelle du théorème 7.9 entre de manière décisive dans la dernière preuve. Sans imposer cette unicité, le localisé $S^{-1}A$ n'est plus caractérisé par cette propriété.

7.2 Idéaux et idéaux premiers des localisés

Soit A un anneau et $S \subset A$ une partie multiplicative. Si I est un idéal de A, on note

$$S^{-1}I = \{[a,s] \in S^{-1}A,\ a \in I\}.$$

Il s'agit bien sûr d'un idéal de $S^{-1}A$. Le théorème suivant indique que tous les idéaux de $S^{-1}A$ sont de cette, et même plus s'ils sont premiers.

Proposition 7.11. *Soit A un anneau et $S \subset A$ une partie multiplicative. On note $\iota : A \longrightarrow S^{-1}A$ le morphisme naturel précédent.*

1. *Tout idéal I de $S^{-1}A$ est égal à $S^{-1}J$, où $J = \iota^{-1}(I)$.*
2. *L'ensemble des idéaux premiers de $S^{-1}A$ est en correspondance bijective avec les idéaux premiers de A qui ne rencontrent pas S, via*

$$\begin{array}{ccc} \mathrm{Spec}(S^{-1}A) & \longleftrightarrow & \left\{ \begin{array}{c} \textit{idéaux premiers de } A \\ \textit{rencontrant pas } S \end{array} \right\} \\ I & \longmapsto & \iota^{-1}(I) \\ S^{-1}J & \longleftarrow\!\shortmid & J \end{array}$$

Démonstration. 1. Étant l'image réciproque de I par le morphisme ι, J est un idéal. Si $[a,s]$ est un élément de I, alors

$$[a,1] = [s,1] \cdot [a,s]$$

en est un aussi, donc $a \in J$ et $I \subset S^{-1}J$.

Réciproquement par définition de J on a $\iota(j) = [j,1] \in I$ pour tout $j \in J$, donc pour tout $(j,s) \in J \times S$ on a $[j,s] = [j,1] \cdot [1,s]$ dans I, c'est à dire $S^{-1}J = I$.

2. Soit $I \in \mathrm{Spec}(S^{-1}A)$ un idéal premier. D'une part l'image réciproque $\iota^{-1}(I)$ est un idéal premier de A. De plus si $s \in \iota^{-1}(I) \cap S$, alors

$$[1,s] \cdot \iota(s) = [1,1]$$

est un élément de I et $I = S^{-1}A$, ce qui contredit le fait qu'il est premier. L'idéal $\iota^{-1}(I)$ ne rencontre donc pas S.

Réciproquement, soit $J \in A$ un idéal premier d'intersection vide avec S. Montrons que l'idéal $S^{-1}J$ est premier : si le produit de deux éléments

$$[a, s] \cdot [b, t] = [ab, st]$$

appartient à $S^{-1}J$, alors $[ab, 1] = [st, 1] \cdot [ab, st]$ de même. On a donc deux éléments $j \in J$ et $u \in S$ tels que

$$[ab, 1] = [j, u],$$

c'est à dire un $x \in S$ tel que $x(abu - j) = 0$. L'élément $(ab)(ux)$ appartient donc à J mais ce dernier est premier et ne rencontre pas S, donc $ux \notin J$ et finalement $ab \in J$. Invoquant à nouveau le fait que J est premier, on a soit $a \in J$, soit $b \in J$, c'est à dire $[a, s] \in S^{-1}J$ ou $[b, t] \in S^{-1}J$. L'idéal $S^{-1}J \subset S^{-1}A$ est premier et la seconde application est bien définie.

Le même raisonnement que celui appliqué à ab précédemment montre que si $J \in \mathrm{Spec}(A)$ ne rencontre pas S et $[\alpha, 1] \in S^{-1}J$, alors $\alpha \in J$. Les ensemble $\mathrm{Spec}(S^{-1}A)$ et des idéaux de $\mathrm{Spec}(A)$ ne rencontrant pas S sont donc bien en bijection.

□

Corollaire 7.12. *Si A est un anneau noethérien et $S \subset A$ est une partie multiplicative, $S^{-1}A$ est lui aussi noethérien.*

Démonstration. Soit

$$\mathcal{C} = I_1 \subset I_2 \subset ...$$

une suite croissante d'idéaux de $S^{-1}A$. Le théorème 7.11 indique que $I_k = S^{-1}J_k$, où $J_k = \{a \in A, \iota(a) \in I_k\}$. Ces idéaux de A sont eux aussi emboités : $\mathcal{C}$ donne ainsi lieu à une chaine d'idéaux $J_1 \subset J_2 \subset ...$ de A, stationnaire car ce dernier est noethérien. Il en va ainsi de même pour $\mathcal{C}$. □

Corollaire 7.13. *Soit A un anneau et $S \subset A$ une partie multiplicative. Le sous-ensemble $U_S \subset \mathrm{Spec}(A)$ des idéaux premiers de A ne rencontrant pas S est spectral pour la topologie induite par celle de Zariski.*

Démonstration. On montre que U_S est homéomorphe à $\mathrm{Spec}(S^{-1}A)$, muni de la topologie de Zariski. La proposition 7.11 indique que U_S et $\mathrm{Spec}(S^{-1}A)$ sont en correspondance bijective, via $I \mapsto \iota^{-1}(I)$. Cette application est continue car elle préserve les inclusions et l'image réciproque de $V(\mathfrak{p}) \cap U_S \subset U_S$ sur l'ensemble des idéaux premiers de $S^{-1}A$ qui contiennent $S^{-1}\mathfrak{p}$, c'est à dire $V(S^{-1}\mathfrak{p})$.

De même pour l'application réciproque $J \longrightarrow S^{-1}J$: l'image inverse du fermé $V(\mathfrak{p}')$ de $\mathrm{Spec}(S^{-1}A)$ est $V(\iota^{-1}(\mathfrak{p}')) \cap U_S$, un fermé de U_S. La bijection du théorème est donc un homéomorphisme. □

Corollaire 7.14. *Tout ouvert standard $D(a) \subset \mathrm{Spec}(A)$ (avec a non-nilpotent) est un espace topologique spectral, pour la topologie induite par celle de Zariski.*

Démonstration. Le sous-ensemble $S_a = \{1, a, a^2, ...\}$ est une partie multiplicative de A. L'ouvert standard $D(a)$ correspond aux idéaux premiers de $\mathrm{Spec}(A)$ qui ne contiennent pas a, c'est à dire à l'ensemble U_{S_a} des idéaux premiers qui ne rencontrent pas S_a. En effet si $\mathfrak{p} \in U_{S_a}$, alors a n'appartient pas à $\mathfrak{p}$ et réciproquement si $\mathfrak{p} \in D(a)$, $a \notin \mathfrak{p}$ et il en va de même pour toute puissance de a. L'idéal $\mathfrak{p}$ ne contenant pas 1 non plus, $\mathfrak{p} \in U_{S_a}$. En vertu du corollaire 7.13, $D(a)$ est homéomorphe à $\mathrm{Spec}(S_a^{-1}A)$. □

7.3 Deux exemples fondamentaux

Corps des fractions

Vous avez vu en première partie du cours (et en L3) la construction très classique du *corps des fractions* d'un anneau intègre. Celle-ci correspond à un cas particulier de localisation : en effet si A est intègre, $S = A \setminus \{0\}$ est une partie multiplicative. Le localisé $S^{-1}A$ est naturellement un corps qui contient A : l'application ι est injective et on a toujours $[a, s]^{-1} = [s, a]$. On note $\mathrm{Frac}(A) := S^{-1}A$ ce corps qu'on appelle le *corps des fractions de A*.

