
**ALGÈBRE
APPROFONDIE**
Notes de M2 (1995–1996)

Chris Peters

**Université de Grenoble I
Saint-Martin d'Hères, France**

26 Mai, 1997

Sommaire

Chapitre 1. Anneaux et idéaux	1
§ 1. Notions de base	1
§ 2. Diviseurs de zéro, nilpotents	3
§ 3. Idéaux premiers, maximaux	4
§ 4. Opérations sur les idéaux	6
§ 5. Extension et contraction des idéaux	8
§ 6. Complément géométrique : topologie de Zariski	8
§ 7. Corps de fractions d'un anneau intègre	9
Chapitre 2. Modules	11
§ 1. Notions de base	11
§ 2. Sommes et produits	12
§ 3. Lemme de Nakayama	13
§ 4. Suites exactes	15
§ 5. Produit tensoriel	17
§ 6. Produit tensoriel et suites exactes	19
§ 7. Algèbres	21
Chapitre 3. Anneaux et modules de fractions	24
§ 1. Fractions : anneaux	24
§ 2. Fractions : modules	26
§ 3. Principe local-global	27
§ 4. Spectre d'un anneau, support d'un module	28
Chapitre 4. Anneaux et modules noethériens et artiniens	31
§ 1. Conditions de chaîne : anneaux	31
§ 2. Théorème de base de Hilbert	31
§ 3. Conditions de chaîne : modules	32
§ 4. Modules et anneaux de longueur finie	33
Chapitre 5. Décomposition primaire	37
§ 1. Idéaux premiers	37
§ 2. Application : spectre d'un anneau noethérien	38
§ 3. Unicité des décompositions primaires	39
§ 4. Assassin et support	40
Chapitre 6. Extensions finies	43
§ 1. Extensions entières ou de type fini	43
§ 2. "Going-up"	45
§ 3. Théorème de normalisation de Noether	46
§ 4. Nullstellensatz	48

Chapitre 7. Anneaux de valuations discrète	51
§ 1. Notions de base	51
§ 2. Caractérisation	52
§ 3. Applications	52
Chapitre 8. Dimension	55
§ 1. Degré de transcendance	55
§ 2. Dimension d'une variété affine	56
§ 3. Dimension de Krull	57
§ 4. Les théorèmes de Krull	59
§ 5. Quelques applications	60
§ 6. Anneaux réguliers	62
Chapitre 9. Algèbre homologique	64
§ 1. Complexes et leur (co)homologie	64
§ 2. Modules projectifs, injectifs et suites exactes scindées	65
§ 3. Ext et Tor	67
§ 4. Dimension homologique	70
§ 5. Théorème des syzygies de Hilbert	71
Références	75

Chapitre 1. Anneaux et idéaux

§ 1. Notions de base

1.1. Définition. Un **anneau** A est un ensemble muni de deux opérations $+$ (addition) et \cdot (multiplication) telles que :

- 1) $(A, +)$ est un groupe abélien.
2. La multiplication est associative :

$$\forall a, b, c \in A \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

et distributif par rapport à l'addition

$$\begin{aligned} \forall a, b, c \in A \quad a \cdot (b + c) &= a \cdot b + a \cdot c; \\ (a + b) \cdot c &= a \cdot c + a \cdot c. \end{aligned}$$

On ne regarde ici que des anneaux **commutatifs** :

$$\forall a, b \in A \quad a \cdot b = b \cdot a$$

muni d'une **unité** 1 :

$$\forall a \in A \quad 1 \cdot a = a \cdot 1 = a.$$

Remarque. On ne supposera pas que $1 \neq 0$ et donc $A = \{0\}$ est un anneau. En effet, si $1 = 0$ on a $\forall a \in A \quad a = a \cdot 1 = a \cdot 0 = 0$ et donc forcément $A = \{0\}$.

1.2. Définition. Un sous-ensemble S d'un anneau A est un **sous-anneau**, si S est un sous-groupe pour l'addition, stable par multiplication et $1 \in S$.

1.3. Définition. Soient A, B deux anneaux. Une application $f : A \rightarrow B$ est un **homomorphisme d'anneaux**, si :

- 1) $\forall a, b \in A \quad f(a + b) = f(a) + f(b),$
- 2) $\forall a, b \in A \quad f(a \cdot b) = f(a) \cdot f(b),$
- 3) $f(1) = 1.$

1.4. Exemples.

- 1) \mathbb{Z}, \mathbb{Q} . De plus \mathbb{Z} est un sous-anneau de \mathbb{Q} .
- 2) Un **corps** k est un anneau (commutatif) $\neq 0$ tel que chaque élément non-nul est inversible : $\forall a \in k, a \neq 0, \exists b \in k$ tel que $b \cdot a = 1$. L'élément b est unique et est noté $b = a^{-1}$ (l'**inverse** de a). Exemples : $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$.
- 3) Soit A un anneau (commutatif). L'anneau polynômial associé est

$$A[X] := \{a_0 + a_1X + \dots + a_kX^k ; k = 0, 1, \dots, a_i \in A, i = 0, \dots, k\}$$

avec l'addition et la multiplication usuelle. A est un sous-anneau de $A[X]$. Plus généralement on a $A[X_1, \dots, X_n]$, l'anneau à n variables avec coefficients dans A .

- 4) L'anneau de séries formelles à coefficients dans un anneau A :

$$A[[X]] := \left\{ \sum_{k=0}^{\infty} a_k X^k ; \forall k \geq 0, a_k \in A \right\}$$

avec l'addition et la multiplication usuelle (i.e. la multiplication est donnée par $\sum_{k=0}^{\infty} a_k X^k \cdot \sum_{k=0}^{\infty} b_k X^k = \sum_{n=0}^{\infty} \left(\sum_{k+\ell=n} a_k b_\ell \right) X^n$.

- 5) L'anneau de séries de Laurent à coefficients dans un anneau A :

$$A\{\{X\}\} := \left\{ \sum_{k=\ell}^{\infty} a_k X^k ; \ell \in \mathbb{Z}, \forall k \geq \ell, a_k \in A \right\}$$

avec l'addition et la multiplication usuelle.

- 6) L'anneau $\mathbb{Z}/n\mathbb{Z}$ (entiers modulo n). L'application $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ qui à un entier associe sa classe modulo n est un homomorphisme d'anneaux.

1.5. Définition. Un sous-ensemble I d'un anneau A est un **idéal**, si I est stable par l'addition et si $\forall a \in A, a \cdot I \subset I$.

N.B. Un idéal est stable par addition et multiplication et donc peut être considéré comme sous-anneau (sans 1), mais la réciproque est faux.

1.6. Exemples.

- 1) Soit $x \in A$. L'idéal engendré par x est l'ensemble $\{a \cdot x ; a \in A\}$. C'est le plus petit idéal contenant x . Plus généralement, soit $S \subset A$. L'idéal engendré par S consiste en les combinaisons linéaires finies d'éléments de S , donc en les éléments de la forme $\{\sum_{j=1}^n a_j \cdot s_j ; a_j \in A; s_j \in S\}$.
- 2) Soient I et J deux idéaux. Leur somme $I + J$ consiste en les sommes de la forme $i + j$, $i \in I, j \in J$. C'est aussi un idéal de A . Leur produit $I \cdot J$ consiste en les sommes finies des produit d'éléments de I et J : $\{\sum_{k=1}^n a_k \cdot i_k \cdot j_k ; a_k \in A; i_k \in I; j_k \in J\}$. C'est le plus petit idéal contenant les produits $i \cdot j$, $i \in I, j \in J$. L'intersection $I \cap J$ est aussi un idéal. On a $I \cdot J \subset I \cap J$. Par exemple pour $A = \mathbb{Z}, I = (n), J = (m), I + J = (\text{pgcd}(m, n)), I \cdot J = (n \cdot m), I \cap J = (\text{ppcm}(n, m))$.

Soit I un idéal de A . On regarde le groupe quotient A/I . La multiplication de A persiste en A/I car si $a' = a + i$, $b' = b + j$, $i, j \in I$, alors $a' \cdot b' = a \cdot b + a \cdot j + b \cdot i + i \cdot j$ et donc dans la même classe modulo I que $a \cdot b$ car I est un idéal. L'application canonique

$$p : A \rightarrow A/I, \quad x \mapsto x + I$$

est un homomorphisme d'anneaux ayant la propriété suivante :

1.7. Lemme. *Il y a une correspondance biunivoque entre les idéaux \bar{J} de A/I et les idéaux J de A contenant I donnée par $J \mapsto p(J)$ et $\bar{J} \mapsto p^{-1}\bar{J}$.*

Soit $f : A \rightarrow B$ un homomorphisme d'anneaux quelconque. Le **noyau** $\text{Ker } f := f^{-1}(0)$ est un idéal de A et l'**image** $\text{Im } f = f(A)$ est un sous-anneau de B . On a :

1.8. Théorème. *Soit $f : A \rightarrow B$ homomorphisme d'anneau. Alors f induit un isomorphisme*

$$\bar{f} : A/\text{Ker } f \xrightarrow{\cong} \text{Im } f.$$

§ 2. Diviseurs de zéro, nilpotents

Soit A anneau commutatif avec 1.

2.1. Définition.

- i. $x \in A$ est un **diviseur de zéro** si $\exists y \neq 0, y \in A$ tel que $x \cdot y = 0$.
- ii. $x \in A$ est **nilpotent** si $\exists n \in \mathbb{N}$ tel que $x^n = 0$.
- iii. $x \in A$ est **inversible** si $\exists y \in A$ tel que $x \cdot y = 1$. L'ensemble d'éléments inversibles de A est un groupe, appelé **groupe des unités** de A et noté A^\times .
- iv. On dit que A est **intègre** si A n'a pas de diviseurs de zéro sauf 0.

2.2. Exemples.

- 1) Soit $\mathbb{Z}/pq\mathbb{Z}$ avec p et q nombres premiers. Les classes de p et q sont des diviseurs de zéro, mais si $p \neq q$ la classe \bar{p} de p n'est pas nilpotente : $\bar{p}^n = 0$ veut dire $p^n = xpq$ et donc $p^{n-1} = xq$, ce qui est impossible.
- 2) Les anneaux \mathbb{Z} , \mathbb{F}_p (p premier), $k[X_1, \dots, X_n]$ (k un corps) sont intègres.
- 3) Soit p premier. Les éléments inversibles de \mathbb{F}_p sont les classes de $1, 2, \dots, p-1$.

Pour déterminer le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ on utilise :

Théorème des restes Chinois. *Soient I et J deux idéaux de A avec $I + J = A$ (on dit que I et J sont étrangers). Alors l'application $x \mapsto (x + I, x + J)$ induit un isomorphisme :*

$$\varphi : A/(I \cdot J) \cong A/I \times A/J.$$

Démonstration.

1. $I \cap J = I \cdot J$. On a toujours $I \cap J \supset I \cdot J$, donc il reste à montrer l'inclusion $I \cap J \subset I \cdot J$. Or, on a

$$1 = x + y, \quad x \in I, y \in J$$

et donc $\forall z \in I \cap J, z = z \cdot 1 = z \cdot (x + y) = z \cdot x + z \cdot y \in I \cdot J$.

2. Injectivité : $\text{Ker } \varphi = I \cap J = I \cdot J$.

3. Surjectivité : $\varphi(x) = (0, 1)$, $\varphi(y) = (1, 0)$ et donc $\varphi(ax + by) = (b, a)$. ■

2.3. Application. Soit $n \in \mathbb{N}$ et soient p_1, \dots, p_m les diviseurs premiers de n . L'anneau $\mathbb{Z}/n\mathbb{Z}$ possède

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right)$$

éléments inversibles.

Démonstration. Si r et s sont étrangers, le théorème implique que $(\mathbb{Z}/rs\mathbb{Z})^\times \cong (\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times$ et donc il suffit de montrer la formule pour $n = p^m$, p premier. Dans ce cas, les éléments non-inversibles sont les p^{m-1} multiples de p , d'où $p^m - p^{m-1} = p^m \left(1 - \frac{1}{p}\right)$ éléments inversibles. ■

§ 3. Idéaux premiers, maximaux

3.1. Définition.

- 1) Un idéal $\mathfrak{p} \subset A$, $\mathfrak{p} \neq A$ est **premier** si $x \cdot y \in \mathfrak{p}$ implique soit $x \in \mathfrak{p}$, soit $y \in \mathfrak{p}$.
- 2) Un idéal $\mathfrak{m} \subset A$, $\mathfrak{m} \neq A$ est **maximal** si pour un idéal I tel que $I \supset \mathfrak{m}$, on a soit $I = \mathfrak{m}$, soit $I = A$.

Le critère suivant est une traduction immédiate de la définition :

3.2. Critère. Un idéal I est premier, resp. maximal si et seulement si A/I est intègre, resp. un corps.

Il existe beaucoup d'idéaux maximaux grâce à :

3.3. Proposition. Tout idéal $I \neq A$ est contenu dans un idéal maximal.

La preuve dépend du principe de "récurrence transfinie" : si I n'est pas maximal, il y a un idéal $J_1 \neq A$ qui le contient. Si on continue cette procédure, on tombe finalement sur un idéal maximal. Ce principe, bien qu'intuitivement clair dépend du fait que chaque fois on choisit un idéal parmi un nombre d'idéaux, qui pourrait être dénombrable ou même pire. Ce principe est connu comme "Lemme du choix" et vous trouvez dans [van der Waerden : Algebra I, §69] la preuve que ce lemme est équivalent au "principe de Zorn" que nous expliciterons. Il s'agit d'un ensemble S non-vide muni d'un **ordre partiel** \leq (i.e. une relation réflexive et transitive définie sur un sous-ensemble de $S \times S$). Un sous-ensemble T totalement ordonné est une chaîne de S ($\forall x, y \in T$, soit $x \leq y$, soit $y \leq x$). Une borne supérieure de T est $s \in S$ t.q. $t \leq s, \forall t \in T$ et un **sup** de T est une borne supérieure s_0 t.q. $s_0 \leq s$ pour chaque borne supérieure s de T . Finalement, un **élément maximal** s de S est tel que pour $s' \in S$, $s \leq s'$, alors $s = s'$.

Principe de Zorn. Soit $S \neq \emptyset$ un ensemble muni d'un ordre partiel \leq . Si chaque chaîne T de S admet un sup, alors S admet un élément maximal.

Dans le cas de la Proposition ci-dessus, on prend l'ordre donné par l'inclusion et pour S on prend l'ensemble d'idéaux $J \neq A$ contenant l'idéal I .

3.4. Exemple.

- 1) Un élément $x \in A$ non-inversible est **irréductible** si $x = u \cdot v$ implique soit u est inversible, soit v est inversible. On dit que A est un **anneau factoriel** si chaque élément s'écrit de façon unique comme produit d'un élément inversible et d'éléments irréductibles. (Unicité dans le sens suivant : les irréductibles dans la décomposition de x sont déterminés uniquement par x). Exemples :

- Un anneau euclidien (par exemple \mathbb{Z} , $\mathbb{Z}[i]$, $k[X]$ avec k un corps).
- (Lemme de Gauss) Si R est factoriel, alors $R[X]$ l'est (par exemple $k[X_1, \dots, X_m]$, k un corps).

Dans un tel anneau un idéal (x) engendré par x est premier si et seulement si x est irréductible.

- 2) Dans l'anneau $\mathbb{Z}[\sqrt{-5}]$, 2 est irréductible, mais (2) n'est pas premier, car $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in (2)$, mais $(1 \pm \sqrt{-5}) \notin 2\mathbb{Z}[\sqrt{-5}]$.
- 3) Un anneau avec un seul idéal maximal \mathfrak{m} est appelé **anneau local**, écrit comme couple (A, \mathfrak{m}) . Le corps A/\mathfrak{m} est appelé **corps résiduel**. Exemples : un corps, l'anneau

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} ; (n, p) = 1 \right\}$$

où p est premier. L'idéal maximal est $p \cdot \mathbb{Z}_{(p)}$. Le corps résiduel est \mathbb{F}_p .

Les anneaux locaux sont caractérisés par la proposition suivante :

3.5. Proposition.

- 1) Soit A un anneau et \mathfrak{m} un idéal tel que $A^\times = A \setminus \mathfrak{m}$. Alors (A, \mathfrak{m}) est un anneau local.
- 2) Soit (A, \mathfrak{m}) un anneau local, alors les éléments de la forme $x = 1 + y$, $y \in \mathfrak{m}$ sont inversibles. Inversement, soit A un anneau et \mathfrak{m} un idéal maximal tel que $1 + \mathfrak{m} \subset A^\times$, alors \mathfrak{m} est le seul idéal maximal.

Démonstration.

- 1) Un idéal $I \neq A$ ne contient que des éléments non-inversibles (car les éléments inversibles engendrent A tout entier). Donc $I \subset \mathfrak{m}$ et \mathfrak{m} est le seul idéal maximal.
- 2) Si $x = 1 + y$ avec $y \in \mathfrak{m}$, alors x est inversible. Sinon, x doit être contenu dans un idéal maximal, forcément \mathfrak{m} , une contradiction, car $1 \notin \mathfrak{m}$. Inversement, soit $x \in A \setminus \mathfrak{m}$. L'idéal engendré par x et \mathfrak{m} est A car \mathfrak{m} est maximal. Donc $\exists t \in \mathfrak{m}$, $1 = x \cdot y + t$ ce qui implique $x \cdot y = 1 - t \in 1 + \mathfrak{m} \subset A^\times$. Conclure en appliquant 1). ■

L'intersection des idéaux premiers et des idéaux maximaux forment eux-mêmes d'idéaux. On verra que le premier est égal au

$$\text{radical de zéro} = \sqrt{0} = \{x \in A ; \exists n \in \mathbb{N}, x^n = 0\}$$

et le dernier par définition est

$$\text{le radical de Jacobson} = \mathfrak{n} = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

On a

3.6. Proposition.

- 1) Le radical de zéro est un idéal.
- 2) On a $\sqrt{0} = \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$.
- 3) Pour le radical de Jacobson on a $\mathfrak{n} = \{x \in A ; 1 - x \cdot y \in A^\times, \forall y \in A\}$

Démonstration.

1) Si $x^n = 0$, $y^m = 0$, le binôme de Newton montre aussitôt que $(x + y)^{n+m-1} = 0$ et puisque $a \cdot (\text{nilpotent})$ est nilpotent, il s'ensuit que $\sqrt{0}$, l'ensemble des nilpotents de A forment bien un idéal.

2) Si $x \in \sqrt{0}$, de $x^n = 0 \in \mathfrak{p}$ pour un idéal premier \mathfrak{p} quelconque, on a $x \in \mathfrak{p}$ et donc l'inclusion $\sqrt{0} \subset \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$.

Pour l'implication réciproque, soit $x \notin \sqrt{0}$. Soit S l'ensemble des idéaux J qui ne contiennent aucune puissance de x . $S \neq \emptyset$ car $0 \in S$. Par le principe de Zorn, il y a un élément maximal $\mathfrak{p} \in S$. A montrer que \mathfrak{p} est premier (cela impliquera $x \notin \mathfrak{p}$). Soient $y, z \notin \mathfrak{p}$, alors les idéaux $\mathfrak{p} + (y)$ et $\mathfrak{p} + (z)$ contiennent \mathfrak{p} strictement et donc n'appartiennent pas à S . Il s'ensuit que $\exists n, m$ tels que $x^n \in \mathfrak{p} + (y)$, $x^m \in \mathfrak{p} + (z)$ et donc $x^{mn} \in \mathfrak{p} + (y \cdot z)$ et aussi $\mathfrak{p} + (y \cdot z)$ n'appartient pas à S . Par conséquent $y \cdot z \notin \mathfrak{p}$.

3) Supposons que $x \in \mathfrak{n}$ et soit $1 - xy$ non-inversible. Il existe un idéal maximal \mathfrak{m} contenant $1 - xy$. Mais $x \in \mathfrak{n} \subset \mathfrak{m}$, donc $xy \in \mathfrak{m}$ et donc $1 \in \mathfrak{m}$. Contradiction.

Inversement, soit $x \in A$ tel que $\exists \mathfrak{m}$, idéal maximal avec $x \notin \mathfrak{m}$. Alors $(\mathfrak{m}, x) = (1) = A$: $\exists z \in \mathfrak{m}, y \in A, z + x \cdot y = 1$ et donc $z = 1 - x \cdot y \in \mathfrak{m}$ et z ne peut pas être inversible. ■

§ 4. Opérations sur les idéaux

On a déjà introduit la somme et le produit de deux idéaux. Plus généralement on a pour un ensemble $I_\alpha, \alpha \in \Sigma$:

$$\sum_{\alpha \in \Sigma} I_\alpha = \left\{ \sum_{\alpha} x_\alpha ; x_\alpha \in I_\alpha, \quad x_\alpha = 0 \text{ sauf pour un nombre fini d'indices } \alpha \right\}.$$

Pour $\Sigma = \{1, \dots, n\}$ fini on a :

$$\prod_{i=1}^n I_i = \left\{ \sum_{i \in I} x_{1,i} \cdot x_{2,i} \cdots x_{n,i} ; x_{j,i} \in I_j, j = 1, \dots, n, \quad I \text{ ensemble fini} \right\}.$$

Un cas particulier: $I^n =$ idéal engendré par les produits de n éléments de I .

L'intersection d'un nombre fini d'idéaux est aussi un idéal et on a montré pour deux idéaux I et J :

$$I \cap J \supset I \cdot J, \quad \text{et on a } I \cap J = I \cdot J \text{ lorsque } I + J = A.$$

Rappel :

4.1. Définition. Soient I et J deux idéaux. On dit que I et J sont étrangers si $I + J = A$.

On a une généralisation du théorème des restes Chinois :

Théorème des restes Chinois. Soient $I_j, j = 1, \dots, n$ des idéaux deux à deux étrangers. Alors on a un isomorphisme d'anneaux :

$$\varphi : A / \prod_{j=1}^n I_j \xrightarrow{\cong} \prod_{j=1}^n (A/I_j)$$

$$\bar{x} \mapsto (x + I_1, \dots, x + I_n) \quad x \in A.$$

Démonstration.

1) Surjectivité. Il suffit de montrer que, pour tout $j = 1, \dots, n$, $\exists x_j \in A$ tel que $x_j = 1 + I_j$, $x_j = 0 + I_k, k \neq j$. Puisque I_k et I_j sont étrangers, pour $k \neq j$ existent $y_k \in I_j, z_k \in I_k$ tel que $y_k + z_k = 1$. Alors $x_j = \prod_{k \neq j} z_k$ convient :

$$x_j = \prod_{k \neq j} (1 - y_k) = 1 + I_j$$

$$x_j \in \prod_{k \neq j} I_k \subset I_k, k \neq j.$$

2) Il faut montrer que le noyau $I_1 \cap \dots \cap I_j$ est égal à $\prod_{j=1}^n I_n$. On le voit par récurrence. On l'a vu pour $n = 2$. On suppose $n > 2$ et on pose (en utilisant l'hypothèse de récurrence) :

$$J = I_2 \cap \dots \cap I_n = I_2 \cdots I_n.$$

Comme dans la preuve de 1) on a $\forall k \neq 1, \exists z_k \in I_1, y_k \in I_k$, tel que $y_k + z_k = 1$ et $y_2 \cdots y_n \in J$ et en même temps on a $y_2 \cdots y_n = 1 + I_1$. Donc $I_1 + J = A$ et par récurrence on a : $I_1 \cdots I_n = I_1 \cdot J = I_1 \cap J = I_1 \cap I_2 \cap \dots \cap I_n$. ■

Trois autres opérations sont utilisées :

4.2. Définition. Soient I, J deux idéaux de A .

- 1) Le **transporteur** de J dans I est $(I : J) = \{x \in A ; x \cdot J \subset I\}$,
- 2) L'**annulateur** de I est $(0 : I) = \{x \in A ; x \cdot I = 0\}$,
- 3) La **racine** (ou le **radical**) de I est $\sqrt{I} = \{x \in A ; x^n \in I\}$.

On vérifie aisément que le transporteur est un idéal. Pour la racine, la preuve déjà donné pour le cas particulier $I = 0$ marche aussi dans le cas général : \sqrt{I} est un idéal.

4.3. Exemple.

- 1) Dans \mathbb{Z} , $I = (n), J = (m)$, alors $(I : J) = \left(\frac{n}{(m,n)}\right)$.
- 2) Dans \mathbb{Z} , si $m = \prod_j p_j^{m_j}, p_j$ premier, on a $\sqrt{(m)} = (\prod_j p_j)$.

Les propriétés du lemme suivant sont laissées au lecteur :

4.4. Lemme.

- 1) Pour deux idéaux I et J on a $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
- 2) Pour un idéal premier \mathfrak{p} on a $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.
- 3) On a $\sqrt{I} = \bigcap_{\mathfrak{p} \text{ premier } \supset I} \mathfrak{p}$.

On a deux propriétés pour les idéaux premiers qui seront utiles plus tard :

4.5. Proposition.

- 1) (Évitement des idéaux premiers) Soient $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ des idéaux premiers tels que $I \subset \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n$, alors I est contenu dans un des \mathfrak{p}_j ,
- 2) Soient I_1, \dots, I_n des idéaux quelconques et \mathfrak{p} un idéal premier tel que $\mathfrak{p} \supset I_1 \cap \dots \cap I_n$. Alors \mathfrak{p} contient un des I_j . De plus si $\mathfrak{p} = I_1 \cap \dots \cap I_n$, alors $\mathfrak{p} = I_j$ pour un indice j .

Démonstration.

1) On montre par récurrence que $I \not\subset \mathfrak{p}_j$, $j = 1, \dots, n$ implique $I \not\subset \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n$. C'est vrai pour $n = 1$ et on suppose donc que $n \geq 2$. Par hypothèse de récurrence, $\forall i, \exists x_i \in I$ et $x_i \notin \mathfrak{p}_j$, $j \neq i$. S'il existe i_0 tel que $x_{i_0} \in I$ et $x_{i_0} \notin \mathfrak{p}_{i_0}$ la preuve se termine. Sinon, $x_i \in \mathfrak{p}_i$ pour $i = 1, \dots, n$ et on considère ($\hat{*}$ signifie qu'il faut omettre $*$) :

$$y = \sum_{j=1}^n x_1 \cdots x_{i-1} \hat{x}_i x_{i+1} \cdots x_n \in I.$$

On ne peut pas avoir $y \in \mathfrak{p}_i$, car dans ce cas $x_1 \cdots x_{i-1} \hat{x}_i x_{i+1} \cdots x_n \in \mathfrak{p}_i$ implique qu'au moins un des x_j est dans \mathfrak{p}_i , contrairement à l'hypothèse. Donc $y \notin \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n$, tandis que $y \in I$, ce qui termine la démonstration.