Théorème 7.15. *Si A est un intègre, tout morphisme d'anneaux $\varphi : A \longrightarrow B$ tel que $\varphi(a)$ est inversible pour tout $a \in A$ non-nul se prolonge en un unique morphisme injectif $\Phi : \mathrm{Frac}(A) \longrightarrow B$.*

Démonstration. D'après la propriété universelle de la localisation, les hypothèses impliquement que φ se prolonge de manière unique en un morphisme

$$\Phi : \mathrm{Frac}(A) \longrightarrow B$$

donné par $\Phi([a, s]) = \varphi(a)\varphi(s)^{-1}$, pour tout s est non-nul. Ce morphisme est clairement injectif, car l'idéal $\ker(\Phi)$ est réduit à 0. □

Corollaire 7.16. *Si A est un anneau intègre et K est un corps contenant A, alors K contient un sous-corps isomorphe à $\mathrm{Frac}(A)$.*

Localisation en un idéal premier

Définition 7.17. *Un anneau A est dit local s'il possède un unique idéal maximal $\mathfrak{m}$. Le quotient $A/\mathfrak{m}$ est appelé le corps résiduel de A.*

La caractérisation suivante est commode et permet même de généraliser sans peine les anneaux locaux au cadre non-commutatif.

Lemme 7.18. *Un anneau A est local si et seulement si l'ensemble des éléments non-inversibles de A est un idéal.*

Démonstration. Si l'ensemble des éléments non-inversibles de A est un idéal, il est nécessairement l'unique idéal maximal de A. Réciproquement si A possède un unique idéal maximal $\mathfrak{m}$, celui-ci correspond aux éléments non-inversibles car si $a \in A$ n'est pas inversible, on a $< a > \subset \mathfrak{m}$ par le théorème de Krull. □

Si A est un anneau et $\mathfrak{p} \in \mathrm{Spec}(A)$ est un idéal premier, le sous-ensemble $S_\mathfrak{p} = A \setminus \mathfrak{p}$ est une partie multiplicative de A. Le localisé $S_\mathfrak{p} A$ est noté $A_\mathfrak{p}$ et est appelé le localisé de A en $\mathfrak{p}$.

Proposition 7.19. *Si A est un anneau et $\mathfrak{p}$ un idéal premier de A, l'anneau $A_\mathfrak{p}$ est un anneau local.*

Démonstration. En vertu du théorème 7.11 les idéaux premiers de $A_\mathfrak{p}$ sont les $S_\mathfrak{p}^{-1}\mathfrak{q}$, où $\mathfrak{q}$ est un idéal premier de A qui ne rencontre pas $A \setminus \mathfrak{p}$, c'est à dire contenu dans $\mathfrak{p}$. Tous les idéaux premiers de $A_\mathfrak{p}$ sont donc contenus dans $S_\mathfrak{p}^{-1}\mathfrak{p}$, qui en est l'unique idéal maximal. □

À tout anneau A et à tout idéal premier $\mathfrak{p} \in \mathrm{Spec}(A)$ on peut donc associer l'anneau local $A_\mathfrak{p}$. Cet anneau et son corps résiduel $\kappa(\mathfrak{p})$, le *corps résiduel de A en $\mathfrak{p}$*, seront essentiels si vous poursuivez l'année prochaine l'étude de la géométrie algébrique.

8 Produit tensoriel

Comme vu précédemment, le spectre du produit direct $A \times B$ de deux anneaux n'est pas un objet très intéressant, il est simplement donné par l'union disjointe de $\mathrm{Spec}(A)$ et $\mathrm{Spec}(B)$, et la topologie de Zariski s'avère être la topologie disjointe.

Étant donnés deux A-modules M et N, nous introduisons désormais un autre «produit» : leur produit tensoriel $M \otimes_A N$. Le produit tensoriel de M et N a pour vocation de proposer un module engendré par des produits formels des éléments de M et N, les tenseurs purs, que l'on note $m \otimes n$. On obtient ainsi un objet très versatile et utile, qui associé aux deux problèmes classiques suivants :

1. (extension des scalaires) Soit V un $\mathbb{R}$-espace vectoriel de base $(e_i)_{i\in\mathcal{I}}$. Comment construire le *complexifié* de V, c'est à dire le «$\mathbb{C}$-espace vectoriel engendré par la famille $(e_i)_{i\in\mathcal{I}}$» ? Cette situation peut s'étudier à la main en base, mais est résolue de manière plus conceptuelle par le produit tensoriel $V \otimes_\mathbb{R} \mathbb{C}$, qui s'applique dans un cadre beaucoup plus général que $\mathbb{R}$ et $\mathbb{C}$.

2. (produit de variétés) On aimerait construire une notion de «produit» pour les variétés algébriques, qui corresponde au produit des ensembles algébriques. Le problème se pose déjà pour le cas le plus simple : le produit tensoriel $\mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y]$ doit correspondre à l'anneaux de polynômes $\mathbb{C}[X, Y]$. Tout élément de $\mathbb{C}[X, Y]$ n'est pas le produit de deux polynômes de $\mathbb{C}[X]$ et $\mathbb{C}[Y]$, mais ce dernier a tout de même une base formée par les monômes $(X^i Y^j)_{(i,j)\in\mathbb{N}^2}$, qui correspondront aux tenseurs purs $(X^i \otimes Y^j)_{(i,j)\in\mathbb{N}^2}$.

8.1 Définition et propriété universelle

Soit A un anneau et M, N, P des A-modules.

Définition 8.1. *Une application $\varphi : M \times N \longrightarrow P$ est A-bilinéaire, si pour tous éléments a, a' de A, m, m' de M et n, n' de N on a*

$$\varphi(am + a'm', n) = a\varphi(m, n) + a'\varphi(m', n)$$
$$\varphi(m, an + a'n') = a\varphi(m, n) + a'\varphi(m, n').$$

Si P est un A-module et X est un ensemble, l'ensemble $\mathrm{Hom}_{\mathrm{Set}}(X, P)$ des applications ensemblistes de X vers P est naturellement muni d'une structure de A-module, via les lois

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x) \text{ et } (a \cdot \varphi)(x) = a\varphi(x).$$

Il en va de même pour les morphismes de A-modules, qu'on note Hom_A.

Lemme 8.2. *L'ensemble $\mathrm{Bil}_A(M \times N, P)$ des applications $M \times N \longrightarrow P$ qui sont A-bilinéaires est un sous-A-module de $\mathrm{Hom}_{\mathrm{Set}}(M, N)$.*

Démonstration. Si $b \in A$ et $\varphi : M \times N \longrightarrow P$, $\psi : M \times N \longrightarrow P$ sont deux applications A-bilinéaires, on montre que $b\varphi + \psi$ est A-bilinéaire.

En effet si $(a, a') \in A^2$, $(m, m') \in M^2$ et $(n, n') \in N^2$, on a immédiatement

$$(b\varphi + \psi)(am + a'm', n) = a(b\varphi + \psi)(m, n) + a'(b\varphi + \psi)(m', n)$$
$$(b\varphi + \psi)(m, an + a'n') = a(b\varphi + \psi)(m, n) + a'(b\varphi + \psi)(m, n').$$

□

Nous allons maintenant construire le module qui vérifie les propriétés escomptées plus haut, et montrer qu'il est solution d'un problème universel. Notons $A^{(M\times N)}$ le A-module libre associé à l'ensemble $M \times N$. Les éléments de $A^{(M\times N)}$ sont les combinaisons linéaires

$$\sum_{(m,n)\in M\times N} a_{m,n}\delta_{m,n},$$

c'est à dire les combinaisons linéaires en les éléments $(\delta_{m,n})_{(m,n)\in M\times N}$, à coefficients $(a_{m,n})_{(m,n)\in M\times N}$ dans A (il s'agit donc de sommes finies).

Le module libre $A^{(M\times N)}$ décrit ponctuellement les morphismes de A-modules $M\times N \longrightarrow A$. Pour forcer la bilinéarité, on considère l'idéal $I \subset A^{(M\times N)}$ engendré par les éléments de la forme

$$\delta_{am+m',n} - a\delta_{m,n} - \delta_{m',n} \tag{8.1}$$
$$\delta_{m,an+n'} - a\delta_{m,n} - \delta_{m,n'} \tag{8.2}$$

avec a appartenant à A, m, m' à M et n, n' à N.

Définition 8.3. *On note $M\otimes_A N = A^{(M\times N)}/I$ le A-module quotient associé, et $m\otimes n$ la classe de $\delta_{m,n}$ dans $M\otimes_A N$.*

Par définition de $M\otimes_A N$, on a les relations

$$(am)\otimes n = a(m\otimes n) = m\otimes(an) \tag{8.3}$$

et tout élément de $M\otimes_A N$ est une somme finie d'éléments de la forme $m\otimes n$.

Remarque 8.4. *Les éléments de $M\otimes_A N$ de la forme $m\otimes n$ sont les tenseurs purs de $M\otimes_A N$. Ils engendrent $M\otimes_A N$, mais les éléments de $M\otimes_A N$ ne sont pas tous des tenseurs purs.*

Proposition 8.5. *Si deux A-modules M et N sont respectivement engendrés par $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$, alors leur produit tensoriel $M\otimes_A N$ est engendré par les tenseurs purs $(e_i\otimes f_j)_{(i,j)\in I\times J}$.*

Démonstration. Si $m\otimes n \in M\otimes_A N$ est un tenseur pur, alors en décomposant $m = \sum_{k=1}^{s} m_{i_k} e_{i_k}$ et $n = \sum_{l=1}^{t} n_{j_l} f_{j_l}$, on obtient

$$m\otimes n = \sum_{k=1}^{s}\sum_{l=1}^{t} m_{i_k} n_{j_l} (e_{i_k}\otimes f_{j_l})$$

Tout élément de $M\otimes_A N$ est une somme finie de tenseurs purs, et ainsi la famille $(e_i\otimes f_j)_{(i,j)\in I\times J}$ engendre $M\otimes_A N$. □

Remarque 8.6. *En particulier, si M et N sont des A-modules de type fini, il en va de même pour leur produit tensoriel.*

Théorème 8.7 (Propriété universelle du produit tensoriel)**.** *Soit A une anneau et M, N des A-modules. Pour tout A-module P on a une bijection*

$$\begin{array}{ccc} \mathrm{Hom}_A(M\otimes_A N, P) & \overset{\sim}{\longleftrightarrow} & \mathrm{Bil}_A(M\times N, P) \\ \varphi & \longmapsto & \Psi(\varphi) : (m,n)\mapsto \varphi(m\otimes n) \\ \Phi(\psi) & \longleftarrow\!\shortmid & \psi \end{array}$$

où $\Phi(\psi) : M \otimes_A N \longrightarrow P$ *est le morphisme de* A*-modules donné sur les tenseurs purs par* $\Phi(\psi)(m \otimes n) = \psi(m, n)$.

Démonstration. La première application est bien définie : étant donnée une application $\varphi \in \mathrm{Hom}_A(M \otimes_A N, P)$, les relations (8.3) assurent que $\Psi(\varphi)$ est A-bilinéaire.

Montrons que l'application Φ est bien définie. Si $\psi \in \mathrm{Bil}_A(M \times N, P)$, on considère le morphisme de A-modules $\tilde{\psi} : A^{(M\times N)} \longrightarrow P$ défini par les images $\tilde{\psi}(\delta_{m,n}) = \psi(m, n)$. L'application $\tilde{\psi}$ étant bilinéaire, $\tilde{\psi}$ s'annule sur les générateurs de $I \subset A(M \times N)$ (8.1) :

$$\tilde{\psi}(\delta_{am+m',n} - a\delta_{m,n} - \delta_{m',n}) = \psi(am + m', n) - a\psi(m, n) - \psi(m', n) = 0.$$
$$\tilde{\psi}(\delta_{m,an+n'} - a\delta_{m,n} - \delta_{m,n'}) = \psi(m, an + n') - a\psi(m, n) - \psi(m, n') = 0.$$

L'application $\tilde{\psi}$ passe donc au quotient et il existe un morphisme

$$\Phi(\psi) : M \otimes_A N \longrightarrow P$$

donné sur les tenseurs purs par $\Phi(\psi)(m \otimes n) = \tilde{\psi}(\delta_{m,n}) = \psi(m, n)$.

Soient donc $\varphi \in \mathrm{Hom}_A(M \otimes_A N, P)$ et $\psi \in \mathrm{Bil}_A(M \times N, P)$.
Pour tout $(m, n) \in M \times N$ on a

$$\Phi \circ \Psi(\varphi)(m \otimes n) = \Psi(\varphi)(m, n) = \varphi(m \otimes n)$$

et de même

$$\Psi \circ \Phi(\psi)(m, n) = \Phi(\psi)(m \otimes n) = \psi(m, n)$$

et Φ, Ψ sont des bijections réciproques. □

8.2 Propriétés du produit tensoriel

La propriété universelle du produit tensoriel est l'outil usuel pour étudier les morphismes $M \otimes_A N \longrightarrow P$ à partir des applications A-bilinéaires $M \times N \longrightarrow P$. Elle est ainsi d'un usage permanent, notamment lorsqu'il s'agit d'identifier le produit tensoriel de deux modules.