2) On suppose que $\mathfrak{p} \not\supset I_j$, $j = 1, \dots, n$. Soit $x_j \in I_j$ tel que $x_j \notin \mathfrak{p}$. Alors $x_1 \cdots x_n \notin \mathfrak{p}$ car \mathfrak{p} est premier, mais $x_1 \cdots x_n \in I_1 \cap I_2 \cdots \cap I_n$.

Finalement, si $\mathfrak{p} = I_1 \cap \dots \cap I_n$, alors, si $\mathfrak{p} \supset I_j$, forcément $\mathfrak{p} = I_j$. ■

§ 5. Extension et contraction des idéaux

Il s'agit d'étudier comment les idéaux se comportent par d'homomorphismes $f : A \rightarrow B$.

L'image $f(I)$ d'un idéal n'est pas toujours un idéal: considérer l'inclusion $\mathbb{Z} \subset \mathbb{Q}$. Il faut donc considérer :

5.1. Définition. L'extension de I dans B , I_B ou $B \cdot f(I)$ est l'idéal engendré par $f(I)$, c'est-à-dire l'ensemble des combinaisons B -linéaires finies $\sum_j b_j \cdot f(x_j)$, $b_j \in B$, $x_j \in I$.

Par contre, pour un idéal J de B l'ensemble $f^{-1}(J)$ est toujours un idéal de A . Si J est premier, $f^{-1}(J)$ reste premier. Les propriétés suivantes sont évidentes, mais énoncées pour référence :

5.2. Lemme. Pour I un idéal de A , J un idéal de B on a :

- $I \subset f^{-1}(I_B)$ et
- $J \supset (f^{-1}J)_B$.

Si \mathfrak{p} est premier dans A , $B \cdot f(\mathfrak{p})$ n'est pas forcément premier, même si f est un inclusion : considérer $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-5}]$. On a vu que l'idéal premier (2) de \mathbb{Z} ne reste pas premier dans $\mathbb{Z}[\sqrt{-5}]$.

§ 6. Complément géométrique : topologie de Zariski

Rappel : une **topologie** sur un ensemble X est donnée par les ensembles ouverts, ou de façon équivalente : par les ensembles fermés. Par définition, l'ensemble des fermés \mathcal{T} satisfait les propriétés suivantes :

- T1. $\emptyset, X \in \mathcal{T}$,
- T2. Si $G_1, \dots, G_k \in \mathcal{T}$, alors $\bigcup_{j=1}^k G_j \in \mathcal{T}$,
- T3. Si $G_\alpha \in \mathcal{T}$, alors $\bigcap_\alpha G_\alpha \in \mathcal{T}$.

On peut munir l'espace vectoriel k^n , k un corps, d'une topologie adaptée à la géométrie algébrique.

6.1. Définition. Un variété algébrique (ou affine) est le lieu de zéros commun d'un nombre fini de polynômes f_1, \dots, f_m :

$$V(f_1, \dots, f_m) = \{x = (x_1, \dots, x_n) \in k^n ; f_j(x) = 0, j = 1, \dots, m\}.$$

Un tel ensemble ne dépend que de l'idéal $I = (f_1, \dots, f_m)$ engendré par les f_j . On peut alors écrire $V(I)$ à la place de $V(f_1, \dots, f_m)$. Le célèbre théorème de base de Hilbert, à montrer plus tard (4.2.1) dit que chaque idéal de $k[x_1, \dots, x_n]$ est engendré par un nombre fini de polynômes et la définition suivante est donc équivalente :

Définition. Un **variété algébrique (ou affine)** est un ensemble de la forme

$$V(I) = \{x = (x_1, \dots, x_n) \in k^n ; f(x) = 0 \quad \forall f \in I\}$$

pour I un idéal de $k[X_1, \dots, X_n]$.

Les ensembles algébriques sont les fermés d'une topologie, la **topologie de Zariski**. On le montre directement grâce à :

6.2. Lemme. On a

- 1) $\bigcap_\alpha V(I_\alpha) = V(\sum_\alpha I_\alpha)$,
- 2) $V(I) \cup V(J) = V(I \cap J) = V(I \cdot J)$.

Démonstration.

1) $V(\sum_\alpha I_\alpha)$ est l'ensemble des zéros commun de toutes les combinaisons linéaires finis $\sum_\alpha f_\alpha$, en particulier on a $V(\sum_\alpha I_\alpha) \subset \bigcap_\alpha V(I_\alpha)$. L'autre inclusion est évidente.

2) Rappelons que $k[x_1, \dots, x_n]$ est un anneau factoriel. $I \cap J$ est engendré par les ppcm(f, g), $f \in I, g \in J$, tandis que $I \cdot J$ est engendré par les produits $f \cdot g, f \in I, g \in J$. Donc $V(I \cap J) = \{x \in k^n ; \text{pgcd}(f, g)(x) = 0, f \in I, g \in J\} = \{x \in k^n ; f(x) \cdot g(x) = 0, f \in I, g \in J\} = V(I \cdot J) = \{x \in k^n ; \text{soit } f(x) = 0, \text{ soit } g(x) = 0, f \in I, g \in J\} = V(I) \cup V(J)$. ■

§ 7. Corps de fractions d'un anneau intègre

Dans ce paragraphe A est un anneau intègre. Le but est de généraliser la construction du corps des fractions rationnelles.

On considère la relation d'équivalence pour les couples $(a, b) \in A \times A \setminus \{0\}$ donnée par

$$(a, b) \equiv (a', b') \iff ab' = ba'.$$

Il faut noter que la vérification de transitivité utilise que A est intègre. On note $\frac{a}{b}$ la classe d'équivalence de (a, b) . L'ensemble $Q(A)$ de ces classes a la structure d'un corps, **le corps de fractions de A** sous les opérations suivantes :

$$\begin{aligned} \frac{a}{b} \cdot \frac{c}{d} &= \frac{a \cdot c}{b \cdot d} \\ \frac{a}{b} + \frac{c}{d} &= \frac{a \cdot d + b \cdot c}{b \cdot d} \end{aligned}$$

Il y a une généralisation immédiate en remplaçant $A \setminus \{0\}$ par un ensemble S **multiplicativement stable** : $1 \in S$ et $a, b \in S \Rightarrow a \cdot b \in S$. Ici, il faut supposer de plus que $0 \notin S$ et on obtient **l'anneau des fractions de A par rapport à S** , un sous-anneau intègre de $Q(A)$:

$$S^{-1}A := \left\{ \frac{a}{s} ; a \in A, s \in S \right\} \subset Q(A).$$

Les fractions $\frac{s}{t}, s, t \in S$ deviennent inversibles dans $S^{-1}A$.

7.1. Exemples.

- 1) $S = A \setminus \{0\}$ est un ensemble multiplicativement stable et $S^{-1}A$ est le corps de fractions.
- 2) Pour \mathfrak{p} idéal premier de A , l'ensemble $S = A \setminus \mathfrak{p}$ est multiplicativement stable. L'anneau $S^{-1}A$ est appelé **la localisation de A en \mathfrak{p}** et sera noté $A_{\mathfrak{p}}$. C'est un anneau local avec idéal maximal $\mathfrak{p} \cdot A_{\mathfrak{p}}$. Cas spécial : $\mathfrak{p} = \{0\}$ donne $Q(A)$ (à noter : A intègre est équivalent à dire que $\{0\}$ est un idéal premier).
- 3) Pour $f \in A$, l'ensemble de puissances non-négatives est un ensemble multiplicativement stable. On dénote l'anneau des fractions correspondant par A_f .

Chapitre 2. Modules

§ 1. Notions de base

Soit A un anneau (commutatif avec 1). Un groupe abélien $(M, +)$ est un A -**module**, si $\forall a \in A, m \in M$ un produit $a \cdot m \in M$ est défini tel que :

- 1) Le produit est distributif :

$$\begin{aligned}\forall a \in A, x, y \in M, a \cdot (x + y) &= a \cdot x + a \cdot y \\ \forall a, b \in A, x \in M, (a + b) \cdot x &= a \cdot x + b \cdot x\end{aligned}$$

- 2) Le produit définit une action multiplicative :

$$\begin{aligned}(a \cdot b) \cdot x &= a \cdot (b \cdot x) \\ 1 \cdot x &= x.\end{aligned}$$

1.1. Exemples.

- 1) Un idéal I de A est un A -module.
- 2) Pour $A = k$, un corps, la notion de k -module est la même chose que celle de k -espace vectoriel.
- 3) Un $k[x]$ -module est la donnée d'un k -espace vectoriel avec une transformation linéaire.
- 4) Un groupe abélien est un \mathbb{Z} -module.

1.2. Définition. Une application $f : M \rightarrow N$ entre A -modules est une **application A -linéaire** ou **homomorphisme de A -modules** si

$$\begin{aligned}\forall x, y \in M, f(x + y) &= f(x) + f(y) \\ \forall a \in A, x \in M, f(a \cdot x) &= a \cdot f(x)\end{aligned}$$

1.3. Exemples.

- 1) Dans le cas d'un corps $A = k$, un corps, la définition ci-dessus est la même que celle donnée dans l'algèbre linéaire.
- 2) La composition de deux applications linéaires est une application linéaire.
- 3) L'ensemble $\text{Hom}_A(M, N)$ des applications A -linéaires $M \rightarrow N$ est lui-même un A -module pour les opérations suivantes :

1) Addition :

$$\forall f, g \in \text{Hom}_A(M, N), x \in M, (f + g)(x) = f(x) + g(x).$$

2) Action par A :

$$\forall a \in A, f \in \text{Hom}_A(M, N), x \in M, (a \cdot f)(x) = a \cdot f(x).$$

Dans le cas $M = N$, la composition de deux endomorphismes de M sert comme produit : on obtient un anneau (non-commutative, mais avec 1). On dit que $\text{End}_A(M) := \text{Hom}_A(M, M)$ est un **algèbre**, notion qu'on étudiera plus tard (§7). Si on fixe $\varphi \in \text{End}_A(M)$ le sous-anneau $A[\varphi]$ engendré par φ est commutatif. On l'utilisera pour l'astuce du déterminant.

4) Si $f : M \rightarrow N$ est injective, on dit que M est un **sous-module** de N . Le groupe quotient N/M hérite de l'action de A sur M la structure d'un A -module, le **module quotient**. Comme pour les anneaux et leurs idéaux on a :

L'image $\text{Im}(f)$ d'une application A -linéaire $f : M \rightarrow N$ est un sous-module de N , son noyau $\text{Ker}(f)$ est un sous-module de M . Le module $\text{Im}(f)$ est isomorphe à $M/\text{Ker}(f)$:

$$\begin{aligned} M/\text{Ker}(f) &\xrightarrow{\cong} \text{Im}(f) \\ x + \text{Ker}(f) &\mapsto f(x) \end{aligned}$$

§ 2. Sommes et produits

Pour une collection $M_i, i \in I$ de sous-modules de M , l'intersection $\bigcap_i M_i$ est un sous-module de M ainsi que leur somme

$$\sum_{i \in I} M_i = \{\text{sommes finies d'éléments dans } M_i\}.$$

Pour I un idéal on définit :

$$I \cdot M = \left\{ \sum_{i=1}^k a_i \cdot x_i ; a_i \in I, x_i \in M \right\}$$

qui est un sous-module de M .

Finalement, pour N, P deux A -modules le **transporteur** de P dans N est

$$(N : P) = \{a \in A ; a \cdot P \subset N\}$$

qui est un idéal de A . Cas spécial : $\text{Ann}(P) = (0 : P)$, l'**annulateur** de P .

2.1. Proposition.

1) Soient $L \supset M \supset N$ trois A -modules. Alors

$$(L/N)/(M/N) \cong L/M.$$

2) Soient M_1, M_2 deux sous-modules de M . Alors,

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

3) Soient M_1, M_2 deux sous-modules de M , alors,

$$\text{Ann}(M_1 + M_2) = \text{Ann}(M_1) \cap \text{Ann}(M_2).$$

Démonstration.

- 1) Puisque $N \subset M$, l'application A -linéaire $L/N \rightarrow L/M$ donnée par $x + N \mapsto x + M$ est bien définie. Elle est surjective avec noyau M/N et on peut appliquer l'exemple 1.3.4 ci-dessus.
- 2) La composition des applications naturelles

$$M_2 \subset M_1 + M_2 \rightarrow (M_1 + M_2)/M_1$$

est surjective avec noyau $M_1 \cap M_2$.

- 3) Soit $a \in \text{Ann}(M_1 + M_2)$. Donc $a \cdot m = 0$ quel que soit $m \in M_1, M_2$ ce qui implique $a \in \text{Ann}M_1 \cup \text{Ann}M_2$. Pour $a \in \text{Ann}M_1 \cup \text{Ann}M_2$ on a $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2 = 0$ et alors $a \in \text{Ann}(M_1 + M_2)$. ■

Maintenant on introduit **la somme directe** d'un nombre quelconque d' A -modules $M_i, i \in I$:

$$\bigoplus_{i \in I} M_i = \{(x_i), x_i \in M_i ; x_i = 0 \text{ sauf pour un nombre fini d'entre eux}\}$$

et le **produit direct**

$$\prod_{i \in I} M_i = \{(x_i) ; x_i \in M_i\}.$$

2.2. Exemples.

- 1) Soient I_1, \dots, I_m des idéaux quelconques d'un anneau A . La somme directe $I_1 \oplus \dots \oplus I_m$ est un A -module. Supposons que l'application qui envoie (x_1, \dots, x_m) vers $\sum_i x_i \in A$ est un isomorphisme

$$I_1 \oplus \dots \oplus I_m \cong A.$$

Dans ce cas les idéaux I_i sont deux à deux différents et $\sum I_i = A$ est une somme directe. Cela implique :

$$1 = e_1 + \dots + e_m, \quad e_i \in I_i, i = 1, \dots, m$$

et l'idéal I_i peut être considéré comme anneau avec $e_i \in I_i$ comme l'unité : de $a = 1 \cdot a = e_1 \cdot a + \dots + e_m \cdot a$ on tire que $\forall a \in I_i, e_i \cdot a = a$. Avec $J_i = \bigoplus_{j \neq i} I_j$ la composition $I_i \subset A \rightarrow A/J_i$ est un isomorphisme d'anneaux, d'où :

$$A \cong \prod_i A/J_i \quad \text{en tant qu'anneau.}$$

- 2) Un **A -module libre** est un A -module de la forme $\bigoplus_i M_i$ avec $\forall i, M_i \cong A$.
- 3) Un A -module M est **de type fini** si $\exists x_1, x_2, \dots, x_m \in M$ tels que $M = A \cdot x_1 + \dots + A \cdot x_m$. De façon équivalente : il y a une surjection $\bigoplus^m A \rightarrow M$.

§ 3. Lemme de Nakayama

Ce lemme est un des outils les plus utiles de l'algèbre commutative. Souvent on l'utilise sous la forme suivante

Soit (A, \mathfrak{m}) un anneau local et M un A -module de type fini tel que $\mathfrak{m} \cdot M = M$ alors $M = 0$.

D'abord on va montrer :

3.1. Propostion (l'astuce du déterminant). Soit M un A -module de type fini, I un idéal de A et $\varphi : M \rightarrow M$ une application A -linéaire telle que $\varphi(M) \subset I \cdot M$. Alors

$$\exists a_i \in I^i, i = 1, \dots, n, \text{ tels que } \varphi^n + a_1 \varphi^{n-1} + \dots + a_n$$

est zéro en tant qu'endomorphisme de M .

Démonstration. M étant de type fini, on écrit $M = A \cdot x_1 + \dots + A \cdot x_n$ et $\varphi(x_i) = \sum_j f_{ij} x_j$, $f_{ij} \in I$. Avec $B = \varphi \cdot \mathbb{1} - (f_{ij})$ cela s'écrit aussi $B\vec{x} = 0$, où \vec{x} est le vecteur colonne à coefficients x_j . On a :

$$(*) \quad B = (B_{ij}) = \begin{pmatrix} \varphi - f_{11} & -f_{12} & \cdots \\ -f_{21} & \varphi - f_{22} & \cdots \\ \vdots & \ddots & \vdots \\ \cdots & \cdots & \varphi - f_{nn} \end{pmatrix}$$

Les coefficients de B sont dans l'anneau commutatif $E = A[\varphi] \subset \text{End}_A(M)$ (voir l'exemple 2.1.3). On considère la matrice B^* des co-facteurs, c.à.d. la matrice à coefficients

$$B_{ij}^* = (-1)^{i+j} \det(B_{kl})_{1 \leq k, l \leq n, k \neq i, l \neq j}.$$

Comme dans l'algèbre linéaire on a

$${}^T B^* \circ B = \det B \cdot \mathbb{1}.$$

Donc $\det B \cdot \vec{x} = ({}^T B^* \circ B)\vec{x} = B^*(B(\vec{x})) = 0$ implique que $\det B$ annule les x_i et donc M tout entier. Utilisant (*) on trouve

$$\det B = \varphi^n + a_1 \varphi^{n-1} + \dots + a_n, \quad a_i \in I^i.$$

■

3.2. Corollaire. Soit I un idéal et M de type fini tel que $I \cdot M = M$. Alors $\exists x \in 1 + I$ tel que $x \cdot M = 0$.

Démonstration. Prenons $\varphi = \text{id}_M$ dans l'astuce du déterminant. Alors $x = 1 + a_1 + \dots + a_n \in 1 + I$ agit trivialement sur M . ■

3.3. Corollaire ("Lemme de Nakayama"). Soit I un idéal de A tel que $\forall x \in I, 1 + x$ est inversible de A . Alors si pour un A -module M de type fini on a $I \cdot M = M$, alors $M = 0$.

Démonstration. Si $I \cdot M = M$, alors $\exists x \in 1 + I$ tel que $x \cdot M = 0$. Un tel x étant inversible, il s'ensuit que $M = 0$. ■

Cas particuliers.

- 1) (A, \mathfrak{m}) anneau local et $I = \mathfrak{m}$,
- 2) A quelconque, mais $I \subset \bigcap_{\mathfrak{m} \text{ idéal maximal}} \mathfrak{m}$ (c.à.d. I est contenu dans le radical de Jacobson).

Démonstration.

- 1) On a vu (1.3.5) qu'un élément de la forme $1 + x$, $x \in \mathfrak{m}$ est inversible.
- 2) Plus généralement, on a vu que pour chaque élément x du radical de Jacobson (intersection des idéaux maximaux) l'élément $1 + x$ est inversible. ■

3.4. Corollaire. *Soit I un idéal de A tel que $\forall x \in I$, $1 + x$ est inversible dans A . Soit N un sous-module d'un A -module M de type fini tel que $M = I \cdot M + N$, alors $M = N$.*

Démonstration. Appliquer le corollaire précédent à M/N . ■

Soit (A, \mathfrak{m}) un anneau local et M un A -module de type fini. $M/(\mathfrak{m} \cdot M)$ est annihilé par les éléments de \mathfrak{m} et est donc un $k = A/(\mathfrak{m} \cdot A)$ -module, avec k le corps résiduel de A . C'est-à-dire $M/(\mathfrak{m} \cdot M)$ est un k -espace vectoriel.

3.5. Corollaire. *Dans la situation ci-dessus, soient $x_1, \dots, x_n \in M$ tels que leurs classes engendrent le k -espace vectoriel $M/\mathfrak{m} \cdot M$. Alors les x_i engendrent M .*

Démonstration. Soit N le sous-module de M engendré par les x_i . La composition

$$N \subset M \rightarrow M/\mathfrak{m} \cdot M$$

est une surjection (par hypothèse). Cela implique $N + \mathfrak{m} \cdot M = M$ et on applique le corollaire précédent. ■

§ 4. Suites exactes

Soit

$$M_\bullet = \{\dots \rightarrow M_{i-1} \xrightarrow{d_{i-1}} M_i \xrightarrow{d_i} M_{i+1} \rightarrow \dots\}$$

une suite d'applications A -linéaires. On dit que M_\bullet est un **complexe (de chaînes)** si $\forall i$, $d_i \circ d_{i-1} = 0$, c'est-à-dire $\text{Ker } d_i \supset \text{Im } d_{i-1}$. Si, pour un indice i , on a l'égalité $\text{Ker } d_i = \text{Im } d_{i-1}$, on dit que M_\bullet est **exacte** en M_i . Si M_\bullet est exacte en M_i quel que soit i , on dit que M_\bullet est exacte.

4.1. Exemples.

- 1) $0 \rightarrow N \xrightarrow{f} M$ est exacte veut dire que f est injective.
- 2) $N \xrightarrow{f} M \rightarrow 0$ est exacte veut dire que f est surjective.
- 3) $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ est exacte $\iff f$ est injective, g est surjective et g induit un isomorphisme $M/M' \cong M''$. Une telle suite est appelée une **suite exacte courte**.

Rappel : Pour une application A -linéaire $f : M \rightarrow N$, $\text{Coker } f = N/\text{Im}(f)$.

4.2. Lemme du serpent. Soit

$$\begin{array}{ccccccccc} 0 & \rightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \rightarrow & 0 \\ & & \downarrow \alpha' & & \downarrow \alpha & & \downarrow \alpha'' & & \\ 0 & \rightarrow & N' & \xrightarrow{f'} & N & \xrightarrow{g'} & N'' & \rightarrow & 0 \end{array}$$

un diagramme commutatif dont les lignes sont exactes. Alors il y a une suite exacte

$$0 \rightarrow \text{Ker } \alpha' \xrightarrow{\bar{f}} \text{Ker } \alpha \xrightarrow{\bar{g}} \text{Ker } \alpha'' \xrightarrow{\bar{d}} \text{Coker } \alpha' \xrightarrow{\bar{f}'} \text{Coker } \alpha \xrightarrow{\bar{g}'} \text{Coker } \alpha'' \rightarrow 0,$$

où \bar{f} , \bar{g} sont les restrictions de f , g et \bar{f}' , \bar{g}' sont induites par f' , g' .

Démonstration.

- 1) Il s'agit de voir que \bar{f} et \bar{g} sont bien-définis. Or, de $\alpha \circ f = f' \circ \alpha'$ il s'en suit que \bar{f} envoie $\text{Ker } \alpha'$ dans $\text{Ker } \alpha$. De façon analogue, \bar{g} envoie $\text{Ker } \alpha$ dans $\text{Ker } \alpha''$.
- 2) Puisque \bar{f} , \bar{g} sont les restrictions de f , g , pour l'exactitude de

$$0 \rightarrow \text{Ker } \alpha' \xrightarrow{\bar{f}} \text{Ker } \alpha \xrightarrow{\bar{g}} \text{Ker } \alpha''$$

il suffit de remarquer que si $g(x) = 0$ pour $x \in \text{Ker } \alpha$, alors $x = f(y)$, $y \in M'$ implique que $y \in \text{Ker } \alpha'$. C'est évident : $\alpha \circ f(y) = f' \circ \alpha'(y) = 0 \Rightarrow \alpha'(y) = 0$ car f' est injectif.

- 3) Il faut définir d . Le diagramme suivant montre comment le faire

$$\begin{array}{ccccccc} & & x & \longmapsto & z & & \\ & & M & \rightarrow & M'' & & \\ & & \downarrow & & \downarrow & & \vdots \\ N' & \rightarrow & N & \rightarrow & N' & & \\ & & y & \longmapsto & \alpha(x) & \longmapsto & 0 \end{array} .$$

Explication : Soit $z \in M''$ tel que $\alpha''(z) = 0$. Puisque g est surjectif, il existe $x \in M$ tel que $g(x) = z$. La commutativité du diagramme entraîne que $0 = \alpha'' \circ g(x) = g' \circ \alpha(x)$. Par l'exactitude de la deuxième ligne $\exists y \in N'$ tel que $f'(y) = \alpha(x)$. On pose $d(z) = y + \text{Im}(\alpha')$. Pour un autre choix de $x \in M$, disons $x' \in M$ on a, par l'exactitude de la première ligne : $x - x' \in \text{Im}(f)$, disons $x - x' = f(t)$. Alors par commutativité $f' \circ \alpha'(t) = \alpha \circ f(t) \Rightarrow f'(y + \alpha'(t)) = \alpha(x + f(t)) = \alpha(x')$ et donc $y + \text{Im}(\alpha') = y + \alpha'(t) + \text{Im}(\alpha')$.

- 4) $\text{Im } \bar{g} = \text{Ker } d$. Regarder le diagramme suivant :

$$\begin{array}{ccccccc} & & t & & f(t); x - f(t) & \longmapsto & z = g(x - f(t)) \\ & & \vdots & & \downarrow & & \vdots \\ & & M' & \rightarrow & M & \rightarrow & M'' \\ & & \downarrow & & \downarrow & & \vdots \\ & & N' & \rightarrow & N & & \\ & & y & \longmapsto & \alpha(x); 0 & \longmapsto & 0 \end{array} .$$

Explication : $y \in \text{Ker } d$ si et seulement si $\exists t \in M'$ tel que $\alpha'(t) = y \in \text{Ker } d$. Dans ce cas $z = g(x - f(t))$ avec $\alpha(x - f(t)) = 0$ et donc $z = \bar{g}(x - f(t))$. Inversement, si $z = g(x)$ avec $\alpha(x) = 0$, alors $y = 0$.

- 5) \bar{f}' et \bar{g}' sont bien définis. Laissez aux lecteurs.
- 6) $\text{Im } d = \text{Ker } \bar{f}'$. Ici l'argument est analogue à celle du point précédent et on l'omet.
- 7) $\text{Ker } \bar{g}' = \text{Im } \bar{f}'$. Or, $x' + \text{Im } \alpha \in \text{Ker } \bar{g}'$ si et seulement si $\exists z, g'(x') = \alpha''(z)$. Soit $x \in M$ tel que $g(x) = z$, alors $\alpha(x) - x' \in \text{Ker } g' = \text{Im } f'$, disons $\alpha(x) - x' = f'(y')$, c'est-à-dire $f'(y') = x' + \text{Im } \alpha$ et donc $x' + \text{Im } \alpha \in \text{Im } \bar{f}'$. Inversement, si $\alpha(x) - x' = f'(y')$, on a $g'(x') = g' \circ \alpha(x) = \alpha''(g(x))$ et $x' + \text{Im } \alpha \in \text{Ker } \bar{g}'$.
- 8) \bar{g}' est surjectif. Cela découle directement du fait que g' est surjectif. ■

§ 5. Produit tensoriel

5.1. Définition. Soient M, N, P trois A -modules.

- 1) Une application $f : M \times N \rightarrow P$ est **A -bilinéaire** si $\forall x \in M$ et $\forall y \in N$ les applications $x, x \mapsto f(x, -)$ et $y \mapsto f(-, y)$ sont A -linéaires.
- 2) Les applications bilinéaires de $M \times N$ dans P forment un A -module $\text{Bil}(M \times N, P)$.
- 3) Un **produit tensoriel** est un couple (T, g) avec T un A -module,

$$g : M \times N \rightarrow T$$

une application A -linéaire, telle que pour toute application A -bilinéaire $f : M \times N \rightarrow P$, il y a une unique application A -linéaire $f' : T \rightarrow P$ qui fait commuter le diagramme :

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & T \\ & \searrow f & \swarrow f' \\ & & P \end{array} .$$

Autrement dit

$$\forall P, \text{Bil}(M \times N, P) = \text{Hom}_A(T, P).$$

5.2. Proposition.

1. Un produit tensoriel existe et est unique dans le sens suivant : si (T', g') est un produit tensoriel, il existe un unique isomorphisme $\varphi : T \rightarrow T'$ tel que le diagramme suivant est commutatif :

$$\begin{array}{ccc} T & \xrightarrow{\varphi} & T' \\ & \swarrow g & \searrow g' \\ & & M \times N \end{array}$$

On l'appelle désormais le **produit tensoriel** $T = M \otimes N$ et on dénote $\forall x \in M, y \in N, g(x, y) = x \otimes y$.