Proposition 8.8 (Associativité et commutativité)**.** *Soit* A *un anneau et* M, N, P *des* A*-modules. On a des isomorphismes de* A*-modules*

$$M \otimes_A N \simeq N \otimes_A M \tag{8.4}$$
$$(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P) \tag{8.5}$$

Démonstration. (8.4) L'application A-bilinéaire

$$\begin{array}{ccc} M \times N & \longrightarrow & N \otimes_A M \\ (m,n) & \longmapsto & n \otimes m \end{array}$$

induit par la propriété universelle du produit tensoriel un morphisme de A-modules $\varphi_1 : M \otimes_A N \longrightarrow N \otimes_A M$ donné sur les tenseurs purs par $\varphi(m \otimes n) = n \otimes m$. Le même raisonnement en remplaçant les rôles de M et N donne lieu à un morphisme $\varphi_2 : N \otimes_A M \longrightarrow M \otimes_A N$ donné par $n \otimes m \mapsto m \otimes n$, et qui est l'inverse de φ_1.

(8.5) En fixant un élément p de P, l'application

$$\begin{array}{ccc} M \times N & \longrightarrow & M \otimes_A (N \otimes_A P) \\ (m,n) & \longmapsto & m \otimes (n \otimes p) \end{array}$$

est A-bilinéaire, et induit donc $\varphi_p : M \otimes_A N \longrightarrow M \otimes_A (N \otimes_A P)$ donnée par $\varphi_p(m \otimes n) = m \otimes (n \otimes p)$.

On obtient en particulier une application A-bilinéaire

$$\varphi : (M \otimes_A N) \times P \longrightarrow M \otimes_A (N \otimes_A P)$$

en posant $(m \otimes n, p) \mapsto \varphi_p(m \otimes n) = m \otimes (n \otimes p)$, qui donne elle-même lieu par propriété universelle au morphisme de A-modules

$$f : (M \otimes_A N) \otimes_A P \longrightarrow M \otimes_A (N \otimes_A P)$$

donné par $f((m \otimes n) \otimes p) = m \otimes (n \otimes p)$. L'inverse de f est construit de la même manière, en construisant par propriété universelle le morphisme

$$g : M \otimes_A (N \otimes_A P) \longrightarrow (M \otimes_A N) \otimes_A P$$

donné apr $g(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$. □

Proposition 8.9. *Si M est un A-module, on a $M \simeq A \otimes_A M$.*

Démonstration. On considère le morphisme de A-modules $f : A \otimes_A M \longrightarrow M$ donnée par $f(a \otimes m) = am$, induite par propriété universelle par l'application A-bilinéaire

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a,m) & \longmapsto & am \end{array}.$$

L'application $g : M \longrightarrow A \otimes_A M$ donnée par $g(m) = 1 \otimes m$ est elle aussi un morphisme de A-module et l'inverse de f, puisque $f(g(m)) = f(1 \otimes m) = m$ et $g(f(a \otimes m)) = g(am) = 1 \otimes am = a \otimes m$. □

Remarque 8.10. *en remplaçant fonction bilinéaires par multilinéaires, il est possible d'adapter la construction du produit tensoriel pour construire directement le produit tensoriel $M_1 \otimes_A ... \otimes_A M_n$ d'une famille $M_1 ... M_k$ de A-modules.*

Théorème 8.11. *Si M, N sont deux A-modules libres de bases respectives $(e_i)_{i\in\mathcal{I}}$ et $(f_j)_{j\in\mathcal{J}}$, leur produit tensoriel $M \otimes_A N$ est libre de base $(e_i \otimes f_j)_{(i,j)\in\mathcal{I}\times\mathcal{J}}$*

Démonstration. Cela découle de la propriété universelle des modules libres. Soit

$$C = A^{(\mathcal{I}\times\mathcal{J})} =< (\delta_{i,j})_{(i,j)\in\mathcal{I}\times\mathcal{J}} >$$

le A-module libre de base $\mathcal{I} \times \mathcal{J}$. On considère d'une part l'application A-linéaire

$$\varphi : C \longrightarrow M \otimes_A N$$

définie par $\varphi(\delta_{i,j}) = e_i \otimes f_j$.

Réciproquement, l'application

$$\begin{array}{rccc} \tilde{\psi} : & M \times N & \longrightarrow & C \\ & \left(\sum_{i\in\mathcal{I}} a_i e_i, \sum_{j\in\mathcal{J}} b_j f_j\right) & \longmapsto & \sum_{(i,j)\in\mathcal{I}\times\mathcal{J}} a_i b_j \delta_{i,j} \end{array}$$

est A-bilinéaire (elle est définie par $\tilde{\psi}(e_i, f_j) = \delta_{i,j}$). Elle induit donc par propriété universelle du produit tensoriel le morphisme de A-modules $\psi : M \otimes_A N \longrightarrow C$ donné sur les tenseurs purs par $\psi(e_i \otimes e_j) = \delta_{i,j}$.

Les applications φ et ψ sont des bijections réciproques. □

Corollaire 8.12. *Si M et N sont des A-modules libres de rangs finis respectifs m et n, leur produit tensoriel $M \otimes_A N$ est libre de rang mn.*

8.3 Produit tensoriel d'algèbres

Définition 8.13. *Soit A un anneau et B un ensemble. On dit que B est une A-algèbres s'il est muni de lois de compositions $(E, +, \cdot, \times)$*
($+$ et $\times$ internes, $\cdot$ externe par A) telles que

1. *$(B, +, \cdot)$ est un A-module ;*
2. *$(B, \times)$ est un anneau ;*
3. *la multiplication $\times : B \times B \longrightarrow B$ est A-bilinéaire.*

Un morphisme de A-algèbres $B \longrightarrow C$ est un morphisme à la fois de A-modules et d'anneaux pour les structures respectives de B et C. Un $\mathbb{Z}$-module étant simplement un groupe abélien, une $\mathbb{Z}$-algèbre est un anneau. On dit qu'une A-algèbre B est commutative si $(B, \times)$ l'est. Dans la suite, sauf mention du contraire, on ne considère que des A-algèbres commutatives.

Proposition 8.14. *Soit A un anneau et B, C deux A-algèbres. La formule sur les tenseurs purs*

$$(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'.$$

munit le produit tensoriel $B \otimes_A C$ d'une unique structure de A-algèbre.

Démonstration. Par propriété universelle, l'application A-multilinéaire

$$\begin{array}{rccc} \tilde{\varphi} : & B \times C \times B \times C & \longrightarrow & B \times_A C \\ & (b, c, b', c') & \longmapsto & bb' \otimes cc' \end{array}$$

induit l'application $\varphi : B \otimes_A C \otimes_A B \otimes_A C \longrightarrow B \otimes_A C$ donnée sur les tenseurs purs par $\varphi(b \otimes c \otimes b' \otimes c') = bb' \otimes cc'$.