2. Soit $\sum_i x_i \otimes y_i = 0$ dans $M \otimes N$. Il y a un A -module M' de type fini contenant les x_i et un A -module de type fini N' contenant les y_j tel que $\sum_i x_i \otimes y_i = 0$ dans $M' \otimes N'$

Démonstration.

- a. **Unicité.** Si on a un couple (T', g') comme dans la proposition, la définition du produit tensoriel appliquée à $g' : M \times N \rightarrow T'$ montre l'existence d'une application A -linéaire $\varphi : T \rightarrow T'$ telle que $\varphi \circ g' = g$. De même façon on a $\psi : T' \rightarrow T$ telle que $\psi \circ g = g'$. Par unicité $\varphi \circ \psi = \psi \circ \varphi = \mathbb{1}$ et ψ et φ sont donc des isomorphismes inverses.

b. Existence. Soit C le A -module libre engendré par $M \times N$:

$$C = \left\{ \sum_i a_i(x_i, y_i) ; a_i \in A, x_i \in M, y_i \in N \right\}$$

et soit D le sous-module engendré par les éléments de la forme $(x + x', y) - (x, y) - (x', y)$, $(x, y + y') - (x, y) - (x, y')$, $(ax, y) - a(x, y)$, $(x, ay) - a(x, y)$, où $x, x' \in M$, $y, y' \in N$ et $a \in A$. On pose $T = C/D$ et $x \otimes y = (x, y) + D$. Le module T est le plus grand quotient de C telle l'application "quotient" $g : C \rightarrow T = C/D$ devient A -bilinéaire. Le couple (T, g) convient comme on le vérifie immédiatement.

c. Supposons que $\sum_i x_i \otimes y_i = 0$ dans $M \otimes N$. Donc $z := \sum_i(x_i, y_i) \in D$. Soit $z = \sum_j \lambda_j(\xi_j, \eta_j)$ l'écriture de z en tant qu'élément de D et soit M' le sous-module de M engendré par les x_i et les ξ_j , N' le sous-module de N engendré par les y_i et les η_j . Alors, dans $M' \otimes N'$ on a aussi $z = 0$. ■

5.3. Exemples.

1. $M = A^m, N = A^n$. On a pour P un A -module quelconque : $\text{Bil}(A^m \times A^n, P) = \text{Hom}_A(A^{nm}, P)$ (une application bilinéaire $\varphi : A^m \times A^n \rightarrow P$ donne l'application linéaire $f_\varphi : A^{nm} \rightarrow P$ définie par $f_\varphi(a_{ij}) = \sum_{i,j} a_{ij}\varphi(e_i, e_j)$) donc $A^m \otimes A^n = A^{nm}$.
2. Si $(n, m) = 1$ on a $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$: si $xm + yn = 1$ on a $1(\bar{a} \otimes \bar{b}) = (xm + yn)(\bar{a} \otimes \bar{b}) = (xm\bar{a} \otimes \bar{b}) + (\bar{a} \otimes yn\bar{b}) = 0$.

5.4. Règles. On a des isomorphismes canoniques :

1. $M \otimes N \xrightarrow{\cong} N \otimes M$ (donné par $x \otimes y \mapsto y \otimes x$).
2. $(M \otimes N) \otimes P \xrightarrow{\cong} M \otimes (N \otimes P)$ (donné par $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$).
3. $(M \oplus N) \otimes P \xrightarrow{\cong} M \otimes P \oplus N \otimes P$ (donné par $(x + y) \otimes z \mapsto x \otimes z + y \otimes z$).
4. $A \otimes M \xrightarrow{\cong} M$ (donné par $a \otimes x \mapsto a \cdot x$).

Démonstration. Les preuves sont toutes de la même nature. Prouvons par exemple 3. L'application $(x + y)z \mapsto x \otimes z + y \otimes z$ induit l'application $f : (M \oplus N) \times P \rightarrow M \otimes P \oplus N \otimes P$ linéaire en $M \oplus N$ et P et donc f induit une application linéaire $g : (M \oplus N) \otimes P \rightarrow M \otimes P \oplus N \otimes P$. Une inverse est construite en partant de $xz + yz \mapsto (x + y) \otimes z$. ■

5.5. Remarque. De façon analogue, on peut introduire les produits multi-tensoriels $M_1 \otimes \dots \otimes M_r$ et on a par exemple $(M \otimes N) \otimes P \xrightarrow{\cong} M \otimes N \otimes P \xrightarrow{\cong} M \otimes (N \otimes P)$ qui étend le règle 5.4.(2) ci-dessus.

On aura besoin du lemme suivant :

5.6. Lemme. Soient A et B deux anneaux, M un A -module, P un B -module et N un (A, B) -bi-module (i.e. N est simultanément un A -module et un B -module et $\forall a \in A, b \in B, x \in N, a \cdot (x \cdot b) = (a \cdot x) \cdot b$). Alors $M \otimes_A N$ est un (A, B) -bi-module, $N \otimes_B P$ est un (A, B) -bi-module, et on a (en tant que (A, B) -bi-modules)

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Démonstration. Une structure de (A, B) -bi-module de $M \otimes_A N$ et de $N \otimes_B P$ est donnée par la règle évidente : pour $x \in M, y \in N, z \in P$ et $a \in A, b \in B$ on a $a \cdot (x \otimes y) \cdot b = ax \otimes yb$ et $a \cdot (y \otimes z) \cdot b = (ay \otimes zb)$. L'application $M \times N \times P \ni (x, y, z) \mapsto x \otimes (y \otimes z) \in M \otimes_A (N \otimes_B P)$ étant A -linéaire en M et N définit d'abord une application $(M \otimes_A N) \times P \rightarrow M \otimes_A (N \otimes_B P)$ et ensuite, puisqu'elle est B -linéaire en $M \otimes_A N$ et P , une application (A, B) -linéaire $(M \otimes_A N) \otimes_B P \rightarrow M \otimes_A (N \otimes_B P)$. L'inverse de cette application est trouvée en partant de l'application $M \times N \times P \ni (x, y, z) \mapsto x \otimes (y \otimes z) \in M \otimes_A (N \otimes_B P)$. ■

Finalement, il faut souvent changer d'anneau utilisant un homomorphisme d'anneaux $f : A \rightarrow B$. Un B -module N hérite de f la structure d'une A -module : $\forall a \in A, x \in N, a \cdot x = f(a) \cdot x$ (**restriction des scalaires**). En particulier B est un A -module et pour un A -module M quelconque on introduit l'**extension M_B des scalaires** de A à B :

$$M_B = B \otimes_A M.$$

Le module M_B est un B -module : $\forall b, b' \in B, x \in M \quad b \cdot (b' \otimes x) = (b \cdot b') \otimes x$. On montre facilement :

5.7. Lemme.

- 1) Supposons que N est de type fini sur B et B est de type fini sur A , alors N est de type fini sur A ,
- 2) Si M est de type fini sur A , alors M_B est de type fini sur B .

5.8. Exemple. Soit (A, \mathfrak{m}) un anneau local avec corps résiduel $k = A/\mathfrak{m}$. L'application naturelle $A \rightarrow k$ munit k d'une structure de A -module et pour chaque A -module M , l'extension des scalaires M_k donne le k -espace vectoriel $M_k = k \otimes_A M$.

§ 6. Produit tensoriel et suites exactes

Il s'agit d'étudier le comportement du produit tensoriel sous les suites exactes. D'abord, pour

$$f : M \rightarrow N, \quad g : P \rightarrow Q$$

deux applications A -linéaires, on introduit les applications

$$\begin{aligned} f \otimes g : M \otimes P &\rightarrow N \otimes Q \\ m \otimes p &\mapsto f(m) \otimes g(p) \end{aligned}$$

et

$$\begin{aligned} \text{Hom}(f, g) : \text{Hom}(N, P) &\rightarrow \text{Hom}(M, Q) \\ h &\mapsto g \circ h \circ f \end{aligned}$$

6.1. Lemme.

1. Soit

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$$

une suite de A -modules. Alors, pour Q un A -module quelconque, on a la suite induite

$$0 \rightarrow \text{Hom}(M'', Q) \xrightarrow{\text{Hom}(g, 1)} \text{Hom}(M, Q) \xrightarrow{\text{Hom}(f, 1)} \text{Hom}(M', Q).$$

Cette suite est exacte pour Q quelconque si et seulement la suite précédente est exacte.

2. Pour

$$0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

on a la suite induite

$$0 \rightarrow \text{Hom}(Q, M') \xrightarrow{\text{Hom}(1, f)} \text{Hom}(Q, M) \xrightarrow{\text{Hom}(1, g)} \text{Hom}(Q, M'').$$

Cette suite est exacte pour Q quelconque, si et seulement la suite précédente est exacte.

Démonstration. C'est une vérification complètement standard. ■

Si on veut considérer le comportement des suites exactes sous tensorisation, l'outil de traduction est le lemme suivant :

6.2. Lemme. Soient M, N, P trois A -modules. Il y a un isomorphisme

$$\text{Hom}_A(M \otimes_A N, P) \xrightarrow{\cong} \text{Hom}_A(M, \text{Hom}_A(N, P))$$

Démonstration. Soit $f : M \times N \rightarrow P$ une application A -bilinéaire. Elle induit une application A -linéaire $M \rightarrow \text{Hom}_A(N, P)$ donnée par $x \mapsto (y \mapsto f(x, y))$. La réciproque est aussi vraie : une application A -linéaire $g : M \rightarrow \text{Hom}_A(N, P)$ induit une application bilinéaire $M \times N \rightarrow P$ donnée par $(x, y) \mapsto g(x)(y)$. D'où une correspondance biunivoque entre $\text{Bil}_A(M \times N, P) = \text{Hom}_A(M \otimes_A N, P)$ et $\text{Hom}_A(M, \text{Hom}_A(N, P))$. ■

6.3. Corollaire. Soit

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$$

une suite exacte, alors pour n'importe quel A -module N la suite induite

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \rightarrow 0$$

est exacte.

Démonstration. Soit (1) la première suite exacte et soit P n'importe quel A -module. Alors par 2.6.1 $\text{Hom}((1), \text{Hom}(N, P))$ est exacte. Le lemme implique que $\text{Hom}((1) \otimes N, P)$ est exacte. De nouveau, par 2.6.1 on déduit que (1) $\otimes N$ est exacte. ■

6.4. Danger. Une application injective ne reste pas forcément injective après tensorisation. Par exemple multiplication par m est une injection $\mathbb{Z} \rightarrow \mathbb{Z}$, mais devient nulle après tensorisation avec $\mathbb{Z}/m\mathbb{Z}$.

6.5. Définition. On dit que N est A -**plat** si pour n'importe quelle application A -linéaire et injective $f : M' \rightarrow M$, l'application $f \otimes 1 : M' \otimes N \rightarrow M \otimes N$ est injective.

6.6. Proposition. Les énoncés suivants sont équivalents:

1. N est plat,
2. $\otimes N$ préserve les suites exactes courtes,
3. Pour n'importe quelle application A -linéaire injective $f : M' \rightarrow M$ entre A -modules de type fini $f \otimes 1 : M' \otimes N \rightarrow M \otimes N$ est injective.

Démonstration.

1. \Rightarrow 2. Appliquer le Corollaire précédent.

2. \Rightarrow 3. Clair.

3. \Rightarrow 1. Supposons que $f : M' \rightarrow M$ soit injective et soit $u = \sum_j x_j \otimes y_j \in M' \otimes N$ est dans le noyau de $f \otimes 1$, c.à.d. $f \otimes 1(u) = \sum_j f(x_j) \otimes y_j = 0$. Soit M'_0 le sous-module de M' engendré par les $x_j \in M'$, un module de type fini. On dénote $k : M'_0 \rightarrow M$ l'inclusion et donc $u_0 = \sum x_j \otimes y_j \in M'_0 \otimes N$ est tel que $k \otimes 1(u_0) = u$. Par 2.5.2 on peut trouver un sous-module M_0 de M de type fini contenant $f(M'_0)$ et tel que $\sum_j f(x_j) \otimes y_j = 0$ dans $M_0 \otimes N$. Si $f_0 = f|_{M'_0} \rightarrow M_0$, l'hypothèse 3. implique que $f_0 \otimes 1$ est injectif et donc $f_0 \otimes 1(u_0) = f \otimes 1(u) = 0$ entraîne que $u_0 = 0$ et donc $u = k \otimes 1(u_0) = 0$. \blacksquare

§ 7. Algèbres

Soient A et B anneaux. Un homomorphisme $f : A \rightarrow B$ munit B d'une structure de A -module : $\forall a \in A, b \in B \quad a \cdot b = f(a)b$. On dit que B est un **A -algèbre**. Si en particulier $A = k$ un corps et $B \neq 0$, f est injectif car $\ker f$ est un idéal de k et donc 0 car $f(1) = 1 \neq 0$ entraîne que $f \neq 0$. Une k -algèbre est donc un anneau contenant k comme sous-anneau, par exemple $A = k[X_1, \dots, X_n]$, l'anneau des polynômes à coefficients dans k .

Soient $f : A \rightarrow B$ et $g : A \rightarrow C$ deux homomorphismes d'anneaux. Donc B et C sont des A -algèbres. Un **homomorphisme d' A -algèbres** $h : B \rightarrow C$ est un homomorphisme d'anneaux qui est en même temps un A -homomorphisme. Donc $\forall a \in A, b \in B$ on a $h(f(a)b) = h(a \cdot b) = a \cdot h(b) = g(a)h(b)$. En particulier, en prenant $b = 1$ on a $h \circ f(a) = g(a)$. Inversement, pour un homomorphisme d'anneaux $h : B \rightarrow C$ tel que $h \circ f = g$ on a $h(f(a)b) = g(a)h(b)$.

Dans ce cas le produit tensoriel $D = B \otimes_A C$ existe en tant que A -module. Nous définissons une multiplication sur D comme suit. Il s'agit de montrer qu'il existe une application A -bilinéaire $\mu : D \times D \rightarrow D$ telle que $\mu(b \otimes c, b' \otimes c') = bb' \otimes cc'$. Or, l'application $B \times C \times B \times C \rightarrow D$ donnée par $(b, c, b', c') \mapsto bb' \otimes cc'$ étant A -linéaire dans chaque facteur, elle induit une application A -linéaire $(B \otimes C) \times (B \otimes C) \rightarrow D$. Le lecteur vérifiera que μ donne à D la structure d'un anneau commutatif avec unité 1×1 . Finalement c'est une A -algèbre car $a \mapsto f(a) \otimes 1 = 1 \otimes g(a)$ est un homomorphisme d'anneaux $A \rightarrow D$ comme on vérifie immédiatement. Conclusion : $D = B \otimes C$ est une A -algèbre.

On a aussi une propriété universelle. Pour l'énoncer introduisons les deux applications $u : B \rightarrow B \otimes C, b \mapsto b \otimes 1$ et $v : C \rightarrow B \otimes C, c \mapsto 1 \otimes c$. Considérons pour n'importe quelle A -algèbre D l'application

$$F : \text{Hom}(B, D) \times \text{Hom}(C, D) \rightarrow \text{Hom}(B \otimes_A C, D) \\ (h, k) \mapsto h \otimes k.$$

Ici Hom sont les homomorphismes de A -algèbres et $h \otimes k$ est l'application $b \otimes c \mapsto h(b)k(c)$, $b \in B, c \in C$. Cette application admet un inverse donné par $h \mapsto (h \circ u, h \circ v)$ et F est donc un bijection. Cette propriété caractérise le produit tensoriel :

$$\text{Hom}_{A\text{-alg}}(B, D) \times \text{Hom}_{A\text{-alg}}(C, D) = \text{Hom}_{A\text{-alg}}(B \otimes_A C, D).$$

7.1. Exemple. On peut utiliser la propriété universelle pour montrer que $A[T_1] \otimes_A A[T_2] = A[T_1, T_2]$.

On aura besoin aussi de quelques algèbres **non-commutatives**: l'algèbre des tenseurs et l'algèbre extérieure. Une A -algèbre non-commutative est un A -module qui est en même temps un anneau non-commutatif avec les compatibilités évidentes entre la multiplication et l'action par A .

7.2. Lemme. Soit M un A -module. On pose

$$T_A^0 M = A, \quad T_A^1 M = M, \quad T_A^n M = \underbrace{M \otimes \cdots \otimes M}_n.$$

L'algèbre tensorielle

$$T_A M = \bigoplus_{n=0}^{\infty} T_A^n M$$

est une algèbre (non-commutative) avec la multiplication $(x_1 \otimes \cdots \otimes x_n) \cdot (y_1 \otimes \cdots \otimes y_m) = x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_m$.

Elle a la propriété suivante :

$$\text{Hom}_{A\text{-alg}}(T_A M, B) = \text{Hom}_A(M, B) \quad B \text{ une } A\text{-algèbre non-commutative quelconque.}$$

(L'identification est donnée par la restriction à $M = T_A^1 M$).

7.3. Exemple. Soit $M = A^m$, un A -module libre. Soit $\{e_1, \dots, e_m\}$ la base canonique. Alors $\{e_{i_1} \otimes \cdots \otimes e_{i_r} ; 1 \leq i_1, \dots, i_r \leq m\}$ est une base de $T_A^r M$. Si $A = k$ on trouve $\dim_k T^r M = m^r$.

On dit que $x \in T_A^k M$ est de degré k . Cela rend TM une A -algèbre graduée : l'addition préserve T^k tandis que le produit d'un élément de degré k et d'un élément de degré l est d'un élément de degré $k + l$.

On peut fabriquer une A -algèbre commutative à partir de TM en divisant par l'idéal bi-latère I engendré par les éléments $x \otimes y - y \otimes x$, $x, y \in M$:

$$S_A M = T_A M / I, \quad \text{l'algèbre symétrique.}$$

$S_A M$ est aussi une algèbre graduée, la graduation provient de $T_A M$.

7.4. Exemple. Pour $M = k^m$, k un corps, on trouve que $SM \cong k[T_1, \dots, T_m]$: soit $\{e_1, \dots, e_m\}$ la base canonique, alors $T_j = e_j$ modulo l'idéal I et un monôme en les e_j de "degré" totale k (e.g. $e_{i_1} \otimes \cdots \otimes e_{i_k}$) correspond au même monôme en les T_j (donc $T_{i_1} \cdots T_{i_k}$).

En divisant par l'idéal bilatère J engendré par les éléments $x \otimes x$, $x \in M$ on obtient **l'algèbre extérieure** :

$$\Lambda_A M = T_A M / J = \bigoplus_{k=0}^{\infty} \Lambda_A^k M, \quad \Lambda_A^k M = T_A^k M / J.$$

C'est une algèbre graduée avec graduation provenant de celle de TM . La multiplication est "anti-commutative" . Pour expliquer cela, notons $x_1 \wedge \cdots \wedge x_k = x_1 \otimes \cdots \otimes x_k$ modulo J . Anti-commutativité veut dire que pour x de degré s et y de degré t on a $x \wedge y = (-1)^{ts} y \wedge x$.

7.5. Exemple. Pour $M = k^m$, $\{e_1, \dots, e_m\}$ la base canonique, une base de $\Lambda^k M$ est donnée par $\{e_{i_1} \wedge \cdots \wedge e_{i_k} ; 1 \leq i_1 < \dots < i_k\}$. En particulier $\dim \Lambda^k M = \binom{m}{k}$ et est donc nulle pour $k > m$.

On a les deux morphismes d' A -modules “symétrisation” et “anti-symétrisation” qui sont donnés par

$$\begin{aligned}
 s : T^k M &\rightarrow T^k M \\
 x_1 \otimes \cdots \otimes x_k &\mapsto \sum_{\pi \in \mathfrak{S}_n} x_{\pi(1)} \otimes \cdots \otimes x_{\pi(k)} \\
 a : T^k M &\rightarrow T^k M \\
 x_1 \otimes \cdots \otimes x_k &\mapsto \sum_{\pi \in \mathfrak{S}_n} \operatorname{sgn}(\pi) x_{\pi(1)} \otimes \cdots \otimes x_{\pi(k)}.
 \end{aligned}$$

Visiblement s factorise par $S^k M$ et a factorise par $\Lambda^k M$:

$$\begin{array}{ccc}
 T_A^k M & \xrightarrow{s} & T_A^k M & & T_A^k M & \xrightarrow{a} & T_A^k M \\
 \downarrow \text{proj} & & \downarrow \text{proj} & & \downarrow \text{proj} & & \downarrow \text{proj} \\
 S_A^k M & \xrightarrow{\cdot k!} & S_A^k M & & \Lambda_A^k M & \xrightarrow{\cdot k!} & \Lambda_A^k M
 \end{array}$$

et si $k!$ est inversible (par exemple si l'anneau A contient \mathbb{Q}) on peut diviser par $k!$ et l'image de s (resp. a) peut s'identifier avec $S_A^k M$ (resp. $\Lambda_A^k M$). Donc, dans ce cas, $S_A^k M$ et $\Lambda_A^k M$ se voient comme des sous-anneaux de $T_A^k M$ et si A contient \mathbb{Q} , on peut considérer $S_A M$ et $\Lambda_A M$ comme des sous-algèbres de $T_A M$.

Chapitre 3. Anneaux et modules de fractions

§ 1. Fractions : anneaux

On généralise ici la construction du Chap. 1§7 au cas que A est un anneau arbitraire. Soit A un anneau (commutatif avec 1) et $S \subset A$ un ensemble multiplicativement stable (donc $1 \in S$ et $a, b \in S$ implique $ab \in S$). On n'exclut pas la possibilité que $0 \in S$. On pose

$$S^{-1}A = A \times S / \sim, \quad \text{où } (a, s) \sim (a', s') \leftrightarrow \exists t \in S \quad t(as' - a's) = 0.$$

La classe d'équivalence de (a, s) sera notée a/s comme avant. Aussi, comme avant, les classes d'équivalence forment un anneau avec l'addition et multiplication usuelle des fractions. L'application

$$f : A \rightarrow S^{-1}A, \quad a \mapsto a/1$$

est un homomorphisme mais pas forcément injectif. Par exemple, si $0 \in S$, $S^{-1}A$ est l'anneau 0 et la réciproque est aussi vrai.

On a la propriété universelle suivante de $(S^{-1}A, f)$:

1.1. Proposition. *Soit $g : A \rightarrow B$ un homomorphisme d'anneaux tel que $g(s)$ est inversible dans B quel que soit $s \in S$. Alors il existe un unique homomorphisme $h : S^{-1}A \rightarrow B$ tel que $h \circ f = g$.*

Démonstration.

- Unicité. On a $h(a/1) = h(f(a)) = g(a)$, $\forall a \in A$ et donc $\forall s \in S$, $h(1/s) = h((s/1)^{-1}) = g(s)^{-1}$ et aussi $h(a/s) = h(a/1)h(1/s) = g(a)g(s)^{-1}$ ce qui détermine h complètement.
- Existence. On pose $h(a/s) = g(a)g(s)^{-1}$. C'est bien défini, car si $a/s = a'/s'$ alors $\exists t \in S$, $t(as' - a's) = 0$ et donc $g(t)[g(a)g(s') - g(a')g(s)] = 0$. Mais $g(t)$ est inversible et donc $g(a)g(s') - g(a')g(s) = 0 \Rightarrow g(a)g(s)^{-1} = g(a')g(s')^{-1}$. ■

Aussi, il y a une caractérisation du couple $(S^{-1}A, f)$:

1.2. Proposition. *Les propriétés suivantes caractérisent $(S^{-1}A, f)$:*

1. *Les éléments de $f(S)$ sont inversibles.*
2. *$f(a) = 0$ si et seulement si $\exists s \in S$, $as = 0$.*
3. *$S^{-1}A = \{f(a)f(s)^{-1} ; a \in A, s \in S\}$.*

Précisément : si $g : A \rightarrow B$ satisfait ces trois propriétés, alors il y a un unique isomorphisme $h : S^{-1}A \rightarrow B$ avec $g = hf$.

Démonstration. Les propriétés 1–3 sont claires. Inversement, si $g : A \rightarrow B$ les possède, alors on définit h par $h(a/s) = g(a)g(s)^{-1}$. Par 3. h est surjectif et l'injectivité utilise 2. : si $h(a/s) = 0 \Rightarrow \exists t \in S, ta = 0$ et donc $a/s = 0$. ■

Considérons maintenant le comportement des idéaux pour la formation de quotients. D'abord, si $I \subset A$ est un idéal, l'idéal engendré par I dans l'anneau $S^{-1}A$ est égal à $S^{-1}I$ car on peut toujours écrire :

$$\sum_{j=1}^n i_j/s_j = 1/(s_1 \cdots s_n) \cdot \text{élément de } I.$$

On a ensuite :

1.3. Proposition. *Soit $f : A \rightarrow S^{-1}A$ l'application naturelle, alors :*

1. *Chaque idéal de $S^{-1}A$ provient d'un idéal de A .*
2. *$I = f^{-1}i$, i idéal de $S^{-1}A$, si et seulement si aucun $s \in S$ est diviseur de zéro dans A/I .*
3. *Il y a une correspondance biunivoque entre les idéaux premiers de $S^{-1}A$ et les idéaux premiers de A disjoints de S .*

Démonstration.

1. Soit i un idéal de $S^{-1}A$ et soit $I = f^{-1}i$. Des règles généraux 1.5.2 disent

$$i \supset S^{-1}(f^{-1}i) = S^{-1}I.$$

D'autre part, si $x/s \in i$ alors $x/1 \in i$ et donc $x \in f^{-1}i = I$ et $x/s \in S^{-1}I$ et on a l'égalité.

2. On va montrer que $I = f^{-1}i$ si et seulement si

$$(*) \quad \forall s \in S, x \in A \quad \text{tel que } sx \in I, \text{ alors } x \in I.$$

L'assertion (*) revient à dire que aucun $s \in S$ est diviseur de zéro de A/I .

\Rightarrow Soient $s \in S, x \in A$ tels que $y = xs \in I = f^{-1}i$. Alors, $x/1 = y/s \in i$ et donc $x \in f^{-1}i = I$.

\Leftarrow On pose $i = S^{-1}I$. On regarde $f^{-1}i = f^{-1}S^{-1}I \supset I$ et il faut montrer l'inclusion inverse $f^{-1}i \subset I$. Soit donc $x \in A$ tel que $x/1 \in i = S^{-1}I \Rightarrow \exists y \in I, s \in S$ tel que $x/1 = y/s$ et donc $\exists s' \in S$ tel que $0 = s'(xs - y) = s'sx - s'y \Rightarrow s'sx \in I$ et (*) implique que $x \in I$.

3. Si \mathfrak{q} est un idéal premier de $S^{-1}A$ alors $\mathfrak{p} = f^{-1}\mathfrak{q}$ est premier. D'autre part, si \mathfrak{p} est un idéal premier de A , alors A/\mathfrak{p} est sans diviseurs de zéro et donc $\mathfrak{p} = f^{-1}\mathfrak{q}$ par 2. Soit $T \subset A/\mathfrak{p}$ l'image de S dans A/\mathfrak{p} . Alors $S^{-1}A/S^{-1}\mathfrak{p} \cong T^{-1}(A/\mathfrak{p})$ est soit 0, soit contenu dans le corps de fractions de A/\mathfrak{p} et donc sans diviseurs de zéro : on a $0 \in T$ si et seulement si $T^{-1}(A/\mathfrak{p}) = 0$ si et seulement si $S^{-1}\mathfrak{p} = (1)$ si et seulement si $\mathfrak{p} \cap S \neq \emptyset$ comme on le voit facilement. Il s'ensuit que si \mathfrak{p} est premier d'un part $\mathfrak{q} = S^{-1}\mathfrak{p}$ ne peut pas être 0 et donc \mathfrak{q} est premier. D'autre part, \mathfrak{q} et $S^{-1}\mathfrak{q}$ étant premier, $S^{-1}A/S^{-1}\mathfrak{q} \neq 0$ et donc $\mathfrak{p} \cap S = \emptyset$. ■

1.4. Corollaire. *Les idéaux premiers de $A_{\mathfrak{p}}$ sont en correspondance biunivoque avec les idéaux premiers de A contenus dans \mathfrak{p} .*

Comparons cela avec le procédé de passage à l'anneau quotient A/\mathfrak{p} : il y a une correspondance biunivoque entre les idéaux de A/\mathfrak{p} et ceux de A qui contiennent \mathfrak{p} . Donc, si on ne considère que des idéaux premiers de A contenus dans un idéal premier \mathfrak{q} et qui contiennent un autre idéal premier $\mathfrak{p} \subset \mathfrak{q}$ il faut passer à $A_{\mathfrak{q}}/\mathfrak{p}A_{\mathfrak{q}} \cong (A/\mathfrak{p})_{\mathfrak{q}'}$ où \mathfrak{q}' est l'idéal $\mathfrak{q} \cdot (A/\mathfrak{p})$. Pour l'isomorphisme ("passage aux quotients commute au passage aux fractions") voir le paragraphe ci-dessous). Le cas spécial $\mathfrak{p} = \mathfrak{q}$ est particulièrement intéressant : $B = A/\mathfrak{p}$ est un anneau intègre avec corps de fractions $k = Q(B)$ qui lui-même est isomorphe au corps résiduel de l'anneau local $A_{\mathfrak{p}}$:

$$\begin{array}{ccc} A & \longrightarrow & A_{\mathfrak{p}} \\ \downarrow & & \downarrow \\ B = A/\mathfrak{p} & \longrightarrow & k = Q(B) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}. \end{array}$$

La démonstration du critère suivant utilise la technique de localisation bien que l'énoncé elle-même n'a rien à voir avec la localisation.

1.5. Critère. Soit $g : A \rightarrow B$ un homomorphisme d'anneaux et soit \mathfrak{p} un idéal premier de A . Alors il existe un idéal premier \mathfrak{q} de B tel que $\mathfrak{p} = g^{-1}\mathfrak{q}$ si et seulement si $\mathfrak{p} = g^{-1}(g(\mathfrak{p})B)$.

Démonstration.

\Rightarrow On a $g(\mathfrak{p})B = g(g^{-1}\mathfrak{q})B \supset \mathfrak{q}$ et donc, en utilisant de nouveau les règles générales d'inclusions 1.5.2 on trouve $\mathfrak{p} \supset g^{-1}(g(\mathfrak{p})B) \supset g^{-1}\mathfrak{q} = \mathfrak{p}$.

\Leftarrow On pose $S = g(A \setminus \mathfrak{p})$. L'idéal $\mathfrak{q}' = g(\mathfrak{p})B$ a la propriété que $\mathfrak{p} = g^{-1}\mathfrak{q}'$ donc \mathfrak{q}' est disjoint de S , engendre un idéal propre dans $S^{-1}B$ qui doit être contenu dans un idéal maximal \mathfrak{m} de $S^{-1}B$. Soit \mathfrak{q} l'idéal de B correspondant. Alors \mathfrak{q} est premier et contient l'idéal \mathfrak{q}' par construction. Donc $g^{-1}\mathfrak{q}$ contient $g^{-1}\mathfrak{q}' = \mathfrak{p}$. D'autre part $\mathfrak{q} \cap S = \emptyset$ et donc $g^{-1}\mathfrak{q}$ est contenu dans \mathfrak{p} par définition de S . Combinant cela avec l'autre inclusion on trouve bien l'égalité $\mathfrak{p} = g^{-1}\mathfrak{q}$. ■

Ensuite donnons les réglés suivants sans donner les démonstrations (faciles, bien sûr) :

1.6. Règles. Pour deux idéaux quelconques I, J de A on a

1. $S^{-1}(I + J) = S^{-1}I + S^{-1}J$,
2. $S^{-1}(I \cdot J) = S^{-1}I \cdot S^{-1}J$,
3. $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$,
4. $S^{-1}(\sqrt{I}) = \sqrt{S^{-1}I}$.

§ 2. Fractions : modules

Pour M un A -module et S un système multiplicativement stable de A on peut recopier la définition $S^{-1}A$. On trouve que $S^{-1}M$ est un $S^{-1}A$ -module sous l'action naturelle :

$$(a/s) \cdot (m/s') = (am/ss').$$

On peut aussi passer aux fractions au niveau des homomorphismes : si $u : M \rightarrow N$ est un A -homomorphisme, alors $m/s \mapsto u(m)/s$ définit un homomorphisme $S^{-1}u : S^{-1}M \rightarrow S^{-1}N$ qui est $S^{-1}A$ -linéaire. De plus, si $v : N \rightarrow P$ est A -linéaire on a $S^{-1}(v \circ u) = S^{-1}v \circ S^{-1}u$.

2.1. Proposition. *L'opération S^{-1} transforme une suite exacte en une suite exacte. Par conséquent S^{-1} transforme sous-modules en sous-modules et modules quotients en modules quotients : si $N \subset M$, alors $S^{-1}N \subset S^{-1}M$ et $S^{-1}(M/N) = S^{-1}M/S^{-1}N$.*

Démonstration. Soit $M' \xrightarrow{f} M \xrightarrow{g} M''$ une suite exacte.

1. De $g \circ f = 0$ on tire $S^{-1}g \circ S^{-1}f = 0$ et donc $\ker(S^{-1}g) \supset \operatorname{im}(S^{-1}f)$.
2. Soit $m/s \in \operatorname{Ker}(S^{-1}g)$. Alors $g(m)/s = 0 \Rightarrow \exists s' \in S, 0 = s'g(m) = g(s'm)$ et donc $\exists m' \in M'$ tel que $f(m') = s'm$ et donc $m/s = f(m')/(s's) = (S^{-1}f)(m')/(ss')$ et donc $\operatorname{Ker}(S^{-1}g) \subset \operatorname{Im}(S^{-1}f)$. ■

2.2. Proposition. *Il y a un unique isomorphisme $f : S^{-1}A \otimes_A M \xrightarrow{\cong} S^{-1}M$ de $S^{-1}A$ -modules. tel que $\forall s \in S, a \in A, m \in M, f((a/s) \otimes m) = (am)/s$.*

Démonstration. L'application $(a/s, m) \mapsto (am)/s$ est un homomorphisme A -bilinéaire $S^{-1}A \times M \rightarrow S^{-1}M$ et donc il y a un unique homomorphisme f avec la propriété souhaitée. Cet homomorphisme est clairement $S^{-1}A$ -linéaire et surjectif. Pour l'injectivité remarquons d'abord que $S^{-1}A \otimes_A M$ consiste en les éléments de la forme $1/s \otimes m$ avec $s \in S, m \in M$: une combinaison linéaire $\sum_{j=1}^n (a_j/s_j) \otimes m_j$ s'écrit $\sum_{j=1}^n (1/t)s_1 \cdots \widehat{s}_j \cdots s_n \otimes a_j m$ avec $t = s_1 \cdots s_n$ et donc équivaut $(1/t)$ fois un élément de M . Maintenant l'injectivité est clair : si $f(\frac{1}{s} \otimes m) = \frac{m}{s} = 0$ alors $\exists s' \in S, s'm = 0$ et donc $\frac{1}{s} \otimes m = \frac{1}{s's} \otimes (s'm) = 0$. ■

2.3. Corollaire. *$S^{-1}A$ est A -plat.*

2.4. Proposition. *Soient M et N deux A -modules. Il y a un isomorphisme unique $f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \xrightarrow{\cong} S^{-1}(M \otimes_A N)$ tel que $\forall s, t \in S, m \in M, n \in N, f(m/s \otimes n/t) = (1/st)(m \otimes n)$.*

En particulier pour un idéal premier \mathfrak{p} de A quelconque on a un isomorphisme "canonique" $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \cong (M \otimes_A N)_{\mathfrak{p}}$

Démonstration. $S^{-1}M \otimes_{S^{-1}A} S^{-1}N = (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} S^{-1}N$ est un $(A, S^{-1}A)$ -bi-module et donc par 2.5.6 ce module équivaut

$$\begin{aligned} M \otimes_A (S^{-1}A \otimes_{S^{-1}A} S^{-1}N) &\cong M \otimes_A S^{-1}N \\ &\cong M \otimes_A (S^{-1}A \otimes_A N) \cong (M \otimes_A N) \otimes_A S^{-1}A \cong S^{-1}(M \otimes_A N). \end{aligned}$$

On vérifie que l'isomorphisme f obtenue en composant tous les isomorphismes ci-dessus satisfait la règle souhaitée. ■

§ 3. Principe local-global

On dit que une propriété (P) est une **propriété locale** si (P) est vraie pour un A -module M si et seulement elle est vraie pour tous les localisations $M_{\mathfrak{p}}$. $M = 0$ est une propriété locale, précisément :

3.1. Lemme. *Les propriétés suivantes sont équivalentes :*

1. $M = 0$,
2. $M_{\mathfrak{p}} = 0$ pour n'importe quel idéal premier \mathfrak{p} de A ,
3. $M_{\mathfrak{m}} = 0$ pour n'importe quel idéal maximal \mathfrak{m} de A .

Démonstration. Seulement l'implication $3 \Rightarrow 1$ nécessite une preuve. On suppose que $M_{\mathfrak{m}} = 0$ pour n'importe quel idéal maximal \mathfrak{m} de A . On suppose aussi que $M \neq 0$ et que $I = \text{Ann}(x)$, $x \neq 0$, $x \in M$. C'est un idéal propre de A et il est donc contenu dans un idéal maximal \mathfrak{m} . Puisque $M_{\mathfrak{m}} = 0$, dans $M_{\mathfrak{m}}$ on a $x/1 = 0$, c.à.d. $\exists a \in A \setminus \mathfrak{m}$ tel que $ax = 0$. C'est une contradiction, car $\text{Ann}(x) = I \subset \mathfrak{m}$. ■

3.2. Lemme. Soit $f : M \rightarrow N$ un homomorphisme de A -modules. Alors les énoncés suivantes sont équivalentes :

1. f est injectif,
2. $f_{\mathfrak{p}}$ est injectif pour n'importe quel idéal premier \mathfrak{p} de A ,
3. $f_{\mathfrak{m}}$ est injectif pour n'importe quel idéal maximal \mathfrak{m} de A .

On peut remplacer le mot "injectif" par "surjectif" ou "isomorphe" dans cet énoncé.

Démonstration. Par 3.2.1 on sait que localiser préserve les suites exactes et donc $\ker(f_{\mathfrak{p}}) = (\ker f)_{\mathfrak{p}}$ et il suffit d'appliquer le lemme précédent. ■

La platitude est aussi une propriété locale :

3.3. Lemme. soit M un A -module, alors les énoncés suivantes sont équivalentes :

1. M est plat,
2. $M_{\mathfrak{p}}$ est plat pour n'importe quel idéal premier \mathfrak{p} de A ,
3. $M_{\mathfrak{m}}$ est plat pour n'importe quel idéal maximal \mathfrak{m} de A .

Démonstration.

$1 \Rightarrow 2$. On a plus généralement que si $f : A \rightarrow B$ est un homomorphisme d'anneaux, alors si M est A -plat, $M_B = M \otimes_A B$ est B -plat. Pour le montrer, supposons que $i : N_1 \rightarrow N_2$ est une injection de B -modules. Platitude de M dit que $i \otimes 1 : N_1 \otimes_A M \rightarrow N_2 \otimes_A M$ est injective. On a pour $i = 1, 2 : N_i \otimes_A M \xrightarrow{\cong} M \otimes_A N_i \xrightarrow{\cong} M \otimes_A (N_i \otimes_B B) \xrightarrow{\cong} M \otimes_A (B \otimes_B N_i)$ et en appliquant le lemme 2.5.6 ce module est isomorphe à $(M \otimes_A B) \otimes_B N_i \xrightarrow{\cong} M_B \otimes_B N_i \xrightarrow{\cong} N_i \otimes_B M_B$. On conclut que $i \otimes 1 : N_1 \otimes_B M_B \rightarrow N_2 \otimes_B M_B$ est injective.

$2 \Rightarrow 3$. Clair.

$3 \Rightarrow 1$ Soit $i : N_1 \rightarrow N_2$ une injection de A -modules. alors $i_{\mathfrak{m}} : (N_1)_{\mathfrak{m}} \rightarrow (N_2)_{\mathfrak{m}}$ est injective et si $M_{\mathfrak{m}}$ est plat, l'application $(i \otimes 1)_{\mathfrak{m}} : (N_1 \otimes M)_{\mathfrak{m}} = (N_1)_{\mathfrak{m}} \otimes M_{\mathfrak{m}} \rightarrow (N_2)_{\mathfrak{m}} \otimes M_{\mathfrak{m}}$ est injective et donc, par le Lemme 3.3.2 $i \otimes 1 : N_1 \otimes M \rightarrow N_2 \otimes M$ est injective. ■

§ 4. Spectre d'un anneau, support d'un module

Le **spectre** $\text{Spec}A$ d'un anneau A est l'ensemble de ses idéaux premiers. Sur $\text{Spec}A$ on définit une topologie en déclarant que les fermés $\hat{V}(E)$, $E \subset A$ quelconque sont :

$$\hat{V}(E) = \{\mathfrak{p} \text{ premier} \subset A ; \mathfrak{p} \supset E\}.$$

On note que si I est l'idéal de A engendré par E , alors $\hat{V}(E) = \hat{V}(I)$ et il suffit donc de considérer les idéaux.

4.1. Proposition.

on a

1. $\hat{V}(0) = \text{Spec}A, \hat{V}((1)) = \emptyset,$
2. $\hat{V}(\bigcup_{i \in I} E_i) = \bigcap_{i \in I} \hat{V}(E_i),$
3. $\hat{V}(I \cap J) = \hat{V}(I \cdot J) = \hat{V}(I) \cup \hat{V}(J), I, J$ idéaux.
4. $\hat{V}(I) = \hat{V}(\sqrt{I}).$

Démonstration. Les énoncés 1. et 2. sont clairs. Pour 3. on note que si \mathfrak{p} est un idéal premier contenant $I \cdot J$, alors par lemme 1.4.5 soit \mathfrak{p} contient I , soit J . Finalement 4. est une traduction du lemme 1.4.4. ■

Par conséquent, les $\hat{V}(I), I$ idéal de A définissent une topologie, la **topologie de Zariski**.

Pour mieux comprendre cette topologie, notons les points de $\text{Spec}A$ par x, y, \dots et leurs idéaux correspondants par $\mathfrak{p}_x, \mathfrak{p}_y, \dots$. La clôture $\overline{\{x\}}$ d'un point $x \in \text{Spec}A$ est l'intersection des fermés contenant x , c.à.d. l'intersection des $\hat{V}(I)$ tels que $x \in \hat{V}(I)$, i.e. $I \subset \mathfrak{p}_x$. on a donc $\overline{\{x\}} = \{x\}$ si et seulement si \mathfrak{p}_x est maximal.

Aussi, $\mathfrak{p}_y \supset \mathfrak{p}_x$ entraîne que y est dans la clôture de x et vice-versa.

Si A est intègre, 0 est premier et sa clôture est $x = \text{Spec}A$. On dit que 0 est le **point générique** de x .

4.2. Exemples.

1. Soit k un corps. $\text{Spec}k = \{0\}$, un seul point fermé.
2. Le spectre de \mathbb{Z} consiste en les nombres premiers (les points fermés) et 0, le point générique de \mathbb{Z} .
3. Soit k un corps algébriquement clos. Alors $\text{Spec}k[x]$ consiste en les idéaux maximaux $(x - a), a \in k$ et le point générique.

Soit M un A -module. On pose

4.3. Définition. Le **support** de M est l'ensemble $\{\mathfrak{p} \in \text{Spec}A ; M_{\mathfrak{p}} \neq 0\}$.

4.4. Proposition.

1. $M \neq 0$ si et seulement si $\text{Supp}M \neq \emptyset,$
2. $\text{Supp}(A/I) = \{\mathfrak{p} \in \text{Spec}A ; \mathfrak{p} \supset I\} = \hat{V}(I).$
3. Soit $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ une suite exacte de A -modules, alors $\text{Supp}M = \text{Supp}M' \cup \text{Supp}M'',$
4. $\text{Supp}(\sum_j M_j) = \bigcup_j \text{Supp}M_j,$
5. Soit M de type fini. Alors $\text{Supp}M = \hat{V}(\text{Ann}M),$

Démonstration.

1. \implies : On utilise le Lemme 3.1.

\impliedby : Soit $M_{\mathfrak{p}} \neq 0$, alors $M \neq 0$.

2. On a $A_{\mathfrak{p}} \neq 0$ et donc $\text{Supp}A = \{\mathfrak{p} \text{ premier} \subset A\}$. Cela implique 2.

3. La localisation préserve les suites exactes (3.2.1).

4. Laissé au lecteur.

5. Soit $M = x_1A + \cdots + x_nA$. Par 4), $\text{Supp}M = \bigcup_i \text{Supp}(x_iA)$. On a $x_iA = A/I_i$ où $I_i = \text{Ann}x_i$. Par 2) $\text{Supp}(x_iA) = \{\mathfrak{p} \in \text{Spec}A ; \mathfrak{p} \supset I_i\}$. Alors $\text{Supp}M$ consiste en les idéaux premiers qui contiennent au moins un des I_i et donc $\bigcap_i I_i$. Pour l'inclusion opposée, le lemme 1.4.5 dit que si \mathfrak{p} contient l'intersection $I_1 \cap \cdots \cap I_n = \text{Ann}(M)$, \mathfrak{p} contient un des I_i . Cela montre 5. ■

Chapitre 4. Anneaux et modules noëthériens et artiniens

§ 1. Conditions de chaîne : anneaux

1.1. Définition. Soit Σ un ensemble partiellement ordonné par \leq . On dit que Σ possède la **condition de chaîne croissante** (ccc), **resp. décroissante** (cdc) si chaque chaîne croissante $s_1 \leq s_2 \leq \dots$, resp. décroissante $\dots \leq s_2 \leq s_1$, avec $s_i \in \Sigma$, se stabilise, c.à.d. $s_n = s_N, \forall n \geq N$.

Remarque. On vérifie sans peine que Σ possède la ccc si et seulement si chaque sous-ensemble non-vide de Σ admet un élément maximal.

Le lemme suivante est facile à montrer :

1.2. Lemme. Soit A un anneau commutatif avec 1 ordonné par l'inclusion. Les énoncés suivants sont équivalents:

1. L'ensemble des idéaux possède la ccc,
2. Un ensemble non-vide d'idéaux admet un élément maximal.
3. Les idéaux sont engendrés par un nombre fini d'éléments.

1.3. Définition. Un **anneau noëthérien** est un anneau vérifiant une des trois propriétés ci-dessus.

1.4. Exemples.

1. Un corps est noëthérien.
2. Un anneau principal est noëthérien.
3. $k[X_1, X_2, \dots]$ (nombre infini de variables) n'est pas noëthérien.
4. Si A est noëthérien, alors $S^{-1}A$ l'est.

1.5. Définition. Un anneau vérifiant la condition cdc pour les idéaux est un **anneau artinien**.

1.6. Exemples. Un corps k est artinien, un anneau de la forme $k[X]/(X^m)$, k un corps, est artinien. \mathbb{Z} n'est pas artinien.

§ 2. Théorème de base de Hilbert

Voici l'énoncé de ce théorème :

2.1. Théorème. *Si A est noethérien, alors $A[X]$ l'est aussi.*

Démonstration. On propose de montrer que chaque idéal de I est engendré par un nombre fini d'éléments. On introduit :

$$J_n = \{a \in A ; f \in I, \quad f = aX^n + \text{termes de degré} < n\}.$$

On vérifie facilement que J_n est un idéal de A et que $J_1 \subset J_2 \subset \dots$. Puisque A est noethérien, cette chaîne se stabilise, disons $J_n = J_{n+1} = \dots$. Supposons que J_k soit engendré par $a_{k,1}, \dots, a_{k,r_k}$, $k = 1, \dots, n$. Soient $f_{k,j} = a_{k,j}X^k + \dots$ les polynômes correspondants. Je prétends que les $f_{k,j}$ engendrent I . Or, soit $f \in I$ et soit $\deg f = m$ avec a le coefficient de X^m . Si $m \geq n$, alors $a \in J_n$ et $a = \sum_i b_i a_{n,i}$. La différence $f - (\sum_i b_i f_{n,i})X^{m-n}$ est de degré $< m$ et on conclut par récurrence. Si $m < n$, $a \in J_m$ et $a = \sum_i b_i a_{m,i}$ et maintenant $f - \sum_i b_i f_{m,i}$ a le degré $< m$ et on conclut aussi par récurrence. ■

2.2. Corollaire. *Chaque algèbre de type fini sur un corps est noethérienne. Cas particulier : soit $V \subset k^n$ une variété affine et $k[V] := k[X_1, \dots, X_n]/I(V)$, l'anneau de V est noethérien.*

Si k est algébriquement clos, on verra plus tard (le théorème des zéros de Hilbert 6.4.5) que les variétés affines sont en correspondance biunivoque avec les idéaux de $k[X_1, \dots, X_n]$ mais les inclusions sont renversés. Puisque $k[X_1, \dots, X_n]$ est noethérien, l'ensemble des variétés affines de k^n possède donc la cdc et chaque collection non-vide de telles variétés admet un élément minimal. On utilise cette remarque pour montrer :

2.3. Lemme. *Chaque variété affine admet une décomposition $X = X_1 \cup \dots \cup X_r$ avec X_i irréductible, c.à.d. si $X_i = Y \cup Z$, avec Y, Z variétés affines, alors, soit $X_i = Y$, soit $X_i = Z$.*

Démonstration. Soit Σ l'ensemble des variétés affines de k^n qui ne se décomposent pas en variétés irréductibles. Si $\Sigma \neq \emptyset$ alors il y a un élément minimal $X_0 \in \Sigma$. Cet élément ne peut pas être irréductible, car $X_0 \in \Sigma$, donc $X_0 = Y \cup Z$. Puisque X_0 est minimal $Y, Z \notin \Sigma$ et Y et Z admettent donc une décomposition en variétés irréductibles et donc aussi X_0 . Cette contradiction montre bien que $\Sigma = \emptyset$. ■

2.4. Remarque. On peut montrer que cette décomposition est essentiellement unique, c.à.d si on normalise la décomposition de telle sorte que $\forall i \neq j, X_i \not\subset X_j$, alors la décomposition est unique à numérotation près.

§ 3. Conditions de chaîne : modules

3.1. Définition. Soit M un A -module. On dit que M est **noethérien** si l'ensemble des sous-modules de M possède la ccc.

Puisque A est un A -module avec pour sous-modules les idéaux, cette définition étend celle des anneaux.

On vérifie sans peine :

3.2. Lemme. *Soit*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

une suite exacte de A -modules. Alors M est noethérien si et seulement si M' et M'' le sont.

3.3. Corollaire.

1. Une somme directe d'un nombre fini de modules noëthériens est noëthérien.
2. Si A est noëthérien et I un idéal de A , alors A/I est noëthérien.
3. Soit A un anneau noëthérien. Un A -module est noëthérien si et seulement si il est de type fini. Dans ce cas chaque sous-module est de type fini.
4. Soit A un anneau noëthérien, $f : A \rightarrow B$ un homomorphisme d'anneaux telle que B est un A -module de type fini sur A , alors B est noëthérien.

Démonstration.

1. Se déduit du Lemme précédent par récurrence :

$$0 \rightarrow M_n \rightarrow \bigoplus_{i=1}^n M_i \rightarrow \bigoplus_{i=1}^{n-1} M_i \rightarrow 0.$$

2. On a la suite exacte $0 \rightarrow I \rightarrow A \rightarrow A/I \rightarrow 0$.
3. Si M est un A -module noëthérien, une chaîne

$$Ax_1 \subset Ax_1 + Ax_2 \subset \dots, \quad x_1 \in M, x_2 \in M \setminus Ax_1, \dots$$

doit se stabiliser pour $n = N$ et donc M est engendré par x_1, \dots, x_N . Le même argument montre que tout sous-module est engendré par un nombre fini d'éléments. Pour la réciproque, si M est de type fini $M = Ax_1 + Ax_2 + \dots + Ax_N$, il y a une suite exacte évidente

$$0 \rightarrow ? \rightarrow A^N \rightarrow M \rightarrow 0$$

avec A^N noëthérien par 1. et M est donc noëthérien.