Puisque par associativité du produit tensoriel on a aussi

$$B \otimes_A C \otimes_A B \otimes_A C \simeq (B \otimes_A C) \otimes_A (B \otimes_A C),$$

l'application φ correspond aussi l'application A-bilinéaire

$$\psi : (B \otimes_A C) \times (B \otimes_A C) \longrightarrow B \otimes_A C$$

donnée sur les tenseurs purs par $\psi((b \otimes c) \otimes (b' \otimes c')) = bb' \otimes cc'$, qui munit donc bien $B \otimes_A C$ d'une unique structure de A-algèbre. □

8.4 Applications

Extensions des scalaires

Soit V un $\mathbb{R}$-espace vectoriel de dimension finie et $(e_i)_{i=1}^n$ une base de V. Le produit tensoriel $\mathbb{C} \otimes_{\mathbb{R}} V$ est un $\mathbb{R}$-espace vectoriel de dimension $2n$, et la famille de tenseurs purs $1 \otimes e_1$, ..., $1 \otimes e_n$, $i \otimes e_1$,..., $i \otimes e_n$ en est une base. Celui-ci peut être muni d'une structure d'espace vectoriel sur $\mathbb{C}$, en posant pour les tenseurs purs

$$z \cdot (z' \otimes v) = zz' \otimes v.$$

On peut vérifier que le $\mathbb{C}$-espace vectorial ainsi obtenu correspond à ceux envisagés en début de section. Un grand avantage de ce procédé est qu'il est *canonique* (il ne dépend pas du choix d'une base de $\mathbb{C}$ comme $\mathbb{R}$-espace vectoriel) et qu'il se généralise très bien comme suit.

Proposition 8.15. *Soient B une A-algèbre et C un A-module. Alors le A-module $B \otimes_A C$ admet une structure de B-module, uniquement déterminée sur les tenseurs purs par*

$$b \cdot (b' \otimes c) = bb' \otimes c$$

Démonstration. L'application

$$\begin{array}{rccc} \tilde{\varphi}: & B \times B \times C & \longrightarrow & B \otimes_A C \\ & (b, b', c) & \longmapsto & bb' \otimes c \end{array}$$

est multilinéaire et induit donc par propriété universelle l'application A-linéaire

$$\begin{array}{rccc} \varphi: & B \otimes_A B \otimes_A C & \longrightarrow & B \otimes_A C \\ & b \otimes b' \otimes c & \longmapsto & bb' \otimes c \end{array}.$$

À nouveau, on obtient une flèche A-bilinéaire $\psi : B \times (B \otimes_A C) \longrightarrow B \otimes A$, donnée par $(b, b' \otimes c) \mapsto bb' \otimes c$ sur les tenseurs purs. On en déduit facilement en écrivant tout élément $x \in B \otimes_A C$ comme une somme de tenseurs purs que $1 \cdot x = \psi(1, x) = x$, et que $b \cdot (b' \cdot x) = bb' \cdot x$. □

Produit de variétés affines

On réalise dans cette section le programme élaboré au début de cette partie : construire des produits d'ensembles algébriques grâce au produit tensoriel.

Proposition 8.16. *Il existe un isomorphisme d'algèbres* $\mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y] \simeq \mathbb{C}[X, Y]$.

Démonstration. L'application $\mathbb{C}$-bilinéaire

$$\begin{array}{rccc} \tilde{\varphi}: & \mathbb{C}[X] \times \mathbb{C}[Y] & \longrightarrow & \mathbb{C}[X, Y] \\ & (P(X), Q(Y)) & \longmapsto & P(X)Q(Y) \end{array}$$

induit le morphisme de $\mathbb{C}$-espace vectoriels $\varphi : \mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y] \longrightarrow \mathbb{C}[X, Y]$ donné par les images $\varphi(P(X) \otimes Q(Y)) = P(X)Q(Y)$.

En vertu du théorème 8.11, le $\mathbb{C}$-espace vectoriel $\mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y]$ a pour base les tenseurs purs $(X^n \otimes Y^m)_{(n,m)\in\mathbb{N}^2}$. Ceux-ci s'envoient via φ sur les monômes $(X^n Y^m)_{(n,m)\in\mathbb{N}^2}$, une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}[X, Y]$; φ est donc un isomorphisme de $\mathbb{C}$-espaces vectoriels. Pour montrer que φ est un morphisme d'algèbres, il suffit de montrer la multiplicativité sur les tenseurs purs, ce qui est clair. □

Remarque 8.17. *Le résultat précédent vaut toujours (avec la même preuve) si* $\mathbb{C}$ *est remplacé par n'importe quel anneau* A*. Il s'étendent aussi bien sûr par associativité ou par multilinéarité à un nombre quelconque de variables.*

Soient $V = Z(P_1, ..., P_k) \subset \mathbb{C}[X_1, ..., X_n]$ et $W = Z(Q_1, ..., Q_s) \subset \mathbb{C}[Y_1, ..., Y_m]$ deux sous ensembles algébriques et

$$\begin{cases} \mathcal{I} =< P_1, ..., P_k > \\ \mathcal{J} =< Q_1, ..., Q_s > \end{cases}$$

les idéaux associés. Le sous-ensemble $V \times W \subset \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]$ est lui aussi algébrique, d'idéal associé $\mathcal{K} =< P_1, ..., P_k, Q_1, ..., Q_s >$.

Proposition 8.18. *On a un isomorphisme d'algèbres*

$$\mathbb{C}[X_1, ..., X_n]/\mathcal{I} \otimes_{\mathbb{C}} \mathbb{C}[Y_1, .., Y_m]/\mathcal{J} \simeq \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K}.$$

Démonstration. Comme $\mathcal{K}$ contient les images de $\mathcal{I}$ et $\mathcal{J}$ dans $\mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]$, l'application $\mathbb{C}$-bilinéaire

$$\begin{array}{rccc} \tilde{\varphi}: & \mathbb{C}[X_1, ..., X_n]/\mathcal{I} \times \mathbb{C}[Y_1, .., Y_m]/\mathcal{J} & \longrightarrow & \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K} \\ & (f \bmod \mathcal{I}, g \bmod \mathcal{J}) & \longmapsto & fg \bmod \mathcal{K} \end{array}$$

est bien définie et induit le morphisme

$$\varphi : \mathbb{C}[X_1, ..., X_n]/\mathcal{I} \otimes_{\mathbb{C}} \mathbb{C}[Y_1, .., Y_m]/\mathcal{J} \simeq \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K}$$

donné par $\varphi(f \otimes g) = fg$, qui est le morphisme d'algèbres de la proposition 8.16 (pour alléger les notations, on n'écrira plus les idéaux).

Le morphisme φ est surjectif, car $\varphi(X^\alpha \otimes Y^\beta) = X^\alpha Y^\beta$ et $\mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K}$ est engendré par ces monômes.