4. C'est un cas particulier de 3. ■

3.4. Définition. On dit que M est **de présentation finie** s'il y a une suite exacte

$$A^s \xrightarrow{f} A^r \xrightarrow{g} M \rightarrow 0.$$

cela veut dire que M est de type fini et que les relations entre les générateurs $\{g(e_i)\}, i = 1, \dots, r$ sont conséquences d'un nombre fini d'entre elles : $\{f(e_j)\}, j = 1, \dots, s$.

Si A est noëthérien, un module de type fini est toujours de présentation finie car $\text{Ker } g$ est engendré par un nombre fini d'éléments définissant une surjection $g : A^s \rightarrow \text{ker } f$. On peut en effet itérer cette procédure pour construire une **résolution libre** (peut-être pas de longueur finie) :

$$\dots A^{n_k} \rightarrow A^{n_{k-1}} \rightarrow \dots A^{n_2} \rightarrow A^{n_1} \rightarrow M \rightarrow 0.$$

§ 4. Modules et anneaux de longueur finie

4.1. Définition. Soit M un A -module. On dit qu'une chaîne de sous-modules

$$(*) \quad 0 = M_0 \subset M_1 \subset \dots \subset M_n = M \quad \text{inclusions strictes}$$

est une **chaîne de décomposition** (de longueur n) si l'on ne peut pas insérer un sous-module entre M_i et M_{i+1} . On dit qu'un module M est **simple** si les seuls sous-modules de M sont 0 et M . On a donc une définition équivalente : une chaîne (*) est chaîne de décomposition si et seulement si les modules $M_{i+1}/M_i, i = 0, \dots, n-1$ sont simples.

4.2. Lemme. Si M admet une chaîne de décomposition de longueur n , alors toute chaîne de décomposition de M est de même longueur n . Toute chaîne de sous-modules de M peut se raffiner en une chaîne de décomposition.

Remarque. La longueur de M , $l(M)$ est la plus petite longueur d'une chaîne de décomposition ($= \infty$ s'il n'y a pas de telle chaîne).

Démonstration.

1) On montre d'abord qu'un sous-module $N \neq M$ a une longueur $< l(M)$. Soit

$$0 = M_0 \subset M_1 \subset \dots \subset M_n = M$$

une chaîne de décomposition de longueur $n = l(M)$. Regardons $N_i = N \cap M_i \subset N \cap M_{i+1} = N_{i+1}$. Puisque N_{i+1}/N_i est un sous-module de M_{i+1}/M_i soit $N_{i+1}/N_i = 0$, soit $N_{i+1}/N_i = M_{i+1}/M_i$. Dans le premier cas $N_i = N_{i+1}$ et on pourra enlever N_i . Dans le deuxième cas N_{i+1}/N_i est simple. Après suppression des répétitions, on arrive à une chaîne de décomposition de N de longueur $\leq n = l(M)$ avec égalité si et seulement s'il n'y a aucune répétition et si les facteurs consécutifs sont les mêmes que pour la chaîne originale. Dans ce cas on a donc $M = N$.

2) Chaque chaîne (sans répétition) est de longueur $\leq l(M)$, car pour chaque cran $M_i \subset M_{i+1}$ on a $l(M_i) < l(M_{i+1})$. Si la longueur est $l(M)$, la chaîne est une chaîne de décomposition, car dans ce cas $l(M_{i+1}) = l(M_i) + 1$ implique que M_{i+1}/M_i est simple.

3) Considérons une chaîne de décomposition de longueur k de M . Alors, 2) implique que $k \leq l(M)$ et donc $k = l(M)$ par minimalité de $l(M)$.

4) Considérons une chaîne arbitraire de longueur k . Si $k = l(M)$ c'est une chaîne de décomposition par 2). Si $k < l(M)$ on peut insérer des sous-modules jusqu'à atteindre une chaîne de décomposition. ■

4.3. Lemme. $l(M)$ est finie si et seulement si M est noethérien et artinien.

Démonstration.

⇒ Chaque chaîne a une longueur finie et donc la ccc et la cdc sont valables.

⇐ On construit une chaîne de décomposition comme suit. Par la ccc, les sous-modules propres de M admettent un élément maximal M_{-1} . Alors M/M_{-1} est simple. De façon similaire, M_{-1} admet un sous-module propre M_{-2} tel que M_{-1}/M_{-2} est simple. Par la cdc ce procédé se termine après un nombre fini n d'itérations : $M_{-n} = 0$. ■

4.4. Exemples.

1. Soit

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

une suite exacte de A -modules. Alors, si M est de longueur finie, on voit facilement que les modules M' et M'' le sont aussi et $l(M) = l(M') + l(M'')$. Inversement, si $l(M') < \infty$ et $l(M'') < \infty$, alors $l(M) = l(M') + l(M'') < \infty$.

2. Soit V un k -espace vectoriel. Alors $l(V) < \infty$ si et seulement si une des conditions suivantes est vraie :

- $\dim_k V < \infty$,

- V a la ccc,
- V a la cdc.

Dans ce cas on a $l(V) = \dim_k V$.

4.5. Proposition. *Soit M un A -module de longueur finie et soit*

$$0 = M_0 \subset M_1 \cdots \subset M_{n-1} \subset M_n = M$$

une chaîne de décomposition. Alors les $\mathfrak{m}_i = \text{Ann}(M_{i+1}/M_i)$ sont des idéaux maximaux de A et la somme des localisations en les \mathfrak{m}_i différents :

$$f = \bigoplus_i f_i : M \rightarrow \bigoplus_i M_{\mathfrak{m}_i}$$

est un isomorphisme.

Démonstration.

On va d'abord regarder plus en détail les A -modules simples S . Ils sont de la forme A/\mathfrak{m} , \mathfrak{m} idéal maximal, car S doit être engendré par un seul élément s et $\text{Ann}(s) = \text{Ann}(S)$ est un idéal de A , forcément maximal, car S est simple. Considérons $S_{\mathfrak{n}}$ pour \mathfrak{n} un idéal maximal de A . Puisque A/\mathfrak{m} est un corps, $S_{\mathfrak{m}} = (A/\mathfrak{m})_0 = S$ et $S_{\mathfrak{n}} = 0$ si $\mathfrak{n} \neq \mathfrak{m}$. En particulier, $(S_{\mathfrak{m}})_{\mathfrak{n}} = 0$ si \mathfrak{m} et \mathfrak{n} sont d'idéaux maximaux différents.

Les quotients $S_i = M_{i+1}/M_i$ de notre chaîne sont simples et $\text{Ann}S_i = \mathfrak{m}_i$ sont des idéaux maximaux. On a vu que $(S_i)_{\mathfrak{m}} = S_i$ si $\mathfrak{m} = \mathfrak{m}_i$ et $= 0$ sinon. Donc pour un idéal maximal \mathfrak{m} quelconque

$$0 = (M_0)_{\mathfrak{m}} \subset (M_1)_{\mathfrak{m}} \cdots \subset (M_{n-1})_{\mathfrak{m}} \subset (M_n)_{\mathfrak{m}} = M_{\mathfrak{m}}$$

donne une chaîne de décomposition de $M_{\mathfrak{m}}$ si on garde les localisations telles que $\text{Ann}S_i = \mathfrak{m}$. Appliquant la discussion ci-dessus, il s'en suit que $(M_{\mathfrak{m}})_{\mathfrak{n}} = 0$ si $\mathfrak{n} \neq \mathfrak{m}$.

Considérons la somme des localisations :

$$f = \bigoplus_i f_i : M \rightarrow \bigoplus M_{\mathfrak{m}_i} \quad \text{Somme sur les idéaux maximaux de } A.$$

Dans cette somme, on peut omettre les termes avec \mathfrak{n} différent d'un des \mathfrak{m}_i , car ceux-ci sont nuls et donc la somme est en réalité une somme finie.

Je dis que f est un isomorphisme. Par 3.3.2 il suffit de montrer cela pour les localisation en tous les idéaux maximaux \mathfrak{n} :

$$f_{\mathfrak{n}} : M_{\mathfrak{n}} \rightarrow \bigoplus (M_{\mathfrak{m}})_{\mathfrak{n}}.$$

Puisque $(M_{\mathfrak{n}})_{\mathfrak{n}} = M_{\mathfrak{n}}$ et $(M_{\mathfrak{m}})_{\mathfrak{n}} = 0$ si $\mathfrak{n} \neq \mathfrak{m}$ le homomorphisme est l'identité et donc un isomorphisme. ■

4.6. Corollaire. *Soit A anneau artinien. Alors A est noethérien et n'a qu'un nombre fini d'idéaux premiers qui sont tous maximaux.*

Démonstration. On considère les idéaux qui sont produit d'un nombre fini d'idéaux maximaux. Puisque A est artinien il y a un idéal $J = \mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdots \mathfrak{m}_k$ minimal avec cette propriété. Donc $J\mathfrak{m} = J$ pour \mathfrak{m} maximal. On montre d'abord que $J = 0$.

On sait que $J \cdot J = J$ et donc, si $J \neq 0$ il y a un idéal I minimal parmi les idéaux I tel que $IJ \neq 0$. On a $(IJ)J = IJ^2 = IJ \neq 0$ et $IJ \subset I$ minimalité implique que $IJ = I$. Soit $f \in I$ tel que $fJ \neq 0$ et par minimalité de I il faut avoir $I = (f)$. De $IJ = I$ on tire qu'il y a $g \in J$ tel que

$f = fg$, c.à.d $(1 - g)f = 0$. Mais g est dans chaque idéal maximal et donc $1 - g$ est un unité et $f = 0$, une contradiction et $J = 0$.

Ensuite montrons que $l(A)$ est finie. Considérons les quotients $V_s = \mathfrak{m}_1 \cdots \mathfrak{m}_s / \mathfrak{m}_1 \cdots \mathfrak{m}_{s+1}$, une $k_s = A/\mathfrak{m}_{s+1}$ -espace vectoriel. Une chaîne descendante de sous-espaces correspond à une chaîne descendante d'idéaux de A et donc se termine. Il s'ensuit que $\dim_{k_s} V_s$ est de dimension finie et donc V_s admettent une chaîne de décomposition. Parce que $\mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdots \mathfrak{m}_k = 0$ on peut rassembler les chaînes d'idéaux de A correspondantes pour $s = 1, \dots, k - 1$ afin d'obtenir une chaîne de décomposition pour A . Donc $l(A)$ est finie et A est noethérien.

Finalement, pour \mathfrak{p} premier quelconque $\mathfrak{p} \supset 0 = \mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdots \mathfrak{m}_k$ et par 1.4.5 \mathfrak{p} contient un des \mathfrak{m}_j et $\mathfrak{p} = \mathfrak{m}_j$. Donc les seules idéaux premiers sont les \mathfrak{m}_j . ■

4.7. Corollaire. *Un anneau artinien est un produit direct d'un nombre fini d'anneaux artinien locaux.*

Démonstration. Un anneau artinien est de longueur finie et il y a donc un nombre fini d'idéaux maximaux \mathfrak{m} tel que la somme des localisations (en tant que modules)

$$A \rightarrow \bigoplus A_{\mathfrak{m}}$$

est un isomorphisme. Mais $\bigoplus A_{\mathfrak{m}}$ en tant qu'anneaux est un produit direct. ■

Chapitre 5. Décomposition primaire

§ 1. Idéaux primaires

On a vu que chaque variété affine est une réunion finie de variétés irréductibles. Ici on veut regarder la situation “duale” pour les idéaux. D’abord on introduit :

1.1. Définition. On dit qu’un idéal I est **indécomposable** si $I = I_1 \cap I_2$ implique $I = I_1$ ou $I = I_2$.

1.2. Lemme. Un idéal I dans un anneau noëthérien s’écrit

$$I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cdots \cap \mathfrak{q}_m$$

avec \mathfrak{q}_j indécomposable, $j = 1, \dots, m$.

La démonstration est la même que pour l’existence d’une décomposition d’une variété en parties irréductibles. Pour identifier les idéaux indécomposables on introduit :

1.3. Définition. Un idéal \mathfrak{q} dans un anneau A (pas forcément noëthérien) est **primaire** si $\mathfrak{q} \neq A$ et $a \cdot b \in \mathfrak{q}$ implique $a \in \mathfrak{q}$ ou $b^n \in \mathfrak{q}$ pour $n \in \mathbb{Z}_{>0}$ convenable (c’est-à-dire $b \in \sqrt{\mathfrak{q}}$). Si $\mathfrak{p} = \sqrt{\mathfrak{q}}$ on dit que \mathfrak{q} est **\mathfrak{p} -primaire**.

Le critère suivant est immédiate :

1.4. Critère. $\mathfrak{q} \subset A$ est primaire si et seulement si $B := A/\mathfrak{q} \neq 0$ et chaque diviseur de zéro de B est nilpotent.

1.5. Exemples.

- 1) Les idéaux premiers sont primaires.
- 2) Dans \mathbb{Z} , les idéaux (p^n) , p nombre premier, sont primaires.
- 3) Dans $A = k[x, y]$, k corps, $\mathfrak{q} = (x, y^2)$ est primaire avec racine $\mathfrak{p} = \sqrt{\mathfrak{q}} = (x, y)$. On a des inclusions strictes :

$$\mathfrak{p}^2 \subset \mathfrak{q} \subset \mathfrak{p}.$$

On a $A/\mathfrak{q} = k[x, y]/(x, y^2) \cong k[y]/(y^2)$ avec diviseurs de zéro $a \cdot y$, $a \in k$. Ils sont nilpotents. On voit facilement que \mathfrak{p}^2 est primaire. Donc il existent des idéaux primaires comme \mathfrak{q} qui ne sont pas puissance d’un idéal premier.

On a par contre :

1.6. Lemme. Si \mathfrak{m} est un idéal maximal, alors \mathfrak{m}^n est primaire. Plus généralement, un idéal I est primaire si \sqrt{I} est maximal.

Démonstration. On pose $\mathfrak{m} = \sqrt{I}$. Soit :

$$q : A \rightarrow A/I$$

l'application canonique. Soit $\bar{\mathfrak{m}}$ l'idéal engendré par $q(\mathfrak{m})$. On a $\bar{\mathfrak{m}} = \sqrt{0}$ car la classe de x est dans $\sqrt{0}$ si et seulement si $\exists n \in \mathbb{Z}$ tel que $x^n \in I$ si et seulement si $x \in \sqrt{I} = \mathfrak{m}$. D'autre part, $\sqrt{0}$ est l'intersection des tous les idéaux premiers \mathfrak{p} de A/I . Pour \mathfrak{p} premier on a $q^{-1}\mathfrak{p} \supset \mathfrak{m}$ et donc (car \mathfrak{m} est maximal) $q^{-1}\mathfrak{p} = \mathfrak{m}$. Conclusion : $\mathfrak{p} = \bar{\mathfrak{m}}$ est le seul idéal premier de A/I et chaque élément de A/I est ou bien inversible ou bien nilpotent. Donc chaque diviseur de zéro est bien nilpotent et I est primaire par le critère ci-dessus. ■

1.7. Exemple. $A = k[x, y, z]/(xy - z^2)$. Les images de x, y, z sont notées $\bar{x}, \bar{y}, \bar{z}$. L'idéal $\mathfrak{p} := (\bar{x}, \bar{z})$ est premier, car $A/\mathfrak{p} = k[y]$ est intègre. Mais \mathfrak{p}^2 n'est pas primaire : $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$ tandis que $\bar{x} \notin \mathfrak{p}^2$ et $\bar{y} \notin \mathfrak{p} = \sqrt{\mathfrak{p}^2}$.

1.8. Proposition. *Soit A un anneau noëthérien. Un idéal indécomposable est primaire. Chaque idéal est intersection d'idéaux primaires.*

Démonstration. Si I est un idéal indécomposable de A , alors 0 est indécomposable dans A/I . On peut donc supposer que $I = 0$. Soient $x, y \in A$ tels que $x \cdot y = 0$. Donc $y \in \text{Ann}(x) \subset \text{Ann}(x^2) \subset \dots \subset \text{Ann}(x^m) \subset \dots$. Cette chaîne se stabilise : $\text{Ann}(x^m) = \text{Ann}(x^{m+1}) = \dots$. Soit $a \in (y) \cap (x^m)$. Alors $a \cdot x = 0$ et $a = bx^m$. Donc $0 = ax = bx^{m+1}$ et $b \in \text{Ann}(x^{m+1}) = \text{Ann}(x^m)$. Il en résulte que $a = bx^m = 0$ et donc $0 = (y) \cap (x^m)$. Mais 0 est indécomposable et donc soit $y = 0$, soit $x^m = 0$, et 0 est alors primaire.

La dernière assertion est une conséquence immédiate du Lemme 5.1.2. ■

§ 2. Application : spectre d'un anneau noëthérien

Pour un anneau noëthérien A quelconque, on peut regarder $\text{Spec}A$ avec sa topologie de Zariski. Comme dans le cas d'une variété affine, un sous-ensemble X de $\text{Spec}A$ est appelé **irréductible** si $X = X_1 \cup X_2$ implique $X = X_1$ ou $X = X_2$ et on montre que pour chaque idéal $I \subset A$ l'ensemble $X = \hat{V}(I)$ admet une décomposition $X = X_1 \cup \dots \cup X_r$. Puisque $\hat{V}(J) = \hat{V}(\sqrt{J})$ (voir 3.4.1), on peut supposer que $X_i = X(I_i)$ avec I_i radical. Alors X_i irréductible implique que I_i est indécomposable et donc primaire par la proposition 5.1.8. Il s'ensuit que $I_i = \mathfrak{p}_i$ est premier : $X_i = \hat{V}(\mathfrak{p}_i)$ avec $\mathfrak{p}_i \supset I$ idéal premier, minimal parmi les idéaux premiers contenant I . On a donc

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \bigcap_{i=1}^r \mathfrak{p}_i$$

$$\hat{V}(I) = \hat{V}(\sqrt{I}) = \bigcup_i \hat{V}(\mathfrak{p}_i).$$

En particulier, pour $I = (0)$ on trouve :

2.1. Lemme. *Un anneau noëthérien n'a qu'un nombre fini d'idéaux premiers minimaux. Leur intersection est le radical de zéro de A .*

On a un complément utile :

2.2. Complément. *Un élément d'un idéal premier minimal est un diviseur de zéro.*

Démonstration. S'il n'y a qu'un seul idéal premier minimal, c'est le radical de zéro et rien n'est à montrer. Si $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ sont les idéaux premiers minimaux, on peut donc supposer que $s \geq 2$. Soit $x \in \mathfrak{p}_1$. Il y a $y \in \bigcap_{j \geq 2} \mathfrak{p}_j$, $y \notin \mathfrak{p}_1$. Sinon, $\bigcap_{j \geq 2} \mathfrak{p}_j \subset \mathfrak{p}_1$ et par la Proposition 1.4.5, \mathfrak{p}_1 contient un des \mathfrak{p}_j , ce qui contredit la minimalité de \mathfrak{p}_1 . Puisque $xy \in \bigcap_{j=1}^s \mathfrak{p}_j = \sqrt{0}$, l'élément xy est nilpotent, disons $(xy)^n = 0$. On a $y \notin \mathfrak{p}_2$ et donc $y^k \neq 0$ et il y a donc un entier $l \geq 0$ tel que $x^l y^k \neq 0$ mais $x^{l+1} y^k = 0$ et x est donc diviseur de zéro. ■

Regardons maintenant ce qui arrive quand on passe à la localisation $S^{-1}A$. Soit $i : A \rightarrow S^{-1}A$ l'homomorphisme canonique. Une traduction du Corollaire 3.1.4 est

2.3. Lemme. *Spec($S^{-1}A$) peut être identifié avec l'ensemble des idéaux premiers de A disjoints de S et sous cette identification la topologie de Zariski de A induit celle de $S^{-1}A$. L'application $i^* : \text{Spec} S^{-1}A \rightarrow \text{Spec} A$ défini par cette identification est donc continue.*

2.4. Exemple. Soit $V \subset k^n$ variété affine irréductible. Alors l'anneau $k[V]$ est intègre. Le corps $k(V)$ des fonctions rationnelles sur V est le corps de fractions de l'anneau $k[V]$ de V . Soit $W = V(\mathfrak{p}) \subset V$ une sous-variété irréductible définie par un idéal premier $\mathfrak{p} \subset k[V]$. On pose

$$\mathcal{O}_W(V) = k[V]_{\mathfrak{p}} \subset k(V).$$

Dans cet exemple, $\text{Spec} \mathcal{O}_W$ s'identifie aux idéaux premiers de $k[V]$ contenue dans \mathfrak{p} .

Cas particulier : $W = \{x\}$ un point de V . Donc $\text{Spec} \mathcal{O}_x(V)$ s'identifie aux idéaux premiers contenus dans l'idéal premier associé à ce point. Si k est algébriquement clos, on verra que le Nullstellensatz (théorème 6.4.5) implique que cet ensemble coïncide avec l'ensemble des sous-variétés irréductibles de V qui passent par x .

§ 3. Unicité des décompositions primaires

Pour avoir l'unicité d'une décomposition primaire il faut d'abord se restreindre aux **décompositions minimales**

$$(DP) \quad I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cdots \cap \mathfrak{q}_m$$

c'est-à-dire telles que

- 1) $\forall i \neq j, \sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$,
- 2) $\mathfrak{q}_i \not\supset \mathfrak{q}_1 \cap \mathfrak{q}_2 \cdots \hat{\mathfrak{q}}_i \cap \cdots \mathfrak{q}_m$.

Il est clair que si $\mathfrak{q}_i \supset \mathfrak{q}_1 \cap \mathfrak{q}_2 \cdots \hat{\mathfrak{q}}_i \cap \cdots \mathfrak{q}_m$ on pourrait omettre \mathfrak{q}_i dans la décomposition (DP) : $I = (\mathfrak{q}_1 \cap \mathfrak{q}_2 \cdots \hat{\mathfrak{q}}_i \cap \cdots \mathfrak{q}_m) \cap \mathfrak{q}_i = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cdots \hat{\mathfrak{q}}_i \cap \cdots \mathfrak{q}_m$. Aussi, si disons $\mathfrak{p} := \sqrt{\mathfrak{q}_1} = \sqrt{\mathfrak{q}_2}$ alors $\mathfrak{q} := \mathfrak{q}_1 \cap \mathfrak{q}_2$ est \mathfrak{p} -primaire : soit $x \cdot y \in \mathfrak{q}, x \notin \mathfrak{q}$, disons $x \notin \mathfrak{q}_1$; puisque $x \cdot y \in \mathfrak{q}_1$, $\exists n \in \mathbb{N}, y^n \in \mathfrak{p} = \sqrt{\mathfrak{q}_1} = \sqrt{\mathfrak{q}_2} = \sqrt{\mathfrak{q}_1 \cap \mathfrak{q}_2} = \sqrt{\mathfrak{q}}$.

Ces deux remarques montrent qu'on peut toujours supposer qu'une décomposition (DP) est minimale. Le but est de montrer le théorème d'unicité suivant :

3.1. Théorème. *Soit A anneau quelconque et $I \subset A$ un idéal. Dans une décomposition minimale $I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_m$ en idéaux primaires, les racines $\mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$ sont déterminées par I : On considère l'ensemble des racines $\sqrt{(I : x)}, x \in A$. Les \mathfrak{p}_j sont précisément les idéaux parmi eux qui sont premiers.*

Avant de montrer ce théorème on a besoin du :

3.2. Lemme. Soit \mathfrak{q} un idéal \mathfrak{p} -primaire dans un anneau A . Alors :

- 1) Si $x \in \mathfrak{q}$, alors $(\mathfrak{q} : x) = A$.
- 2) Si $x \notin \mathfrak{q}$, alors $(\mathfrak{q} : x)$ est \mathfrak{p} -primaire.

Démonstration. 1) $(\mathfrak{q} : x) = \{a \in A ; ax \in \mathfrak{q}\} = A$ car $x \in \mathfrak{q}$.

2) De $a \cdot x \in \mathfrak{q}$, $x \notin \mathfrak{q}$ on tire que $a \in \mathfrak{p}$ et donc

$$\mathfrak{q} \subset (\mathfrak{q} : x) \subset \mathfrak{p}.$$

En prenant les racines on trouve bien que $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$. Aussi, $(\mathfrak{q} : x)$ est \mathfrak{p} -primaire : si $a \cdot b \in (\mathfrak{q} : x)$, $a \notin \mathfrak{p}$, de $a \cdot (b \cdot x) \in \mathfrak{q}$ on tire que $b \cdot x \in \mathfrak{q}$, c'est-à-dire $b \in (\mathfrak{q} : x)$. ■

Démonstration du Théorème. Soit $x \in A$. On a $(I : x) = (\bigcap_{j=1}^m \mathfrak{q}_j : x) = \bigcap_{j=1}^m (\mathfrak{q}_j : x)$ et donc $\sqrt{(I : x)} = \bigcap_{j=1}^m \sqrt{(\mathfrak{q}_j : x)} = \bigcap_{j=1}^m \mathfrak{p}_j$. Par le lemme il suffit de prendre l'intersection parmi les \mathfrak{p}_j tels que $x \notin \mathfrak{q}_j$, $j = 1, \dots, m$. Puisque la décomposition est minimale, $\exists x_j \in \mathfrak{q}_1 \cap \dots \cap \hat{\mathfrak{q}}_j \cap \dots \cap \mathfrak{q}_m$, $x_j \notin \mathfrak{q}_j$ et donc $\sqrt{(I : x_j)} = \mathfrak{p}_j$.

Pour la réciproque, si $\sqrt{(I : x)} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_m$ est premier, il existe $j \in \mathbb{N}$ tel que $\sqrt{(I : x)} = \sqrt{(\mathfrak{q}_j : x)} = \mathfrak{p}_j$ (car un idéal premier qui est l'intersection d'un nombre fini d'idéaux est égal à un de ces idéaux; voir Chap I, §4, Prop. 5). ■

Considérons ensuite les anneaux noethériens.