Reste à montrer que φ est injectif. D'une part en fixant des bases $(e_x)_{x\in\mathfrak{X}}$ et $(f_y)_{y\in\mathfrak{Y}}$ aux $\mathbb{C}$-espaces vectoriels $\mathbb{C}[X_1, ..., X_n]/\mathcal{I}$ et $\mathbb{C}[Y_1, .., Y_m]/\mathcal{J}$, on peut écrire tout élément de $\mathbb{C}[X_1, ..., X_n]/\mathcal{I} \otimes_{\mathbb{C}} \mathbb{C}[Y_1, .., Y_m]/\mathcal{J}$ comme une combinaison linéaire de tenseurs purs de la forme $e_i \otimes \cdot$ (en déplaçant les scalaires à droite). Prenons donc un élément $h \in \ker(\varphi)$ et écrivons le

$$h = \sum_{x\in\mathfrak{X}} e_x \otimes h_x.$$

Le fait que h appartienne au noyau de φ implique que pour tout couple $i_0 \in Z(\mathcal{I})$, $j_0 \in Z(\mathcal{J})$, on a $(i_0, j_0) \in Z(h) \subset \mathbb{C}^{n+m}$, c'est à dire

$$0 = h(i_0, j_0) = \sum_{x\in X} e_x(i_0)h_x(j_0).$$

On regarde tout d'abord ces inégalités à j_0 fixé. Les $(e_x)_{x\in\mathfrak{X}}$ formant une base et i_0 étant quelconque, on obtient que pour tout $h_x(j_0) = 0$, pour tout $x \in \mathfrak{X}$. Ceci étant valable pour tout j_0, on obtient en réalité que h_x est la classe nulle, pour tout $x \in \mathfrak{X}$, et donc $h = 0$ et φ est un isomorphisme d'algèbres. □

9 Anneaux de valuation discrète

9.1 Anneaux de valuation

Définition 9.1. *Un anneau intègre A est un anneau de valuation s'il n'est pas un corps, et si pour tout $x \in \mathrm{Frac}(A)$, on a soit $x \in A$, soit $x^{-1} \in A$.*

Lemme 9.2. *Un anneau de valuation est local.*

Démonstration. Si I et J sont deux idéaux de A, montrons que $I \subset J$ ou $J \subset I$. Supposons $I \not\subset J$, et considérons $i \in I \setminus J$. Pour tout $j \in J$ non nul, l'élément $[i,j] \in Frac(A)$ n'appartient pas à A. En effet sinon on aurait pour un $a \in A$, $[a,1] = [i,j]$ et $i = aj$ serait un élément de J (on identifie ici A et $\iota(A)$). On a donc $[i,j]^{-1} = [j,i] \in A$, et $j = i \cdot [j,i]$ appartient un I, c'est à dire $J \subset I$.

L'inclusion induit donc un ordre total sur l'ensemble des idéaux de A, qui possède de fait un unique idéal maximal. □

Proposition 9.3. *Un anneau de valuation est intégralement clos.*

Démonstration. Soit $P(X) = X^n + a_{n-1}X^{n-1} + .. + a_0$ un polynôme unitaire à coefficients dans un anneau de valuation A et x une racine de P dans $Frac(A)$. Si x est dans A il n'y a rien à montrer. Si ce n'est pas le cas x^{-1} appartient à A.

Par hypothèse on a l'égalité

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0,$$

c'est à dire $x^n = -(a_{n-1}x^{n-1} + ... + a_1x + a_0)$. En divisant par x^{n-1} on obtient

$$x = -(a_{n-1} + a_{n-2}x^{-1} + ... + a_0x^{-n+1})$$

et x est bien lui aussi un élément de A. □

9.2 Définition et caractérisation algébrique

Définition 9.4. *Une valuation discrète sur un corps K est une fonction*

$$v : K^* \longrightarrow \mathbb{Z}$$

qui vérifie les propriétés suivantes :

1. *v est surjective ;*
2. *$v(xy) = v(x) + v(y)$;*
3. *si $x \neq y$, $v(x+y) \geq \min\{v(x), v(y)\}$.*

Il est d'usage de poser de plus $v(0) = \infty$ pour étendre la propriété 3. à tout couple $(x,y) \in (K^*)^2$.

Lemme 9.5. *Si v est une valuation discrète sur un corps K, l'ensemble*

$$K_v = \{x \in K,\ v(x) \geq 0\}$$

est un anneau de valuation.

Démonstration. On montre d'une part que K_v est un sous-anneau de K. Par hypothèse on a $0 \in K_v$, et par la propriété 2. $1 \in K_v$ car $v(1) = 0$ d'après l'égalité

$$v(1) = v(1 \cdot 1) = v(1) + v(1).$$

Les propriétés 2. et 3. assurent que K_v est stable par somme et produit.

L'anneau K_v est intègre (car contenu dans K) et $\mathrm{Frac}(A)$ est contenu dans K. D'après 2. et $v(1) = 0$, on a $v(b) + v([1, b]) = 0$ donc naturellement

$$v([a, b]) = v(a) - v(b)$$

pour tout $[a, b] \in \mathrm{Frac}(A)$. En particulier $v([a, b]) = -v([b, a])$ et K_v est un anneau de valuation car il n'est pas un corps (sinon v serait identiquement nulle, ce qui contredit sa surjectivité). □

Définition 9.6. *Un anneau intègre A est un anneau de valuation discrète, s'il existe une valuation v sur* $\mathrm{Frac}(A)$ *pour laquelle* $A = \mathrm{Frac}(A)_v$.

Lemme 9.7. *Soit A un anneau de valuation discrète. Un élément $a \in A^*$ est inversible si et seulement si $v(a) = 0$.*

Démonstration. On a vu que $v(1) = 0$. Si $a \in A$ est inversible, on a nécessairement $v(a) + v(a^{-1}) = v(1) = 0$, c'est à dire $v(a) = v(a^{-1}) = 0$.

Réciproquement si $a \in A^*$ est de valuation nulle, on calcule dans $\mathrm{Frac}(A)$

$$0 = v(1) = v(a \cdot [1, a]) = v(a) + v([1, a])$$

donc $a^{-1} = [1, a]$ est de valuation nulle et a est bien inversible dans A. □

Proposition 9.8. *Un anneau de valuation discrète est euclidien, donc principal.*

Démonstration. Un tel anneau A est intègre, et v définit un stasthme euclidien. Soient a, b sont deux éléments de A^*, avec b non-nul. Si $v(b) \leq v(a)$, alors l'élément $[a, b] \in \mathrm{Frac}(A)$ appartient à A, donc on peut poser

$$a = b \cdot [a, b] + 0,$$

et si $v(b) > v(a)$, alors on peut simplement poser $a = 0 \cdot b + a$. □

Exemples 9.9. *1. Si k est un corps, l'anneau $k[[X]]$ des séries formelles est de valuation discrète.*

2. Les entiers p-adiques forment un anneau de valuation discrète.

Définition 9.10. *Si A est un anneau de valuation discrète, un élément a de A qui satisfait $v(a) = 1$ est appelé une uniformistante.*

La valuation v étant surjective par hypothèse, tout anneau de valuation discrète admet une uniformisante.

Proposition 9.11. *Soit A un anneau de valuation discrète, t une uniformisante.*

1. *Si $x \in \mathrm{Frac}(A)^*$, il existe u inversible tel que $x = ut^{v(x)}$.*
2. *Tout idéal propre de A est principal, engendré par une puissance de t.*
3. *L'anneau A a pour unique idéal maximal $< t >= \{a \in A,\ v(a) > 0\}$ et son spectre est $\mathrm{Spec}(A) = \{\{0\}, < t >\}$.*

Démonstration.

1. L'élément $u = xt^{-v(x)}$ est de valuation 0, c'est donc un élément inversible de A. On obtient bien alors $x = ut^{v(x)}$.
2. Si I est un idéal de A, on fixe $i \in I$ un élément de valuation minimale. Si $v(i) = 0$ alors $I = A$, et si $v(i) = n$, alors $i = ut^n$ pour u inversible, c'est à dire $< t^n > \subset I$. Réciproquement si $j \in I$ est non nul, alors $j = u't^m$ avec $m \geq n$ et u' inversible donc $I =< t^n >$.
3. Les idéaux propres de A sont les $< t^n >$, avec $n \geq 1$. Ces idéaux sont emboîtés puisque pour tout entier k on a une inclusion stricte $< t^{k+1} > \subsetneq < t^k >$ (A est intègre). Le seul idéal premier non-nul de A est ainsi $< t >$, qui est maximal.

□

On désormais établir une première caractérisation algébrique des anneaux de valuation discrète.

Théorème 9.12. *Soit A un anneau. Les assertions suivantes sont équivalentes.*

1. *A est un anneau de valuation discrète ;*
2. *A est un anneau local et principal, sans être un corps ;*
3. *A est factoriel avec un unique élément irréductible (à association près).*

Démonstration. 1. $\Rightarrow$ 2. Découle des lemmes 9.2 et 9.8.

2. $\Rightarrow$ 3. A est principal donc factoriel. En outre, à association près, les éléments irréductibles de A sont en bijection avec les idéaux maximaux non-nuls de A. L'anneau A étant local sans être un corps, il possède un unique élément irréductible (toujours à association près).

3. $\Rightarrow$ 1. En notant t un élément irréductible de A, tout élément de A^* est associé par factorialité à une puissance de t (nulle pour les inversibles). En particulier si $x \in \mathrm{Frac}(A)$ appartient à son corps des fractions on a un entier n_x et un inversible $u \in A$ tel que $x = ut^{n_x}$. L'application

$$\begin{array}{rccc} v : & \mathrm{Frac}(A) & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & n_x \end{array}$$

est clairement une valuation, avec $A = \mathrm{Frac}(A)_v$. □

9.3 Lemme de Nakayama

Théorème 9.13. *Soit A un anneau et M un A-module de type fini, $\varphi \in \mathrm{Hom}_A(M,M)$ et I un idéal de A tel que $\varphi(M) \subset IM$. Alors φ est annulé par un polynôme unitaire à coefficients dans I.*

Démonstration. En notant $\{m_1, ..., m_n\}$ un système de générateurs de M, on observe d'une part que tout élément de IM s'écrit comme une somme $i_1m_1+...+i_nm_n$, où les $(i_j)_{j=1}^n$ sont des éléments de I.

Par hypothèse pour tout $i = 1, ..., n$ on a on a $\varphi(m_i) \in IM$, c'est à dire

$$\varphi(m_i) = \sum_{j=1}^{n} c_{ij}m_j$$

avec $(c_{ij})_{j=1}^n$ dans I. Le morphisme φ agit donc via la matrice $C = (c_{ij})_{i,j=1}^n$. Le théorème de Cayley-Hamilton implique donc que χ est racine du polynôme caractéristique de C qui est bien unitaire et à coefficients dans I. □

Corollaire 9.14. *Soit A un anneau, M un A-module de type fini et I un idéal de A tel que $IM = M$. Alors il existe $x \in 1 + I$ tel que $xM = \{0\}$.*

Démonstration. On applique le théorème 9.13 à l'application $\varphi = Id_M$.

Puisqu'on a $\varphi(M) = M = IM$, il existe des éléments $i_1, ..., i_n$ dans I tel que

$$\varphi^n + i_1\varphi^{n-1} + ... + i_{n-1}\varphi + i_n id_M = 0$$

mais φ étant elle-même l'identité on obtient

$$(1 + i_1 + ... + i_n)\varphi = 0.$$

L'élément $x = 1 + i_1 + ... + i_n \in 1 + I$ vérifie donc

$$xM = x\varphi(M) = (x\varphi)(M) = 0.$$

□

Définition 9.15. *L'intersection de tous les idéaux maximaux d'un anneau A est le radical de Jacobson de A.*

Corollaire 9.16 (Lemme de Nakayama)**.** *Soit A un anneau.*

1. *Si A est local d'idéal maximal $\mathfrak{m}$, alors pour tout A-module M de type fini, $M\mathfrak{m} = 0$ implique $M = 0$.*
2. *Si $\mathfrak{R}$ est le radical de Jacobson de A, alors pour tout A-module M de type fini, $\mathfrak{R}M = M$ implique $M = 0$.*

Démonstration. 1. Le corollaire 9.14 avec $I = \mathfrak{m}$ indique $(1+a)M = 0$ pour un $a \in \mathfrak{m}$, mais $1+a$ n'appartient pas à $\mathfrak{m}$ donc est inversible, et $M = 0$.

2. À nouveau on a $a \in \mathfrak{R}$ tel que $(1+a)M = 0$, et il reste à montrer que $1+a$ est inversible. S'il ne l'était pas, l'idéal $< 1+a >$ serait contenu dans un idéal maximal $\mathfrak{m}$, mais $a \in \mathfrak{R} \subset \mathfrak{m}$ donc 1 appartient à $\mathfrak{m}$, absurde.

□

9.4 Une caractérisation géométrique

À l'aide du lemme de Nakayama, nous allons désormais proposer une nouvelle caractérisation des anneaux de valuation discrète, à la saveur plus géométrique.

Définition 9.17. *Si X est un espace topologique, une chaîne de fermés irréductibles de X de longueur n est une suite*

$$Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_n \subset X$$

où $Z_0, ..., Z_n$ sont des fermés irréductibles de X. La dimension (ou dimension de Krull) de X est le supremum des longueurs de des chaînes de fermés irréductibles de X ; on la note $\dim(X)$.

Le théorème 6.26 justifie la définition suivante.

Définition 9.18. *La dimension (ou dimension de Krull) d'un anneau A est la dimension du spectre* $\mathrm{Spec}(A)$*, muni de la topologie de Zariski ; on la note* $\dim(A)$. *Elle correspond au supremum des longueurs de chaînes d'idéaux premiers*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_n.$$

Exemples 9.19. *1. Un corps k est de dimension 0 ;*

2. L'anneau $\mathbb{Z}$ est de dimension 1 ;

3. L'anneau $k[X_1, ...X_n]$ des polynômes en n variables à coefficients dans un corps k est de dimension n.

Proposition 9.20. *Le spectre* $\mathrm{Spec}(A)$ *d'un anneau, muni de la topologie de Zariski, est séparé si et seulement s'il est de dimension* 0.

Démonstration. Il s'agit simplement d'une traduction de la proposition 6.12. □

Théorème 9.21. *Soit A un anneau noethérien et I un idéal de A. Si $x \in \bigcap_{n=1}^{\infty} I^n$, alors $x \in xI$.*

Démonstration. Si $a_1, ..., a_m$ est un système de générateurs de I et $x \in \bigcap_{n=1}^{\infty} I^n$, alors pour tout $n \in \mathbb{N}^*$, on a un polynôme homogène $P_n \in A[X_1, ..., X_m]$ tel que

$$x = P_n(a_1, ..., a_n).$$

Pour tout $n \geq 1$, on note J_n l'idéal de $A[X_1, ..., X_m]$ engendré par les polynômes $P_1, ..., P_n$. La suite d'idéaux $(J_n)_{n\geq 1}$ est croissante donc stationnaire, car $A[X_1, ..., X_m]$ est noethérien. En choisissant un entier N tel que $J_N = J_{N+1}$, on a donc des polynômes $Q_1, ..., Q_N$ tels que

$$P_{N+1}(X_1, ..., X_m) = \sum_{k=0}^{N} Q_k(X_1, ..., X_m) P_k(X_1, ..., X_m).$$

L'évaluation en $(a_1, ..., a_m)$ donne ainsi

$$x = P_{N+1}(a_1, ..., a_m) = x \left(\sum_{k=0}^{N} Q_k(a_1, ..., a_m) \right)$$

est bien un élément de xI. □

Corollaire 9.22 (Théorème d'intersection de Krull)**.** *Soit A un anneau noethérien. Dans les deux situations suivantes*

1. *A est intègre et I est un idéal propre ;*
2. *A est quelconque et I est contenu dans le radical de Jacobson A*

on a $\bigcap_{n=1}^{\infty} I^n = 0$.