3.3. Lemme. Soit A un anneau noethérien. Soit \mathfrak{q} un idéal \mathfrak{p} -primaire. Alors, il existe $n \in \mathbb{N}$ tel que $\mathfrak{p}^n \subset \mathfrak{q}$ et donc :

$$\mathfrak{p}^n \subset \mathfrak{q} \subset \mathfrak{p}.$$

Démonstration. Soit $\mathfrak{p} = (f_1, \dots, f_m)$ et soit $a_i \in \mathbb{N}$ t.q. $f_i^{a_i} \in \mathfrak{q}$, $i = 1, \dots, m$. Alors $n := (\sum_i (a_i - 1)) + 1$ convient. ■

Ce lemme permet de remplacer $\sqrt{(I : x)}$ par $(I : x)$ dans le théorème :

3.4. Théorème. Soit I un idéal dans un anneau noethérien. Dans une décomposition minimale $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$, les idéaux $\mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$ sont ceux parmi les idéaux $(I : x)$ qui sont premiers.

Démonstration. Si $(I : x)$ est premier, aussi sa racine l'est. Pour montrer la réciproque, il suffit de considérer le cas $I = 0$. Donc, soit $0 = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ une décomposition minimale. On pose $I_j = \mathfrak{q}_1 \cap \dots \cap \hat{\mathfrak{q}}_j \cap \dots \cap \mathfrak{q}_m$. On a vu que $\forall x \in I_j$, $x \neq 0$ on a $\sqrt{\text{Ann}(x)} = \sqrt{(0 : x)} = \mathfrak{p}_j$ et donc

$$(*) \quad \text{Ann}(x) \subset \sqrt{\text{Ann}(x)} = \mathfrak{p}_j.$$

Le lemme implique qu'on peut trouver m tel que $\mathfrak{p}_j^m \subset \mathfrak{q}_j$ et donc

$$I_j \cdot \mathfrak{p}_j^m \subset I_j \cap \mathfrak{p}_j^m \subset I_j \cap \mathfrak{q}_j = 0.$$

On peut supposer que m soit minimale avec cette propriété et donc $\exists y \neq 0$, $y \in I_j \mathfrak{p}_j^{m-1}$. Puisque $\mathfrak{p}_j \cdot y = 0$ on a aussi $\text{Ann}(y) \supset \mathfrak{p}_j$ et donc vu (*) on a l'égalité $\text{Ann}(y) = \mathfrak{p}_j$. ■

§ 4. Assassin et support

Soit I un idéal d'un anneau A . Alors $(I : x) = \{y \in A ; y \cdot x \in I\} = \{y \in A ; y \cdot \bar{x} = 0 \in A/I\}$. Ici \bar{x} est la classe de x dans A/I et on a considéré A/I comme A -module : $(I : x) = \text{Ann}(\bar{x})$. Dans la section précédente on a considéré les $(I : x)$ tels que $(I : x)$ est premier. Plus généralement on a :

4.1. Définition. Soit M un A -module. Un idéal premier \mathfrak{p} de A tel que $\exists m \in M, \mathfrak{p} = \text{Ann}(m)$ s'appelle un **assassin** de M (ou idéal premier associé à M).

L'ensemble des assassins est l'**assassin de** M , noté $\text{Ass}(M) \subset \text{Spec}(A)$.

on a $\mathfrak{p} \in \text{Ass}(M) \iff \exists L$ sous-module de M tel que $L \cong A/\mathfrak{p}$.

Dans ce langage les éléments de $\text{Ass}(A/I)$ sont précisément les idéaux premiers \mathfrak{p} tels que $\mathfrak{p} = (I : x)$. donc on pourra reformuler le théorème 2.4 :

4.2. Théorème. Soit I un idéal dans un anneau noethérien. Dans une décomposition minimale $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$, avec $\mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$ on a $\text{Ass}(A/I) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$.

Rappelons 3.4.3 que pour un A -module M , le support $\text{sup } M$ est l'ensemble d'idéaux premiers \mathfrak{p} tels que $M_{\mathfrak{p}} \neq 0$. Rappelons aussi qu'on a introduit la topologie de Zariski sur $\text{Spec}A$ de telle façon que les ensembles fermés sont donnés par $\hat{V}(S) = \{\mathfrak{p} \in \text{Spec}A ; \mathfrak{p} \supset S\}$, $S \subset \text{Spec}A$ un sous-ensemble quelconque.

Le but est de montrer le théorème suivant :

4.3. Théorème. Soit A un anneau noethérien, alors

- 1) $\mathfrak{p} \in \text{Ass}M \Rightarrow \hat{V}(\mathfrak{p}) \subset \text{Supp}M$,
- 2) Soit $\mathfrak{p} \in \text{Supp}M$ un idéal minimal (si M est de type fini, cela équivaut à dire que $\hat{V}(\mathfrak{p})$ est une composante irréductible maximale de $\text{Supp}M$), alors $\mathfrak{p} \in \text{Ass}M$.

Avant de donner la démonstration, nous avons besoin du :

4.4. Lemme.

Soit A noethérien, alors $\text{Ass}M \neq \emptyset$, plus précisément : un élément maximal \mathfrak{p} de l'ensemble $\{\text{Ann}(x) ; x \in M \setminus \{0\}\}$ est un idéal premier et donc $\mathfrak{p} \in \text{Ass}M$.

Démonstration. Supposons que I est un élément maximal de l'ensemble

$$\Sigma = \{\text{Ann}(x) ; x \in M \setminus \{0\}\}.$$

Soient $a, b \in A$ tels que $a \cdot b \in I = \text{Ann}(x)$, donc $a \cdot b \cdot x = 0$. Dans le cas où $b \cdot x = 0$ on a $b \in \text{Ann}(x) = I$. Sinon, avec $y = b \cdot x$ on a $y \neq 0$ et $\text{Ann}(y) \supset \text{Ann}(x)$ et donc on a égalité vu la maximalité de $I \in \Sigma$. Donc de $a \cdot y = 0$ il s'ensuit que $a \cdot x = 0$, c'est-à-dire $a \in \text{Ann}(x) = I$. Il suit que I est premier. ■

Démonstration du théorème.

- a) $\text{Ass}(M) \neq \emptyset$, supposons $\mathfrak{p} \in \text{Ass}(M)$. Donc M contient un sous-module L isomorphe à A/\mathfrak{p} . Les idéaux premiers de A/\mathfrak{p} correspondent aux idéaux premiers $\mathfrak{q} \supset \mathfrak{p}$ de A . Pour tous les idéaux premiers $\mathfrak{q} \supset \mathfrak{p}$ la localisation de A/\mathfrak{p} dans \mathfrak{q} est non-nulle. Donc $M_{\mathfrak{q}}$ contient un sous-module non-nulle et donc $\mathfrak{q} \in \text{Supp}(M)$.

b) Soit $\mathfrak{p} \in \text{Supp}(M)$ minimal et soit $B = A_{\mathfrak{p}}$. Minimalité veut dire que $M_{\mathfrak{q}} = 0$ si $\mathfrak{q} \subset \mathfrak{p}, \mathfrak{q} \neq \mathfrak{p}$ et donc $\text{Supp}_B(M_{\mathfrak{p}}) = \{\mathfrak{p}B\}$. On sait que $\text{Ass}_B(M_{\mathfrak{p}}) \neq \emptyset$, donc $\text{Ass}_B(M_{\mathfrak{p}}) = \text{Supp}(M_{\mathfrak{p}}) = \mathfrak{p}B$.
Donc

$$\exists \frac{m}{s}, \frac{m}{s} \neq 0, \text{Ann}_B\left(\frac{m}{s}\right) = \mathfrak{p}B.$$

Il faut revenir à A . Je dis que

$$\exists t \in A \quad \text{tel que } \text{Ann}(t \cdot m) = \mathfrak{p}.$$

En fait, on écrit $\mathfrak{p} = (f_1, \dots, f_m)$. On a $f_i \cdot (m/s) = 0 \Rightarrow \exists t_i \in A \setminus \mathfrak{p}$ tel que $t_i \cdot f_i \cdot m = 0$. L'élément $t = t_1 \cdots t_m$ convient : D'un part $\mathfrak{p} \cdot (t \cdot m) = 0 \Rightarrow \mathfrak{p} \subset \text{Ann}(t \cdot m)$. D'autre part $t, s \in A \setminus \mathfrak{p}$ et dans $A_{\mathfrak{p}}$ on a

$$a \cdot \frac{m}{s} = a \cdot \frac{t \cdot m}{t \cdot s} = 0, \quad \forall a \in \text{Ann}(tm).$$

Donc $\text{Ann}_A(tm) \subset \text{Ann}_A(m/s) = \mathfrak{p}$. ■

Maintenant regardons le cas d'un A -module de type fini. Rappelons (3.4.4) que dans ce cas $\text{Supp}(M) = \hat{V}(\text{Ann}M)$.

4.5. Corollaire. *Pour M de type fini on a*

$$\text{Supp}(M) = \bigcup_{\mathfrak{p} \in \text{Ass}M} \hat{V}(\mathfrak{p}).$$

Démonstration. $\text{Supp}M = \hat{V}(\text{Ann}M) = \hat{V}(\mathfrak{p}_1) \cup \hat{V}(\mathfrak{p}_2) \cdots \cup \hat{V}(\mathfrak{p}_m)$, où les $\hat{V}(\mathfrak{p}_j)$ sont les composantes irréductibles maximales de $\text{Supp}M$. Dans cette réunion on peut supposer que les $\hat{V}(\mathfrak{p}_j)$ soient maximales et donc, par le théorème $\mathfrak{p}_j \in \text{Ass}M$. ■

Chapitre 6. Extensions finies

§ 1. Extensions entières ou de type fini

1.1. Définitions. Soit A un anneau et B une A -algèbre.

- 1) B est une **A -algèbre finie** si B est de type fini en tant que A -module.
- 2) B est une **A -algèbre de type fini** si B est engendré comme A -algèbre par un nombre fini d'éléments.
- 3) $y \in B$ est **entier sur A** si $\exists P \in A[X]$, unitaire (c'est-à-dire $P = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n$) tel que $P(y) = 0$. On dit que $P = 0$ est une relation de dépendance intégrale pour y .
- 4) B est une **A -algèbre entière** si chaque $y \in B$ est A -entier.
- 5) Soit I un idéal de A . On dit que $y \in B$ est **I -entier** si y admet une relation de dépendance intégrale avec $a_i \in I$.

1.2. Exemples.

- 1) $A[X_1, \dots, X_n]$ est une A -algèbre de type fini.
- 2) Si $V \subset k^n$ est une k -variété, l'anneau de coordonnées $k[V]$ est de type fini sur k .
- 3) L'élément X est entier sur $k[X^2]$ car X satisfait l'équation $Y^2 - X^2 = 0$.
- 4) L'élément $\frac{1}{2}(1 + \sqrt{5})$ est entier sur \mathbb{Z} (l'équation de $\frac{1}{2}(1 + \sqrt{5})$ est $X^2 - X - 1 = 0$).
- 5) Soit B une A -algèbre finie, $I_B = B \cdot I$ l'extension d'un idéal $I \subset A$. Alors $y \in I_B$ est I -entier : appliquer l'astuce du déterminant [Chap II, 3.1] à la multiplication μ_y par y dans l'algèbre B ($y \cdot B \subset I_B = I \cdot B$) :

$$(\mu_y^n + a_1 \mu_y^{n-1} + \dots + a_n \cdot \mathbb{1}_B)1_B = y^n + a_1 y^{n-1} + \dots + a_n = 0, \quad a_1, \dots, a_n \in I.$$

Plus généralement si $x^k = y \in I_B$ on voit que x^k et donc aussi x est I -entier : les éléments de $\sqrt{I_B}$ sont des I -entiers.

Si on applique l'exemple 2.5 à $I = (1)$, on trouve qu'une A -algèbre de type fini est finie si et seulement si elle est entière. Plus généralement on a :

1.3. Lemme. Soit B une A -algèbre. Les énoncés suivants sont équivalents :

- i) y est A -entier,
- ii) Le sous-anneau $A[y]$ de B engendré par y est une A -algèbre finie,
- iii) Il y a une A -sous-algèbre C de B , finie sur A , telle que $C \supset A[y]$.

Démonstration.

Pour simplifier on suppose que $A \subset B$. i) \Rightarrow ii) : Supposons que $y^n + a_1 y^{n-1} + \dots + a_n = 0$. Cette relation implique que $A[y] = A \cdot 1 + A \cdot y + \dots + A \cdot y^{n-1}$, c'est-à-dire $A[y]$ est un A -module de type fini.

ii) \Rightarrow iii) On peut prendre $C = A[y]$.

iii) \Rightarrow i) Par l'exemple 2.5 on sait que y est entier. ■

Remarque. Si C est un B -module fini, qui à son tour est un A -module fini, alors C est un A -module fini : si C est engendré comme B -module par y_1, \dots, y_m et si B est engendré sur A par x_1, \dots, x_n , alors C est engendré sur A par les produits $x_i y_j, i = 1, \dots, n, j = 1, \dots, m$.

1.4. Corollaire. Soit B une A -algèbre.

a) Soient $y_1, \dots, y_m \in B$ tous A -entiers, alors $A[y_1, \dots, y_m]$ est finie sur A .

b) Si C est un anneau qui est B -module entier, qui à son tour est un A -module entier, alors C est un A -module entier,

Démonstration.

a) Récurrence sur m . Pour $m = 1$, c'est le lemme précédent. Par récurrence, l'algèbre $A[y_1, \dots, y_{m-1}]$ est un A -module de type fini et par le lemme précédent $A[y_1, \dots, y_m]$ est un $A[y_1, \dots, y_{m-1}]$ -module de type fini. La remarque précédente donne la conclusion.

b) Soit $z \in C$ et $z^n + b_1 z^{n-1} + \dots + b_n, b_i \in B$ une relation unitaire pour z . Soit $A' = A[b_1, \dots, b_{n-1}]$, alors l'algèbre $A'[z]$ est finie sur A' , qui est elle-même une algèbre finie sur A . Par la remarque précédente, $A'[z]$ est fini sur A et donc, par le lemme, z est entier sur A . ■

Le corollaire (b) entraîne que l'ensemble $A' = \{y \in B ; y \text{ est } A\text{-entier}\}$ est un sous-anneau de B : si $x, y \in B$ sont A -entiers, alors $A[x, y]$ est A -entier et donc $x \pm y$ et $x \cdot y$ sont A -entiers. De plus, si $y \in B$ est entier sur A' , alors y est entier sur A et donc $y \in A'$. Cela explique la terminologie suivante :

1.5. Définition.

i) L'anneau $A' = \{y \in B ; y \text{ est } A\text{-entier}\}$ est **la clôture intégrale** de A dans B .

ii) Un anneau A est **normal** si A est un anneau intègre égal à sa clôture intégrale dans le corps de fractions $Q(A)$ de A .

1.6. Exemples.

1) Un anneau factoriel A est normal. Soit $y^n + a_1 y^{n-1} z + \dots + a_n z^n = 0$, une relation de dépendance intégrale pour $y/z \in Q(A)$. Si on suppose que y et z sont étrangers, du fait que z divise y^n on tire que $z \in A$ doit être inversible et $y/z \in A$.

2) Soit n un entier sans facteurs carrés. La clôture intégrale de \mathbb{Z} dans $\mathbb{Q}(\sqrt{n})$ est $\mathbb{Z}[\sqrt{n}]$ si $n \not\equiv 1 \pmod{4}$ et $\mathbb{Z}[\frac{1}{2}(1+\sqrt{n})]$ si $n \equiv 1 \pmod{4}$. Les éléments 1 et \sqrt{n} sont entier et si $n \equiv 1 \pmod{4}$, l'élément $\frac{1}{2}(1 + \sqrt{n})$ est entier. Inversement, si $\xi = \frac{a + b\sqrt{n}}{c}$, $a, b, c \in \mathbb{Z}$ est entier, alors le conjugué $\frac{a - b\sqrt{n}}{c}$ est entier et donc la somme $2a/c$ et le produit $(a^2 - b^2 n)/c^2$ le sont. Mais \mathbb{Z} étant normal cela implique que $2a/c \in \mathbb{Z}$ et $(a^2 - b^2 n)/c^2 \in \mathbb{Z}$ et donc $c|2a$ et $c^2|a^2 - b^2 n$.

On peut supposer que $0 \leq a/c < 1$ et $0 \leq b/c < 1$, donc soit $a = 0 = b$, soit $c = 2$, $a = 1$, $b = 1$ et dans ce cas $n \equiv 1 \pmod{4}$.

- 3) Soit $A = k[X, Y]/(Y^2 - X^3)$, k corps. Soient x et y les classes de X et Y modulo $(Y^2 - X^3)$. Le corps de fractions est $k(t)$, $t := y/x$. En effet, on a $x^3 = y^2 \Rightarrow x = y^2/x^2 = t^2$ et $y = x^3/y = x^2 \cdot (1/t) = t^3$, donc $k(t)$ est le plus petit corps qui contient A . Aussi, t est entier sur A mais $t \notin A$ et A n'est donc pas normal.

Plus généralement, si $I \subset A$ est un idéal, on définit :

1.7. Définition. La clôture intégrale d'un idéal $I \subset A$ dans B est

$$I'_B = \{y \in B ; y \text{ est } I\text{-entier}\}.$$

Si $x \in I'_B$, alors l'équation de dépendance intégrale pour x montre que $y = x^n \in A' \cdot I = I_{A'}$. Inversement, si $y = x^n \in A' \cdot I$, $y = \sum_j a_j x_j$ avec $x_j \in I$ et $a_j \in A'$. Puisque $y \in A[a_1, \dots, a_n]$, une A -algèbre finie, on peut appliquer l'exemple 1.2 (5) ci-dessus pour voir que y est I -entier. On a donc démontré le :

1.8. Lemme. Soit A' la clôture intégrale de A dans B . Alors

$$\{y \in B ; y \text{ est } I\text{-entier}\} = \sqrt{I_{A'}}$$

et en particulier c'est un ensemble stable par addition et multiplication.

La proposition suivante montre que la dépendance entière passe aux quotients et aux fractions :

1.9. Proposition. Soient $A \subset B$ deux anneaux. Supposons que B est entier sur A .

1. Soit J un idéal de B et $I = A \cap J$. Alors B/J est A/I -entier.
2. Soit S un sous-ensemble multiplicativement stable de A . Alors $S^{-1}B$ est $S^{-1}A$ -entier.

Démonstration.

1. Si $x \in B$ satisfait à $x^n + a_1 x^{n-1} + \dots + a_n = 0$ avec $a_i \in A$, la classe $x + J$ satisfait à $x^n + \bar{a}_1 x^{n-1} + \dots + \bar{a}_n = 0$ où $\bar{a}_i \in A + I$ sont les classes de a_i dans A/I .
2. Si x satisfait à l'équation ci-dessus, $\forall s \in S$ on a :

$$\left(\frac{x}{s}\right)^n + \left(\frac{a_1}{s}\right)\left(\frac{x}{s}\right)^{n-1} + \dots + \left(\frac{a_n}{s^n}\right) = 0,$$

ce qui montre que x/s est $S^{-1}A$ -entier. ■

§ 2. “Going-up”

On a vu que si $A \subset B$ et si \mathfrak{p} est un idéal premier dans A , son extension $\mathfrak{p} \cdot B$ n'est pas forcément premier dans B . On veut montrer :

2.1. Proposition. Soient $A \subset B$ deux anneaux tels que B est A -entier. Soit \mathfrak{p} un idéal premier de A . Alors il y a un idéal premier $\mathfrak{q} \subset B$ qui relève \mathfrak{p} , c.à.d. tel que $\mathfrak{q} \cap A = \mathfrak{p}$. De plus, \mathfrak{q} est maximal si et seulement si \mathfrak{p} l'est.

Démonstration. L'idée est localiser en \mathfrak{p} (c.à.d. on pose $S = A \setminus \mathfrak{p}$ multiplicativement stable dans A ainsi que dans B). On dénote comme d'habitude $A_{\mathfrak{p}} = S^{-1}A$ mais aussi $B_{\mathfrak{p}} = S^{-1}B$. Avec $i : A \rightarrow A_{\mathfrak{p}}$ et $j : B \rightarrow B_{\mathfrak{p}}$ les homomorphismes canoniques, on a le diagramme commutatif :

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow i & & \downarrow j \\ A_{\mathfrak{p}} & \hookrightarrow & B_{\mathfrak{p}} \end{array}$$

La proposition 6.1.9 montre que $B_{\mathfrak{p}}$ est $A_{\mathfrak{p}}$ -entier. On sait que $A_{\mathfrak{p}}$ est un anneau local, mais ce n'est pas forcément vrai pour $B_{\mathfrak{p}}$. Soit \mathfrak{n} un idéal maximal de $B_{\mathfrak{p}}$. On va montrer que $\mathfrak{m} = \mathfrak{n} \cap A_{\mathfrak{p}}$ est maximal. Il s'ensuit que \mathfrak{m} est l'unique idéal maximal de $A_{\mathfrak{p}}$. Alors $\mathfrak{q} = j^{-1}\mathfrak{n}$ est premier dans B et du fait que que \mathfrak{m} est l'idéal maximal de $A_{\mathfrak{m}}$ on tire que $\mathfrak{q} \cap A = i^{-1}\mathfrak{m} = \mathfrak{p}$.

Il suffit maintenant de montrer :

Critère Soient $A \subset B$ deux anneaux avec B entier sur A . Soit \mathfrak{q} un idéal premier de B . Alors $\mathfrak{p} = \mathfrak{q} \cap A$ est maximal si et seulement si \mathfrak{q} l'est.

Preuve du critère. Puisque $A' = A/\mathfrak{p} \subset B' = B/\mathfrak{q}$ sont des anneaux intègres c'est équivalent de montrer que B' est un corps si et seulement si A' l'est. Supposons que A' est un corps et supposons qu'une équation de dépendance intégrale pour $B' \ni y \neq 0$ est

$$(*) \quad y^n + a_1 y^{n-1} + \dots + a_n = 0, \quad a_i \in A'$$

avec $a_n \neq 0$ (c'est possible car B' est intègre). Alors $y^{-1} = -a_n^{-1}(y^{n-1} + a_1 y^{n-2} + \dots + a_{n-1}) \in B'$ et B' est donc un corps. Pour l'implication réciproque on note que $a \in A'$ possède un inverse $y \in B'$ avec une relation de dépendance intégrale (*). On a $y = y(ya)^{n-1} = y^n a^{n-1} = -a^{n-1}(a_1 y^{n-1} + \dots + a_n) = -(a_1 + a_2 a + \dots + a_n a^{n-1}) \in A'$. ■

2.2. Corollaire ("Incompatibilité"). Soient $A \subset B$ deux anneaux avec B entier sur A . Soient $\mathfrak{q}_1 \subset \mathfrak{q}_2$ deux idéaux premiers de B avec $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{p}$, alors $\mathfrak{q}_1 = \mathfrak{q}_2$.

Démonstration. On sait (Proposition 6.1.9) que $B_{\mathfrak{p}}$ est $A_{\mathfrak{p}}$ -entier. Soit $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$ et $\mathfrak{n}_j = \mathfrak{q}_j B_{\mathfrak{p}}$, $j = 1, 2$. On a $\mathfrak{n}_1 \subset \mathfrak{n}_2$ et $\mathfrak{n}_1 \cap A = \mathfrak{n}_2 \cap A = \mathfrak{m}$. Le critère implique que \mathfrak{n}_1 et \mathfrak{n}_2 sont maximaux et donc égaux et donc aussi les idéaux \mathfrak{q}_1 et \mathfrak{q}_2 le sont. ■

On a donc vu comment trouver un idéal premier dans B qui étend \mathfrak{p} . Plus généralement on peut étendre une chaîne d'idéaux premiers :

2.3. Théorème de montée ("Going-up"). Soient $A \subset B$ deux anneaux avec B entier sur A . Soit $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots \subset \mathfrak{p}_n$ dans A une chaîne croissante d'idéaux premiers tels que les m premiers d'entre eux aient été étendus aux idéaux premiers $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \dots \subset \mathfrak{q}_m$ dans B , alors on peut trouver des idéaux premiers \mathfrak{q}_j , $j = m+1, \dots, n$ avec $\mathfrak{q}_j \cap A = \mathfrak{p}_j$ qui étendent la chaîne à $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \dots \subset \mathfrak{q}_n$.

Démonstration. Par récurrence on est amené au cas $m = 1$ et $n = 2$. L'anneau $\bar{B} = B/\mathfrak{q}_1$ est entier sur $\bar{A} = A/\mathfrak{p}_1$ (par la Proposition 6.1.9) et l'argument ci-dessus produit un idéal premier $\bar{\mathfrak{q}}_2$ dans \bar{B} tel que $\bar{\mathfrak{q}}_2 \cap \bar{A} =$ l'image de \mathfrak{p}_2 dans \bar{A} . L'image inverse dans B de $\bar{\mathfrak{q}}_2$ contient \mathfrak{q}_1 et son intersection avec A est égale à \mathfrak{p}_2 . ■

§ 3. Théorème de normalisation de Noether

Soit k un corps et A une k -algèbre. On dit que y_1, y_2, \dots, y_m sont algébriquement indépendants sur k s'il n'y a pas de relation polynômiale entre les y_j , c.à.d. si la sous-algèbre engendrée par les y_j est isomorphe à l'algèbre des polynômes $k[X_1, \dots, X_m]$.

3.1. Théorème (Normalisation de Noether). Soit k un corps et A une k -algèbre engendrée par n éléments. Alors,

$$\exists z_1, \dots, z_m \text{ algébriquement indépendants}/k \quad m \leq n$$

telle que A est finie sur $B = k[z_1, \dots, z_m]$, c.à.d. A est finie sur une algèbre de polynômes.

Le théorème est une conséquence de la proposition suivante :

3.2. Proposition. Soit $A = k[y_1, \dots, y_n]$. Si les y_i sont algébriquement dépendants, $\exists y'_1, \dots, y'_{n-1} \in A$ tels que y_n est A' -entier, où $A' = k[y'_1, \dots, y'_{n-1}]$, et $A = A'[y_n]$. Plus précisément, si $f \in k[X_1, \dots, X_n]$ est un polynôme de dépendance pour les y_j , $f(y'_1, \dots, y'_{n-1}, X)$ est un polynôme unitaire avec racine y_n .

Proposition \Rightarrow Théorème : On le fait par récurrence sur n , le cas $n = 0$ étant clair. On suppose donc que $n > 0$. Si y_1, \dots, y_n sont algébriquement indépendants on termine. Sinon, il y a une relation polynômiale entre les y_j . La proposition fournit $t_1, \dots, t_{n-1} \in A$ tel que y_n est A' -entier, $A' = A[t_1, \dots, t_{n-1}]$ et $A = A'[y_n]$. Par récurrence applique à A' on trouve $z_1, \dots, z_m \in A'$, algébriquement indépendants / k et tels que A' est finie sur $B = k[z_1, \dots, z_m]$. On a

$$B = k[z_1, \dots, z_m] \subset A' \subset A'[y_n] = A.$$

Puisque A' est finie sur B et A est finie sur A' (car y_n est A' -entier) il s'ensuit que A est finie sur B . ■

Démonstration de la proposition

On suppose pour simplifier que **le corps k n'est pas fini**. Sinon, la proposition reste vraie mais la démonstration est différente. Voir [Re2, §4].

Sous l'hypothèse que k est infini on va construire les y'_i comme expressions linéaires en y_1, \dots, y_n .

Soit $f \in k[X_1, \dots, X_n]$ un polynôme de dépendance pour les y_j . On va remplacer y_i par $y'_i = y_i - \alpha_i y_n$, $i = 1, \dots, n-1$ tel que

$$g(y'_1, \dots, y'_{n-1}, y_n) := f(y_1, \dots, y_n) = f(y'_1 + \alpha_1 y_n, \dots, y'_{n-1} + \alpha_{n-1} y_n, y_n)$$

soit unitaire en tant que polynôme en y_n . Si $\deg f = d$ on écrit $f = F + h$, où F est homogène de degré d et $\deg h < d$. Alors

$$g(y'_1, \dots, y'_{n-1}, y_n) = F(\alpha_1, \dots, \alpha_{n-1}, 1)y_n^d + \text{termes de degré } < d \text{ en } y_n.$$

Il suffit de trouver α_i tels que $F(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. Ici on utilise l'hypothèse que k contient un infini d'éléments. Si par exemple $n = 2$ il s'agit de choisir α_1 différent d'un des zéros du polynôme $F(X, 1)$. Le cas général se déduit par récurrence sur n : on peut supposer que $F(X_1, \dots, X_{n-1}, 1) = G(X_1, \dots, X_{n-2})X_{n-1}^d + \dots$ avec $G \neq 0$ et par récurrence on trouve $\alpha_1, \dots, \alpha_{n-2}$ tels que $G(\alpha_1, \dots, \alpha_{n-2}) \neq 0$. Alors $H(X) = F(\alpha_1, \dots, \alpha_{n-2}, X_{n-1}, 1)$ est de degré d en X_{n-1} et par le cas $n = 2$ on peut trouver α_{n-1} tel que $F(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. ■

Plus loin on aura besoin de quelques précisions dans ce théorème.

3.3. Corollaire. On suppose que k soit un corps infini. Soit $A = k[x_1, \dots, x_n]$ un k -algèbre de type fini. Alors il y a $m \leq n$ combinaisons linéaires z_1, \dots, z_m des x_i et $f \in A$ telles que

1. Les z_j sont algébriquement indépendants,
2. A est une algèbre $k[z_1, \dots, z_m]$ -finie,
3. Si A est intègre, le corps de fractions de A est $k(z_1, \dots, z_m, f)$.

Pour la démonstration dans le cas général voir [Re1]. Ici on suppose pour simplifier que k est de caractéristique zéro. Dans ce cas on peut utiliser le théorème de l'élément primitif :

3.4. Théorème. Soit K un corps de caractéristique 0 et $L|K$ une extension algébrique finie. Alors il existe $x \in L$ t.q. $L = K(x)$.

Démonstration. Supposons que $L = K(a_1, \dots, a_m)$ avec $m \geq 2$. Par récurrence on se ramène au cas $m = 2$. Soit $f_j(X)$ le polynôme minimal de a_j , $j = 1, 2$. Supposons que les racines de f_j sont $\xi_{jk}, k = 1, \dots, \deg f_j$ (dans une clôture algébrique de K). Supposons que $a_1 = \xi_{11}$ et $a_2 = \xi_{21}$. On cherche $c \in K$ t.q. $x = a_1 + ca_2$ engendre $L|K$. Le polynôme $g(X) = f_1(x - cX) \in K(x)[X]$ admet la racine $X = a_2$ car $0 = f_1(a_1) = f_1(x - ca_2)$. On calcule que $X = \xi_{2j}$ est aussi racine si et seulement si

$$\exists k \geq 2 \text{ t.q. } c = \frac{\xi_{1k} - a_1}{a_2 - \xi_{2j}}.$$

Il est à noter que $a_2 \neq \xi_{2j}$ car f_2 est sans racines multiples (sinon, f_j ne serait pas minimal, ici on utilise que $\text{car}(K)=0$). Si on choisit c différent des éléments $\frac{\xi_{1k} - a_1}{a_2 - \xi_{2j}}$, la seule racine commun à $g(X)$ et f_2 (dans une clôture algébrique) est a_2 . Donc l'idéal dans $K(x)[X]$ engendré par $g(X)$ et f_2 est $(X - a_2)$ et donc $a_2 \in K(x)$ et donc aussi $a_1 \in K(x)$ et $L = K(x)$. ■

La preuve montre qu'on peut dire de plus :

3.5. Précision. Si $L = K(z_1, \dots, z_k)$, alors on peut prendre pour x une combinaison linéaire des z_j .

Démonstration du Corollaire. Les x_j engendrent le corps K des fractions de A sur k et donc aussi sur $k(z_1, \dots, z_m)$. La précision montre qu'il y $f \in K$ telle que $K = k(z_1, \dots, z_m)(f)$ avec f combinaison linéaire des x_i avec coefficients dans $k(z_1, \dots, z_m)$. Après multiplication avec le dénominateur commun on peut supposer que ces coefficients sont dans $k[z_1, \dots, z_m]$ et donc $f \in A$. ■

§ 4. Nullstellensatz

On montre d'abord

4.1. Théorème (Nullstellensatz faible). Soient K et k deux corps tels que K soit une k -algèbre de type fini. Alors K est une k -extension finie.

Démonstration. Par normalisation de Noether, $\exists z_1, \dots, z_m \in K$, algébriquement indépendants, tels que K soit une $k[z_1, \dots, z_m]$ -algèbre finie. Posons $A = k[z_1, \dots, z_m]$. L'algèbre K est donc A -entière. Puisque K est un corps, le critère 6.2.1 implique que $A = k[z_1, \dots, z_m]$ est un corps c.à.d. $A = k$ puisque les z_j sont algébriquement indépendants. Il s'ensuit que K est une k -extension finie. ■

4.2. Corollaire. Si k est algébriquement clos, un idéal maximal \mathfrak{m} de $k[X_1, \dots, X_n]$ est de la forme $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$, $a_i \in k$.

Démonstration. $K = k[X_1, \dots, X_n]/\mathfrak{m}$ est en même temps une k -algèbre de type finie et un corps, donc de degré fini sur k , mais k est algébriquement clos et donc $k = K$ et donc $\exists a_i \in k$ tel que $X_i + \mathfrak{m} = a_i$, $i = 1, \dots, n$. ■

Rappelons quelques notations :

1. Pour un sous-ensemble $X \subset k^n$ on écrit

$$I(X) = \{f \in k[X_1, \dots, X_n] ; f(x) = 0 \forall x \in X\} \quad \text{l'idéal de } X \text{ dans } k[X_1, \dots, X_n].$$

2. Pour un idéal I de $k[X_1, \dots, X_n]$ on écrit

$$V(I) = \{P \in k^n ; f(P) = 0, \forall f \in I\} \quad \text{l'ensemble des zéros de } I.$$

Les ensembles $V(I)$ sont par définition les **variétés affines**.

4.3. Lemme.

1. $X \subset Y \Rightarrow I(X) \supset I(Y)$,
2. $I \subset J \Rightarrow V(I) \supset V(J)$,
3. $J \subset I(V(J))$.
4. On a $X \subset V(I(X))$ avec $=$ si et seulement si X est une variété affine.

Démonstration. 1. , 2. et 3. sont triviaux, ainsi que l'inclusion de 4.

Si $X = V(J)$, parmi les fonction qui s'annulent sur X se trouvent les fonctions de J , donc $V(I(X)) \subset V(J) = X$ et on a égalité.

Si $X = V(I(X))$, X est une variété algébrique avec $I = I(X)$. ■

On peut avoir une inclusion stricte $J \subset I(V(J))$:

4.4. Exemples.

1. Si k n'est pas algébriquement clos, $f \in k[X]$ non-constante avec ses racines hors de k . Alors $J = (f) \neq k[X]$. Mais $V(J) = \emptyset$ car f n'a pas de racines dans k . Donc $I(V(J)) = k[X] \neq J$.
2. On a toujours $V(f^n) = V(f)$ et donc $f \in I(V(f^n))$ mais en générale $f \notin (f^n)$, par exemple $f = X \in k[X]$ et $n = 2$.

Le théorème suivant dit que ces deux possibilités de produire des inclusions strictes sont les seules :

4.5. Théorème (Nullstellensatz de Hilbert). *On suppose que k est un corps algébriquement clos. Les trois énoncés suivants sont équivalents :*

1. Tout idéal maximal de $k[X_1, \dots, X_n]$ est de la forme $(X_1 - a_1, \dots, X_n - a_n)$, $a_j \in k$,
2. Pour tout I , idéal propre de $k[X_1, \dots, X_n]$, il y a un point $P \in k^n$ dans le lieu de zéros de I : $f(P) = 0, \forall f \in I$.
3. Pour tout J , idéal de $k[X_1, \dots, X_n]$ on a

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

C'est-à-dire si $f(P) = 0$ quel que soit $P \in V(J)$ alors $\exists n \in \mathbb{N}$ tel que $f^n \in J$.

Démonstration.

1 \Rightarrow 2 I est contenu dans un idéal maximal qui doit être de la forme $(X_1 - a_1, \dots, X_n - a_n)$, $a_j \in k$, et donc en posant $P = (a_1, \dots, a_n)$ on a $f(P) = 0$ quel que soit $f \in I$.

2 \Rightarrow 3 Soit f un polynôme tel que $f(x) = 0$ quel que soit $x \in V(J)$. On introduit une nouvelle variable T et on considère l'idéal $J_1 = (J, fT - 1) \in k[X_1, \dots, X_n, T]$. La variété associée n'a aucun point. Sinon $\exists (a_1, \dots, a_n, b) \in k^{n+1}$ tel que $g(a_1, \dots, a_n) = 0$ si $g \in J$ et donc $(a_1, \dots, a_n) \in V(J)$ et par hypothèse $f(a_1, \dots, a_n) = 0$. Mais aussi $f(a_1, \dots, a_n)b - 1 = 0$, une contradiction. Donc $V(J_1) = \emptyset \Rightarrow J_1 = k[X_1, \dots, X_n, T]$ contient 1, et dans $k[X_1, \dots, X_n, T]$ on a :

$$1 = \sum_j g_j f_j + g_0(fT - 1), \quad f_j \in J, g_0, g_j \in k[X_1, \dots, X_n, T].$$

En substituant $T = 1/f$ on trouve

$$1 = \sum_i \frac{h_i(X_1, \dots, X_n)}{f^{n_i}} f_i \Rightarrow f^N \in J.$$

3 \Rightarrow 1 Soit \mathfrak{m} maximal. On a $I(V(\mathfrak{m})) = \mathfrak{m}$ et donc $V(\mathfrak{m}) \neq \emptyset$. Soit $P = (a_1, \dots, a_n)$ un point de $V(\mathfrak{m})$ avec idéal maximal $I(P) \supset I(V(\mathfrak{m})) = \mathfrak{m}$. On a l'égalité par maximalité de \mathfrak{m} et $\mathfrak{m} = I(P) = (X_1 - a_1, \dots, X_n - a_n)$. ■

4.6. Corollaire. *Sous les hypothèses du Nullstellensatz on a une correspondance biunivoque entre les idéaux radicaux I , c.à.d. $I = \sqrt{I}$ et les variétés affines. Sous cette correspondance les idéaux premiers correspondent aux variétés irréductibles.*

Plus généralement on a :

4.7. Proposition. *Soit k un corps algébriquement clos et A un k -algèbre de type fini, disons $A = k[X_1, \dots, X_n]/J$. Alors $\text{Spec} A = \{ \text{variétés irréductibles contenues dans } V(J) \}$.*

4.8. Normalisation de Noether : version géométrique. *Soit $V \subset k^n$ variété algébrique irréductible (k corps algébriquement clos). Il y a une projection linéaire $k^n \rightarrow k^m$ telle que la restriction à V donne une surjection $V \rightarrow k^m$ à fibres finies.*

Démonstration. Soit $I = I(V)$ l'idéal de V . L'anneau $k[V] = k[X_1, \dots, X_n]/I = k[x_1, \dots, x_n]$ est un k -algèbre de type fini et on peut appliquer le Corollaire du théorème de normalisation de Noether. Les z_j sont des combinaisons linéaires en les x_k . Les mêmes combinaisons linéaires en X_k définissent une projection $\pi : k^n \rightarrow k^m$. La restriction p de π à V est une application $p : V \rightarrow k^m$ qui reflète l'extension entière $A' = k[z_1, \dots, z_m] \subset k[x_1, \dots, x_n] = A$.

A montrer :

1. π est surjectif,
2. Les fibres de π sont finies.

Pour montrer 1. on fixe $Q = (b_1, \dots, b_m) \in k^m$ et soit $\mathfrak{m}' \in A'$ l'idéal maximal correspondant. Alors, par 6.2.1 il y a un idéal maximal $\mathfrak{m} \in A$ tel que $\mathfrak{m} \cap A' = \mathfrak{m}'$. Par le "Nullstellensatz" l'idéal \mathfrak{m} est l'idéal d'un point $P \in V$ qui, par construction, s'applique à Q .

Pour montrer 2. il suffit de remarquer que les $x_i \in A$ étant entiers sur A' satisfont une équation polynômiale avec coefficients dans A' . Si dans une de ces équations on substitue $z_j = b_j$ on ne trouve qu'un nombre fini de solutions pour la coordonnée x_i d'un point qui est envoyé sur P . Donc il n'y a qu'un nombre fini de points dans la fibre de P . ■

Chapitre 7. Anneaux de valuations discrète

§ 1. Notions de base

On commence avec un corps K muni d'une valuation discrète :

1.1. Définition.

1. Une application **surjective**

$$v : K \setminus \{0\} \rightarrow \mathbb{Z}$$

est une **valuation discrète** si

- a. $\forall a, b \in K \setminus \{0\}, v(ab) = v(a) + v(b)$
 - b. $\forall a, b \in K \setminus \{0\}, v(a \pm b) \geq \min\{v(a), v(b)\}$.
2. L'anneau associé $A = 0 \cup \{x \in K ; v(x) \geq 0\}$ est l'**anneau de valuation discrète** associé.

Remarques. Les propriétés de v garantissent que A est un anneau avec 1. En effet, $v(1) = v(1 \cdot 1) = v(1) + v(1)$ implique que $v(1) = 0$ et donc $1 \in A$. Plus généralement, si u est inversible dans A , alors $v(u) + v(u^{-1}) = v(1) = 0$ entraîne que $v(u) = 0$. Inversement, si $v(u) = 0$, $u^{-1} \in A$ et donc u est inversible dans A .

Puisque $v(ab) = v(a) + v(b)$, l'image $v(K \setminus \{0\})$ est un sous-groupe de \mathbb{Z} et donc engendré par disons $v_0 \in \mathbb{N}$ avec $v(t) = v_0$. Si $x \in A$ avec $v(x) = nv_0$, pour l'élément $u = xt^{-n} \in k$ on a $v(u) = v(x) - nv_0 = 0$ et donc u est inversible dans A :

$$x = ut^n$$

et c'est une écriture unique. Donc A est un anneau factoriel et donc intégralement clos. De plus, les éléments non-inversibles forment l'idéal $\mathfrak{m} = (t)$ qui est forcément maximal : (A, \mathfrak{m}) est un anneau local. Puisqu'un idéal non-nul de A est engendré par t^N , l'anneau est aussi noethérien.

1.2. Exemples.

1. Soit p un nombre premier. L'application $v_p : \mathbb{Q} \rightarrow \mathbb{Z}$ est donnée par la méthode suivante : on écrit une fraction $a/b = p^n(a'/b')$, où a' et b' sont sans diviseurs p^a . Alors $v_p(a/b) = n$ et on vérifie que c'est une valuation discrète. L'anneau correspondant est l'anneau $\mathbb{Z}_{(p)}$ (\mathbb{Z} localisé en (p)).
2. On vérifie que $d : k(X) \rightarrow \mathbb{Z}, d(f/g) = \deg(f) - \deg(g)$ n'est PAS une valuation discrète. Mais si on fixe $F \in k[X]$ irréductible on peut définir une valuation discrète $v_F : k(X) \rightarrow \mathbb{Z}$ comme dans l'exemple précédent.
3. Soit $k((T))$ le corps des séries de Laurent formelles $a_k T^k + a_{k+1} T^{k+1} + \dots +$ où k peut être négatif. On pose $v(a_k T^k + a_{k+1} T^{k+1} + \dots) = k$. L'anneau correspondant est $k[[T]]$.

§ 2. Caractérisation

2.1. Lemme. Soit (A, \mathfrak{m}) un anneau local intègre noëthérien tel que \mathfrak{m} est principal, disons $\mathfrak{m} = (t)$. Alors A est un anneau de valuation discrète.

Démonstration. Un élément $x \in A$ est inversible si et seulement si $x \in A \setminus \mathfrak{m}$. Si $x \in \mathfrak{m}$ on écrit $x = tx_1 = t^2x_2 = \dots$ et on note que cela doit terminer :

1. Supposons que $(y) = (ty)$, $y \neq 0$. Donc $\exists a \in A$ tel que $y = aty \Rightarrow (at - 1)y = 0$ et donc $at = 1$ car A est intègre, contradiction.
2. Il résulte une chaîne stricte $(x) \subset (x_1) \subset (x_2) \cdots$ qui se termine car A est noëthérien.

Conclusion : chaque $x \in \mathfrak{m}$ s'écrit de manière unique $x = ut^n$, avec u inversible et donc chaque élément non-nulle x du corps de fractions K de A s'écrit $\{\text{unité de } A\} \cdot t^k$, $k \in \mathbb{Z}$ avec k déterminé par x et on pose $v(x) = k$. Clairement $v(x) \geq 0$ si et seulement si $x \in A$ et $v(xy) = v(x) + v(y)$. Supposons maintenant que $y \in K$, $y \neq 0$, et que $x \in K$ est tel que $v(x) \geq v(y)$. Alors $v(xy^{-1}) = v(x) - v(y) \geq 0$ et donc $xy^{-1} \in A$. Donc $(x \pm y)y^{-1} = xy^{-1} \pm 1 \in A \Rightarrow v((x \pm y)y^{-1}) \geq 0$ et $v(x \pm y) \geq v(y)$ ce qui montre l'autre propriété souhaitée pour une valuation discrète. ■

2.2. Caractérisation. Soit A un anneau intègre. Alors A est un anneau de valuation discrète si et seulement si A est normal, noëthérien et il n'y a qu'un seul idéal premier \mathfrak{m} différent de 0.

Démonstration. On a déjà vu qu'un anneau de valuation discrète est normal, noëthérien et local avec idéal maximal non-nul. Pour la réciproque, grâce au lemme précédent, il suffit de montrer que \mathfrak{m} est principal.

Montrons d'abord que $\mathfrak{m} \neq \mathfrak{m}^2$. Sinon, on aurait un idéal $I \neq 0$ avec $I\mathfrak{m} = \mathfrak{m}$, mais I est un A -module de type fini car A est noëthérien et donc I serait 0 à cause du lemme de Nakayama 2.3.3.

Ensuite, montrons que $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ engendre \mathfrak{m} . Sinon, le A -module $M := \mathfrak{m}/(x)$ serait non-nulle et aurait des assassins. L'assassin 0 est exclu car M ne contient pas de sous-module isomorphe à A . Donc l'assassin de M est \mathfrak{m} et il y a $y \in \mathfrak{m} \setminus (x)$ tel que $y\mathfrak{m} \subset (x)$.

Soit K le corps de fractions de A . L'élément $z = y/x \in K$ n'appartient pas à A puisque $y \in \mathfrak{m} \setminus (x)$. D'autre part, $y\mathfrak{m} \subset (x)$ implique que $I = (y/x)\mathfrak{m}$ est un idéal de A . Si $I = A$, alors $\exists y' \in \mathfrak{m}$ tel que $(yy')/x = 1$ et donc $x = yy' \in \mathfrak{m}^2$. Ce n'étant pas le cas on a $I \neq A$ et $I \subset \mathfrak{m}$. Mais dans ce cas, la multiplication avec $z = y/x$ envoie \mathfrak{m} , un A -module de type fini en \mathfrak{m} et l'astuce du déterminant 2.3.1 implique qu'il y a un polynôme unitaire $P[T] \in A[T]$ tel que $P(z)\mathfrak{m} = 0$ et donc $P(z) = 0$ car A est intègre. A étant intégralement clos, $z = (y/x) \in A$ et donc $y \in (x)$, contraire à l'hypothèse que $y \in \mathfrak{m} \setminus (x)$.

Finalement on a arrivé à une contradiction et donc $M = 0$, c.à.d. $\mathfrak{m} = (x)$. ■

§ 3. Applications

Soit A un anneau intègre et $K = Q(A)$ son corps de fractions, $x \in K$ quelconque.

3.1. Définition. L'idéal des dénominateurs de x est

$$\begin{aligned} \partial(x) &= \{b \in A ; bx \in A\} \\ &= \{b \in A ; \exists a \in A, x = a/b\} \cup \{0\}. \end{aligned}$$

Voici un énoncé utile :

3.2. Lemme. *L'idéal $\partial(x)$ est un idéal propre si et seulement si $x \in K \setminus A$. Soit \mathfrak{m} un idéal maximal contenant $\partial(x)$. Alors $x \notin A_{\mathfrak{m}}$.*

Démonstration. On a : $x \notin A_{\mathfrak{m}}$ si et seulement si pour toute écriture $x = a/b$ on a $b \in \mathfrak{m}$, c.à.d. $\partial(x) \subset \mathfrak{m}$. ■

On a d'abord besoin du fait que A est l'intersection dans K des localisations en tous les idéaux premiers (ou en tous les idéaux maximaux) :

3.3. Lemme. *Pour A intègre $A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$ (\mathfrak{p} , resp. \mathfrak{m} parcourt les idéaux premiers, resp. maximaux).*

Démonstration. Par le lemme ci-dessus, l'idéal $\partial(x)$ des dénominateurs de x est un idéal propre si et seulement si $x \in K \setminus A$. C'est le cas si et seulement si $\partial(x)$ est contenu dans un idéal maximal \mathfrak{m} de A . On a aussi que $x \notin A_{\mathfrak{m}}$. Donc $x \in K \setminus A$ si et seulement s'il y a un idéal maximal \mathfrak{m} de A tel que $x \notin A_{\mathfrak{m}}$. ■

Ensuite on verra que la normalité est une propriété locale :

3.4. Proposition. *Pour un anneau intègre A , les propriétés suivantes sont équivalentes :*

1. A est normal,
2. $A_{\mathfrak{p}}$ est normal pour un idéal premier \mathfrak{p} quelconque de A ,
3. $A_{\mathfrak{m}}$ est normal pour un idéal maximal \mathfrak{m} quelconque de A ,

Démonstration.

1. \Rightarrow 2. On montre que plus généralement que $S^{-1}A$ est normale pour $S \subset A$ multiplicativement stable. Soit $x \in K = Q(A)$, le corps des fractions de A entier sur $S^{-1}A$ et soit

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad a_i = \frac{b_i}{c_i} \in K, \quad c_i \in S$$

une équation de dépendance intégrale. On la multiplie avec $(c_1 \cdots c_n)^n$ pour obtenir une relation de dépendance intégrale sur A de $(c_1 \cdots c_n)x = y$. Donc $y \in A$ et $x \in S^{-1}A$.

2. \Rightarrow 3. Clair

3. \Rightarrow 1. Si $x \in K$ est A -entier, du fait que $A \subset A_{\mathfrak{m}}$ il s'ensuit que x est $A_{\mathfrak{m}}$ -entier et donc $x \in A_{\mathfrak{m}}$. Par le lemme précédent, $x \in A$. ■

3.5. Lemme technique. *Soit A un anneau intègre, normal et noëthérien et $x \in A$ non-nul. Un assassin non-nul de $A/(x)$ est un idéal premier, minimal parmi les idéaux non-nuls de A .*

Démonstration.

Soit \mathfrak{p} un assassin de A/I où $I = (x)$. On localise en \mathfrak{p} . Avec $J = (x) \cdot A_{\mathfrak{p}}$ on a $B = A_{\mathfrak{p}}/J = (A/(x))_{\mathfrak{p}}$. Si $\mathfrak{p} \in \text{Ass}(A)$ est l'annulateur de la classe de a dans A/I , on vérifie tout de suite que l'annulateur de la classe de $a/1$ dans B est $\mathfrak{p}A_{\mathfrak{p}}$ et donc $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$ est un assassin de $A_{\mathfrak{p}}/J$. Il suffit alors de montrer que \mathfrak{m} est minimal.

Donc on peut supposer que (A, \mathfrak{m}) est local, noethérien et normal et que \mathfrak{m} est assasin non-nul de $A/(x)$. Il y a donc $y \in A \setminus (x)$ tel que $y\mathfrak{m} \subset (x)$. Soit K le corps de fractions de A . L'élément $z = y/x \in K$ n'appartient pas à A puisque $y \in A \setminus (x)$. D'autre part, $y\mathfrak{m} \subset (x)$ implique que $I = (y/x)\mathfrak{m}$ est un idéal de A . Si $I \neq A$, alors $I \subset \mathfrak{m}$. Dans ce cas, la multiplication avec $z = y/x$ envoie \mathfrak{m} , un A -module de type fini en \mathfrak{m} et l'astuce du déterminant 2.3.1 implique qu'il y a un polynôme unitaire $P[T] \in A[T]$ tel que $P(z)\mathfrak{m} = 0$ et donc $P(z) = 0$ car A est intègre. A étant intégralement clos, $z = (y/x) \in A$ et donc $y \in (x)$, contraire à l'hypothèse que $y \in A \setminus (x)$. Donc $I = A$ et $1 = t(y/x)$, $t \in \mathfrak{m}$ et donc $\mathfrak{m} = \mathfrak{m}t(y/x) = It = At$.

Par le lemme 7.2.1 A est un anneau de valuation discrète et par 7.2.2 A n'a qu'un idéal premier outre que 0 et c'est \mathfrak{m} . Forcément \mathfrak{m} est minimal et non-nul. ■

Voici le résultat principal :

3.6. Théorème. *Un anneau A intègre, normal et noethérien est l'intersection des anneaux $A_{\mathfrak{p}}$, \mathfrak{p} premier, non-nul et minimal. Chacun de tels anneaux est un anneau de valuation discrète.*

Démonstration.