Démonstration. D'après le théorème 9.21 on sait que si $x \in \bigcap_{n=1}^{\infty} I^n$, alors il existe $i \in I$ tel que $x = xi$.

1. Si A est intègre, on a donc bien $x(1 - i) = 0$ et $i \neq 1$ (I est propre) donc $x = 0$.
2. On a vu au cours de la preuve du corollaire 9.16, 2. que si $a \in A$ appartient au radical de Jacobson $\mathfrak{R}$, alors $1 + a$ est inversible. L'égalité $x(1 - i)$ avec $i \in I \subset \mathfrak{R}$ donne donc bien $x = 0$.

□

Remarque 9.23. *D'autres preuves plus classiques du théorème d'intersection de Krull reposent sur lemme de Nakamaya.*

Théorème 9.24. *Pour A intègre, les conditions suivantes sont équivalentes.*

1. *A est un anneau de valuation discrète.*
2. *A est noethérien, intégralement clos, local et de dimension 1.*

3. A est noethérien, local et d'idéal maximal monogène, sans être un corps.

Démonstration. $\boxed{1. \Rightarrow 2.}$ On a en effet montré précédemment qu'un anneau de valuation discrète est intégralement clos (proposition 9.3), local (lemme 9.2) et de dimension 1 (proposition 9.11).

$\boxed{2. \Rightarrow 3.}$ Comme A est de dimension 1, ce n'est pas un corps. Il s'agit donc de montrer que l'idéal maximal $\mathfrak{m}$ de A est monogène. D'une part comme A est local et noethérien $\mathfrak{m}$ est de type fini et égal à son radical de Jacobson. Par lemme de Nakayama, on a $\mathfrak{m}^2 \neq \mathfrak{m}$. On choisit donc un élément $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ et on montre que t engendre $\mathfrak{m}$.

D'une part, on a $\mathfrak{m} = \sqrt{< t >}$ car $\mathrm{Spec}(A) = \{(0), \mathfrak{m}\}$ (l'anneau A est local et de dimension 1). Supposons que l'entier minimal n_t tel que $\mathfrak{m}^n \subset < t >$ est strictement plus grand que 1. Si $x \in \mathfrak{m}^{n-1}$ n'appartenant pas à $< t >$, on a tout de même $x\mathfrak{m} \subset \mathfrak{m}^n \subset < t >$.

Montrons que l'élément $y = [x, t] \in \mathrm{Frac}(A)$ est entier sur A. Puisqu'on a $x\mathfrak{m} \subset < t >$, $y\mathfrak{m}$ est un idéal contenu dans A. D'une part, c'est un idéal propre car $1 = ym$ implique que $t = tym = xm$ appartient à $\mathfrak{m}^n \subset \mathfrak{m}^2$, ce qui contredit la définition de t. Donc $y\mathfrak{m}$ est un idéal propre, contenu dans $\mathfrak{m}$.

Soient $m_1, ..., m_s$ un système de générateurs de $\mathfrak{m}$. Pour $1 \leq j \leq s$, on a des éléments $a_{ij} \in A$ tel que

$$ym_j = \sum_{i=0}^{s} a_{ij} m_i,$$

c'est à dire pour tout j,

$$\sum_{i=0}^{s} (\delta_{ij} y - a_{ij}) m_i = 0,$$

où δ_{ij} est le symbole de Kronecker. En notant Δ le déterminant de la matrice, le Lemme 2.5 indique que $\Delta\mathfrak{m} = 0$. Comme A est intègre et $\mathfrak{m}$ est non-nul, on obtient $d = 0$, c'est à dire que y est entier, solution du polynôme

$$\Delta(X) = \det\left[((\delta_{ij} X - a_{ij}) m_i)_{i,j}\right].$$

L'anneau A étant intégralement clos on a $y = [x, t] \in A$, donc $x = at$ et $x \in < t >$, contradiction. On a donc $n = 1$ et $\mathfrak{m} = < t >$ est monogène.

$\boxed{3. \Rightarrow 1.}$ D'une part A n'est pas un corps, par hypothèse. On note $< t >$ l'idéal maximal de A. Considérons la une suite décroissante d'idéaux

$$A = < 1 > \subset < t > \subset < t^2 > \subset < t^3 > ...$$

Si a est un élément de A^*, on pose $n_a = \max\{n,\ a \in < t^n >\}$, qui est bien défini car $\bigcap_{n \geq 0} < t^n > = 0$ (corollaire 9.22). On a $a \in A^\times$ si et seulement si $n_a = 0$ et plus généralement par maximalité de n_a, on a $a = ut^{n_a}$ pour un inversible u.

Si I est un idéal de A, on note $N = \min\{n_i,\ i \in I\}$. Tout élément $x \in I$ tel que $n_x = N$ est un engendre l'idéal I. L'anneau A est donc local et principal, c'est à dire un anneau de valuation discrète par le théorème 9.12. □

Corollaire 9.25. *Un anneau A intègre est de valuation discrète si et seulement s'il est local, de Dedekind, et n'est pas un corps.*

Corollaire 9.26. *Un anneau de valuation A est un anneau de valuation discrète si et seulement si A est noethérien.*

Démonstration. Si A est un anneau de valuation discrète, c'est un anneau principal par la proposition 9.8, donc un anneau noethérien.

Réciproquement si A est noethérien et $I =< a_1, ..., a_n >$ est un idéal de A, on montre que I est en réalité monogène. On a en effet vu lors de la preuve du lemme 9.2 que l'inclusion induit un ordre total sur les idéaux de A, donc on a un idéal $< a_{i_0} >$ maximal parmi les $< a_i >_{i=1}^n$ et a_{i_0} engendre I. L'anneau A est donc principal et local, donc de valuation discrète par le théorème 9.12. □

Corollaire 9.27. *Soit A un anneau intègre, noethérien et intégralement clos. Si $\mathfrak{p} \in \mathrm{Spec}(A)$ est minimal et non-nul, alors $A_\mathfrak{p}$ est un anneau de valuation discrète.*

Démonstration. Le localisé $A_\mathfrak{p}$ n'est pas un corps car $\mathfrak{p}$ est non-nul, c'est un anneau noethérien, intégralement clos, local et de dimension 1. □

Bibliographie

[1] Lang, S., *Algebra*, Graduate Texts in Mathematics 211, Springer (2002)