1. On sait que $A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$ où \mathfrak{p} parcourt tous les idéaux premiers. Il suffit donc de montrer que si $x = a/b \in K \setminus A$, alors on peut trouver un idéal premier \mathfrak{p} minimal, tel que x n'est pas contenu dans $A_{\mathfrak{p}}$. Regardons

$$\begin{aligned} \partial(x) &= \{y \in A ; yx \in A\} \\ &= \{y \in A ; ya \in (b)\} \\ &= ((b) : a) = \text{Ann}_A(\bar{a}), \quad \bar{a} \equiv a \pmod{b} \end{aligned}$$

et supposons que $x \notin A$, i.e. $\bar{a} \neq 0$.

Dans ce cas $\partial(x) \neq A$. Considérons l'ensemble d'idéaux

$$\Sigma = \{J \supset \partial(x) ; J = \text{Ann}_A(y), \quad y \neq 0, y \in A/(b)\}.$$

Cet ensemble étant non-vide possède un élément maximal \mathfrak{p} . Par 5.4.4 un tel idéal est premier et donc $\mathfrak{p} \in \text{Ass}(A/(b))$. Le lemme technique implique que \mathfrak{p} est un idéal premier minimal non-nul de A . Puisque \mathfrak{p} contient $\partial(x)$, $x \notin A_{\mathfrak{p}}$ par 7.3.2.

2. Les idéaux premiers de $A_{\mathfrak{p}}$ sont en correspondance biunivoque avec les idéaux premiers de A contenus dans \mathfrak{p} . Donc, si \mathfrak{p} est minimal $A_{\mathfrak{p}}$ n'a que deux idéaux premiers : 0 et l'idéal maximal. Donc, par 7.2.2 $A_{\mathfrak{p}}$ est un anneau de valuation discrète. ■

Chapitre 8. Dimension

§ 1. Degré de transcendance

Soit $L|K$ une extension de corps. On introduit les notions suivantes :

1.1. Définition.

- i. Un ensemble $\{u_1, \dots, u_n\}$ d'éléments de L est **algébriquement indépendant** s'il n'existe aucune relation polynômiale entre les u_j .
- ii. Un ensemble $\{u_1, \dots, u_n\}$ d'éléments de L est **générateur** si l'extension $L|K(u_1, \dots, u_m)$ est algébrique.
- iii. Un tel ensemble est une **base de transcendance** s'il est à la fois générateur et algébriquement indépendant.

1.2. Théorème-Définition. Soit $L|K$ une extension engendrée par un nombre fini d'éléments de L . Alors il existe une base de transcendance (finie) et chaque base de transcendance a le même nombre $\text{trdeg}_K L$ d'éléments. Ce nombre est le degré de transcendance de $L|K$.

Démonstration. Si $L|K$ est algébrique l'ensemble vide est une base de transcendance et on peut donc supposer que $L|K$ n'est pas algébrique. On trouve au moins un élément $u_1 \in L$ transcendant sur K . Si $L|K(u_1)$ est algébrique on a fini. Sinon on peut continuer en rajoutant un élément u_2 qui est transcendant sur $K(u_1)$. Ce procédé s'arrête après un nombre fini de pas et donne la base de transcendance cherchée.

Pour montrer que $\text{trdeg}_K L$ est bien défini, il suffit de montrer:

1.3. Lemme. Soit $\{u_1, \dots, u_m\}$ algébriquement indépendant et soit $\{w_1, \dots, w_n\}$ génératrice dans L . On peut trouver m éléments parmi les w_j qu'on peut remplacer par $\{u_1, \dots, u_m\}$ t.q. le nouvel ensemble est toujours génératrice dans L . En particulier $m \leq n$.

La démonstration se fait comme dans l'algèbre linéaire. On utilise une récurrence sur m . Le cas $m = 0$ est trivial. Par récurrence on a $n \geq m - 1$ et on peut remplacer $m - 1$ éléments de $\{w_1, \dots, w_n\}$ par $\{u_1, \dots, u_{m-1}\}$ t.q. on obtienne un ensemble S qui soit générateur. L'extension $L|K(S)$ est algébrique et donc $u_m \in L$ est racine d'un polynôme à coefficients dans $K(S)$. On prend le sous-ensemble $T \subset S$ minimal tel que u_m est algébrique sur $k(T)$. Supposons que $F(u_1, \dots, u_m, \dots, w_j \dots) = 0$ est la relation de dépendance. Il y a au moins un w_k dans T , car les u_1, \dots, u_m sont algébriquement indépendantes. On remplace w_k par u_m . Soit T' le nouveau système. La variable w_k figure effectivement en F (minimalité de T) et donc w_k est algébriquement dépendant de T' . Soit S' le système qu'on obtient en remplaçant w_k par u_m dans S . Alors S' contient T' et w_k est algébriquement dépendant de S' . Aussi $L|K(S')$ est donc toujours une extension algébrique car $\{S', w_k\} = \{S, u_m\}$ et $L|K(S, u_m)$ ainsi que $K(S', w_k)|K(S')$ sont des extensions algébriques. ■

1.4. Définition. Soit B anneau et M un B -module. Une **dérivation** est une application $d : B \rightarrow M$ qui satisfait la règle de Leibniz :

$$\forall b, b' \in B \quad d(bb') = bd(b') + b'd(b).$$

Si de plus B est une A -algèbre et d est linéaire on dit que d est une A -dérivation. L'ensemble de telles dérivations $\text{Der}_A(B, M)$ est un B -module avec multiplication donnée par

$$\forall b \in B, d \in \text{Der}_A(B, M), \quad b \cdot d : y \mapsto b \cdot d(y).$$

1.5. Exemples.

1. Si $A = k$ un corps et $B = M = k(X)$, alors la dérivation par rapport à X est une k -dérivation. Plus généralement, si $B = M = k(X_1, \dots, X_n)$, la dérivation partielle par rapport à X_i , disons ∂_i est une k -dérivation de B . Une k -dérivation d de B est uniquement spécifiée par les valeurs $d(X_i) = d_i \in k(X_1, \dots, X_n)$ car pour un polynôme P , on a $d(P) = \sum_i \frac{\partial P}{\partial X_i} d(X_i)$ et pour une fonction rationnelle $d(P/Q) = 1/Q^2(Pd(Q) - Qd(P))$. Il s'en suit que

$$\text{Der}_k(k(X_1, \dots, X_n), k(X_1, \dots, X_n))$$

est un $k(X_1, \dots, X_n)$ -espace vectoriel engendré par les ∂_i et donc de dimension n .

2. Pour une A -algèbre B , le module $\Omega_{B/A}$ des **différentielles kähleriennes** est le quotient du B -module libre engendré par les symboles df , $f \in B$ modulo les relations suivantes :

$$\begin{aligned} \forall f, g \in B \quad d(fg) &= fd(g) + gd(f) \text{ (Leibniz)} \\ \forall a, b \in A, f, g \in B \quad d(af + bg) &= adf + bdg \text{ (A-linéarité)}. \end{aligned}$$

L'application $d : B \rightarrow \Omega_{B/A}$, $b \mapsto db$ est une A -dérivation. Chaque A -dérivation $e : B \rightarrow M$ est induite par une unique application B -linéaire $e' : \Omega_{B/A} \rightarrow M$ telle que $e = e' \circ d$ et on a

$$\text{Der}_A(B, M) = \text{Hom}_B(\Omega_{B/A}, M).$$

En particulier $\text{Der}_A(B, B)$ est le dual de $\Omega_{B/A}$ en tant que B -module (dualité entre dérivations et différentielles).

1.6. Théorème. Soit K un corps de caractéristique 0 et $K \subset L$ une extension de corps engendrée par un nombre fini d'éléments. Alors $\text{Der}_K(L, L)$ est un L -espace de dimension $= \text{trdeg}_K L$.

Démonstration. Il y a n éléments $x_1, \dots, x_n \in L$, algébriquement indépendants / K tels que $L' = K(x_1, \dots, x_n) \subset L$ est une extension algébrique. Par l'exemple 1.5.1 ci-dessus, $\text{Der}_K(L', L')$ est un L' -espace vectoriel de dimension n . Il suffit donc de montrer que chaque K -dérivation d de L' s'étend de manière unique à une K -dérivation de L . Puisque la caractéristique de K est nul, par le Théorème 6.3.4 on a $L = L'(y)$. Soit $F(X) \in L'[X]$ son polynôme minimal. Puisque $F(y) = 0$ on a forcément $0 = d(F(y)) = (dF)(y) + F'(y)d(y)$ où $(dF)[X]$ est le polynôme obtenu en dérivant les coefficients de F par rapport à d . Puisque $F(X)$ est sans racines multiples dans une clôture algébrique de K , $F'(y) \neq 0$ et la formule précédente détermine dy de façon unique. Finalement on vérifie que cette détermination donne une dérivation. ■

1.7. Remarque. En caractéristique quelconque le théorème n'est pas vrai. Voir [Ma, §26] pour ce cas.

§ 2. Dimension d'une variété affine

On suppose que k est un corps algébriquement clos de caractéristique 0 et que $V \subset k^n$ est une variété affine irréductible avec idéal premier \mathfrak{p} . Pour $P \in k^n$, et $F \in k[X_1, \dots, X_n]$ soit $dF(P) : k^n \rightarrow k$ la forme k -linéaire donnée par $dF(P) = (\partial_1 F|_P, \dots, \partial_n F|_P)$. Alors le sous-espace linéaire de k^n :

$$U = \{Q \in k^n ; dF(P)(Q) = 0 \forall F \in \mathfrak{p}\}$$

définit l'espace tangent en P :

$$T_P V = P + U = P + \bigcap_{F \in \mathfrak{p}} \ker dF(P).$$

On montre :

2.1. Théorème. V contient un ouvert de Zariski non-vide U tel que $\forall P \in U$, $\dim T_P V$ est constant et égal à $\text{trdeg}_k k(V)$.

Démonstration. Soit $\mathfrak{p} = (f_1, \dots, f_m)$ et soit

$$J = \left(\frac{\partial f_i}{\partial X_j} \right) : k(V)^n \rightarrow k(V)^m$$

l'application jacobienne associée. On voit que :

$$\begin{aligned} \text{Der}_k(k(V), k(V)) &= \text{Der}_k(k[V], k(V)) \\ &= \{d \in \text{Der}_k(k[X_1, \dots, X_n], k(V)) ; d\mathfrak{p} = 0\} \\ &= \ker \{J : k(V)^n \rightarrow k(V)^m\} \end{aligned}$$

et donc

$$\text{trdeg}_k k(V) = \dim \ker(J) = n - \text{rang} J.$$

Soit r le rang de J sur $k(V)$. Par l'algèbre linéaire il y a deux matrices inversibles à coefficients dans $k(V)$, disons A, B tels que $AJB = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$. Soit $A = A'/a$, $B = B'/b$ avec $a, b \in k[V]$ et A', B' à coefficients dans $k[V]$. Soit U l'ouvert de Zariski $\{P \in V ; \det(A') \det(B') ab \neq 0\}$, alors, A et B sont définies et inversibles aux points $P \in U$. L'application $J(P) : k^n \rightarrow k^m$ est de rang $= r$ sur cet ouvert et $\dim T_P = n - r$ est donc constante sur U . ■

2.2. Définition. La dimension de V est $\dim V = \text{trdeg}_k k(V)$. Si $P \in V$ tel que $\dim T_P V = \dim V$, on dit que P est non-singulier.

§ 3. Dimension de Krull

3.1. Définition. Soit A un anneau commutatif. Alors

1. La **dimension** de A , $\dim(A)$ est la longueur maximale k d'une chaîne d'idéaux premiers $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_k$, $\forall i, \mathfrak{p}_i \neq \mathfrak{p}_{i+1}$.
2. La **hauteur** $\text{ht}(\mathfrak{p})$ d'un idéal premier \mathfrak{p} est la longueur maximale de telles chaînes terminant à $\mathfrak{p} = \mathfrak{p}_k$. En particulier, pour un idéal maximal \mathfrak{m} , on a $\text{ht}(\mathfrak{m}) = \dim A$.

3.2. Exemples.

1. $\dim \mathbb{Z} = 1$,
2. $\dim k[X] = 1$, k corps,
3. $\dim k = 0$, k corps.
4. Soit k algébriquement clos, $V = V(\mathfrak{p}) \subset k^n$ une variété irréductible associée à un idéal premier $\mathfrak{p} \subset k[X_1, \dots, X_n]$. Alors par 5.2.4 $\text{ht} \mathfrak{p}$ est le maximum des longueurs r d'une chaîne de sous-variétés irréductibles

$$V = V_0 \subset V_1 \cdots \subset V_r = k^n.$$

De même, si $W \subset V$ est une sous-variété irréductible de V correspondant à un idéal premier $\mathfrak{q} \subset k[V]$, la hauteur de \mathfrak{q} est le maximum des longueurs r d'une chaîne de variétés irréductibles

$$W = W_0 \subset W_1 \cdots \subset W_r = V.$$

3.3. Proposition. *Pour un corps quelconque $\dim k[X_1, \dots, X_n] = n$ et chaque chaîne maximale stricte d'idéaux premiers (dans le sens qu'on ne peut ni insérer d'idéaux premiers ni prolonger la chaîne dans une des deux directions) est de longueur n .*

Démonstration. Récurrence sur n , le cas $n = 1$ étant l'exemple 3.2.2.

Soit $0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_m$ une chaîne maximale d'idéaux premiers distincts. Soit $f \in \mathfrak{p}_1$ non-nul. On peut supposer que f est irréductible (car \mathfrak{p}_1 est premier) et que l'idéal premier (f) coïncide avec \mathfrak{p}_1 (sinon il y aura une chaîne de longueur $m + 1$). Dans $A = k[X_1, \dots, X_n]/(f)$ les X_i sont algébriquement dépendants et f donne une relation de dépendance. Par le lemme 6.3.2 on peut supposer qu'en remplaçant les $n - 1$ premières variables f est unitaire en X_n et donc donne une relation de dépendance intégrale pour la classe de X_n : $X_n^k + a_1(X_1, \dots, X_{n-1}) + \cdots + a_k(X_1, \dots, X_{n-1}) \in (f)$. cela signifie que X_n est $B = k[X_1, \dots, X_{n-1}, f]$ -entier et donc $k[X_1, \dots, X_n]$ est entier sur B . On intersecte la chaîne avec B . Par 6.2.2 et 6.2.3 la longueur reste la même et la chaîne reste maximale. Dans $B/\mathfrak{p}_1 = B/(f) = k[X_1, \dots, X_{n-1}]$ la chaîne induite est maximale et sa longueur est $m - 1$. Par récurrence, $m - 1 = n - 1$ et donc $m = n$. ■

3.4. Corollaire. *On a*

$$\dim k[X_1, \dots, X_n] = \text{trdeg}_k k(X_1, \dots, X_n) = \dim k^n.$$

On va étendre ce Corollaire au cas d'une variété quelconque :

3.5. Théorème. *Soit $V = V(\mathfrak{p}) \subset k^n$ une variété irréductible. Alors $\dim V = \dim k[V]$.*

Démonstration.

D'abord, si $k[V] = k[X_1, \dots, X_n]/\mathfrak{p}$, \mathfrak{p} idéal premier, on peut appliquer le Corollaire 6.3.3. On sait donc qu'après un changement des coordonnées $k[V]$ est $k[X_1, \dots, X_m]$ -entier et que $\text{trdeg}_k(V) = \dim k[X_1, \dots, X_m] = m$. Par "Going up" (6.2.3) on a l'inégalité $\dim k[V] \geq m$. Il suffit de montrer l'inégalité opposée. Cela découle de l'"Incompatibilité" (6.2.2)

3.6. Corollaire. *Soit $V = V(\mathfrak{p}) \subset k^n$ une variété irréductible. Alors $\dim k[V] + \text{ht}(\mathfrak{p}) = n$.*

Démonstration. On considère une chaîne d'idéaux premiers de $k[V]$ de longueur $d = \dim k[V]$. Cela donne une chaîne d'idéaux de $k[X_1, \dots, X_n]$ de longueur d qui commence avec \mathfrak{p} . On la combine avec une chaîne de longueur $\text{ht}(\mathfrak{p})$ terminant à \mathfrak{p} . La chaîne qui résulte est une chaîne maximal de $k[X_1, \dots, X_n]$ (dans le sens de la proposition 3.3) et donc de longueur $n = \dim k[V] + \text{ht}(\mathfrak{p})$. ■

3.7. Exemple. soit $V = V(\mathfrak{p}) \subset k^n$ une variété algébrique irréductible et $W = V(\mathfrak{q}) \subset V$ une sous-variété irréductible. On a que $\dim \mathcal{O}_W(V)$ est la hauteur de l'idéal $\bar{\mathfrak{q}} \subset k[V]$, image de \mathfrak{q} dans $k[V] = k[X_1, \dots, X_n]/\mathfrak{p}$. Donc $\dim \mathcal{O}_W(V) = \text{ht} \bar{\mathfrak{q}} = \dim k[V] - \dim k[W] = \dim V - \dim W$. En particulier, la dimension de l'anneau locale $\mathcal{O}_x(V)$ est toujours égale à $\dim V$.

§ 4. Les théorèmes de Krull

Rappel. Pour un anneau noethérien et $I \subset A$ un idéal quelconque, on a une décomposition primaire $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ et les racines $\mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$ sont uniquement déterminés par I : ce sont les assassins de A/I . Celles qui sont minimales (par rapport à l'inclusion) sont appelées les **diviseurs premiers minimaux de I** . Dans le cas géométrique ($A = k[X_1, \dots, X_n]$), ces idéaux donnent les composantes irréductibles de la variété $V(I)$.

Pour un anneau A noethérien et normal, et un idéal principal $I = (f)$ de A , le "lemme technique" 7.3.5 dit que chaque assassin \mathfrak{p} de A/I est un idéal premier, minimal parmi les idéaux non-nuls c.à.d. $\text{ht}(\mathfrak{p}) = 1$. Conclusion ; les diviseurs premiers minimaux de I ont tous hauteur = 1. Dans le cas général on a :

4.1. Proposition. Soit (A, \mathfrak{m}) un anneau local et noethérien. Soit $I = (f)$ un idéal principal de A , $I \neq A$ telle que \mathfrak{m} soit un diviseur premier minimal de I . Pour un idéal premier $\mathfrak{p} \neq \mathfrak{m}$ on a $\text{ht}(\mathfrak{p}) = 0$ (et donc $\text{ht}(\mathfrak{m}) \leq 1$).

Démonstration. Soit $i : A \rightarrow A_{\mathfrak{p}}$ la localisation de A et définissons

$$\mathfrak{p}^{(k)} = i^{-1} \mathfrak{p}^k A_{\mathfrak{p}}.$$

Considérons la chaîne

$$(f) + \mathfrak{p}^{(1)} \supset (f) + \mathfrak{p}^{(2)} \supset \dots$$

Puisque \mathfrak{m} est un diviseur minimal de (f) , l'anneau $B = A/(f)$ n'a qu'un seul idéal premier, \mathfrak{n} , l'image de \mathfrak{m} . Il s'ensuit que $\mathfrak{n} = \sqrt{0}$, et chaque idéal $I \neq (1)$ de B étant finiment engendré est donc nilpotent. Donc la chaîne ci-dessus se stabilise donc et $\exists n \in \mathbb{N}$ avec $(f) + \mathfrak{p}^{(n)} = (f) + \mathfrak{p}^{(n+1)}$. Si on écrit $x \in \mathfrak{p}^{(n)}$ sous la forme $x = af + y$, $a \in A$, $y \in \mathfrak{p}^{(n+1)}$ on a $af \in \mathfrak{p}^{(n)}$. Puisque $\mathfrak{p} \subset \mathfrak{m}$ et \mathfrak{m} est minimal parmi les idéaux premiers contenant f , on a $f \notin \mathfrak{p}$. Par conséquent $i(a) = (af)/f \in \mathfrak{p}^n A_{\mathfrak{p}}$ et donc $a \in \mathfrak{p}^{(n)}$ d'après la définition de $\mathfrak{p}^{(n)}$. Il s'en suit que

$$\mathfrak{p}^{(n)} = f\mathfrak{p}^{(n)} + \mathfrak{p}^{(n+1)}$$

et donc $\mathfrak{p}^{(n)} = \mathfrak{p}^{(n+1)}$ par Nakayama, car $f \in \mathfrak{m}$. Dans $A_{\mathfrak{p}}$ on a $\mathfrak{p}^n A_{\mathfrak{p}} = \mathfrak{p}^{n+1} A_{\mathfrak{p}}$ et donc $\mathfrak{p}^n A_{\mathfrak{p}} = (0)$ de nouveau par Nakayama. L'idéal maximal $\mathfrak{m}' = \mathfrak{p} A_{\mathfrak{p}}$ de $A_{\mathfrak{p}}$ étant nilpotent, on a bien $\text{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}} = 0$ (si $x \in \mathfrak{m}$, alors $0 = x^n$ implique x est contenu dans chaque idéal premier \mathfrak{p}' et en particulier, si $\mathfrak{p}' \subset \mathfrak{m}'$ est non-nul $\mathfrak{p}' = \mathfrak{m}'$). ■

4.2. Corollaire. Soit A un anneau noethérien. Soit $I = (f)$ un idéal propre de A avec \mathfrak{p} un diviseur premier minimal. Alors $\text{ht}(\mathfrak{p}) \leq 1$ et $\text{ht}(\mathfrak{p}) = 0$ implique que f est diviseur de zéro.

Démonstration. Le lemme précédent qui implique que pour un anneau local (A, \mathfrak{m}) tel que \mathfrak{m} est un diviseur minimal d'un élément non-inversible de A , on a $\text{ht}(\mathfrak{m}) \leq 1$. En général, on localise en \mathfrak{p} et on note que l'image de f dans $A_{\mathfrak{p}}$ est non-inversible et que \mathfrak{p} et $\mathfrak{p}A_{\mathfrak{p}}$ ont même hauteur. Le cas local donne donc l'inégalité.

Ensuite traitons le cas $\text{ht}(\mathfrak{p}) = 0$. Un tel idéal \mathfrak{p} par définition est un idéal premier minimal. Rappelons (5.2.2) qu'un élément d'un idéal minimal dans un anneau noethérien est toujours diviseur de zéro. Donc, si f admet \mathfrak{p} comme diviseur premier minimal, f doit être diviseur de zéro. ■

4.3. Corollaire. *Soit A un noethérien et soit $\mathfrak{p}_1 \subset \mathfrak{p}_2$ une chaîne stricte d'idéaux premiers. On suppose de plus qu'il y a des idéaux premiers \mathfrak{q}_i de A tels que $\mathfrak{p}_2 \not\subset \mathfrak{q}_i$, $i = 1, \dots, s$. Si $\dim A_{\mathfrak{p}_2}/\mathfrak{p}_1 A_{\mathfrak{p}_2} \geq 2$, il y a un idéal premier \mathfrak{p} dans une chaîne stricte $\mathfrak{p}_1 \subset \mathfrak{p} \subset \mathfrak{p}_2$ telle que $\mathfrak{p} \not\subset \mathfrak{q}_i$, $i = 1, \dots, s$*

Démonstration. Par la Proposition 1.4.5 il y a $x \in \mathfrak{p}_2$ tels que $x \notin \mathfrak{q}_i$, $i = 1, \dots, s$, $x \notin \mathfrak{p}_1$. Un diviseur premier minimal de $x A_{\mathfrak{p}_2} + \mathfrak{p}_1 R_{\mathfrak{p}_2}$ dans l'anneau $A_{\mathfrak{p}_2}$ est de la forme $\mathfrak{p} A_{\mathfrak{p}_2}$ avec $\mathfrak{p} \subset A$ premier et $\mathfrak{p}_1 \subset \mathfrak{p} \subset \mathfrak{p}_2$. Par le Corollaire, $\text{ht}(\mathfrak{p}/\mathfrak{p}_1) \leq 1$ et par hypothèse $\dim A_{\mathfrak{p}_2}/\mathfrak{p}_1 A_{\mathfrak{p}_2} \geq 2$, on ne peut pas avoir $\mathfrak{p} = \mathfrak{p}_2$. Aussi, $\mathfrak{p} \not\subset \mathfrak{q}_i$ et $\mathfrak{p} \neq \mathfrak{p}_1$ car $x \in \mathfrak{p}$ (par construction), $x \notin \mathfrak{q}_i$, $x \notin \mathfrak{p}_1$. ■

4.4. Théorème. *Soit A un anneau noethérien. Soit $I = (f_1, \dots, f_m)$ un idéal propre de A avec \mathfrak{p} un diviseur premier minimal. Alors $\text{ht}(\mathfrak{p}) \leq m$.*

Démonstration. Par récurrence sur m , le cas $m = 1$ étant déjà montré.

Soient \mathfrak{q}_j , $j = 1, \dots, s$ les diviseurs premiers minimaux de (f_1, \dots, f_{m-1}) . Par récurrence $\text{ht}(\mathfrak{q}_i) \leq m - 1$. Soit maintenant

$$(*) \quad \mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_l$$

une chaîne d'idéaux premiers de longueur $l \geq 2$ (si une telle chaîne n'existait pas, on pourrait terminer). On peut supposer que \mathfrak{p} n'est pas contenu dans $\bigcup \mathfrak{q}_i$. Sinon \mathfrak{p} serait contenue dans un des \mathfrak{q}_i et $\text{ht}(\mathfrak{p}) \leq m - 1$.

Appliquant le Corollaire précédent plusieurs fois, on peut supposer que la chaîne $(*)$ satisfait $\mathfrak{p}_{l-1} \not\subset \bigcup \mathfrak{q}_i$. Soit

$$I' = (f_1, \dots, f_{m-1}), \quad B = A/I'.$$

Puisque l'image \mathfrak{p}' de \mathfrak{p} dans B est un diviseur minimal de l'image de f_m , on a $\text{ht}(\mathfrak{p}') \leq 1$.

De $\mathfrak{p}_{l-1} \not\subset \mathfrak{q}_i$ et $(f_1, \dots, f_{m-1}) \subset \mathfrak{q}_i$ on déduit que dans B on a $\mathfrak{p}_{l-1}/I' \not\subset \mathfrak{q}_i/I'$. Puisque les seuls diviseurs possibles de \mathfrak{p}_{l-1}/I' contenue dans $\mathfrak{p}' = \mathfrak{p}/I'$ sont les \mathfrak{q}_i/I' il s'en suit que \mathfrak{p}' est un diviseur premier minimal de \mathfrak{p}_{l-1}/I' et donc que \mathfrak{p} est un diviseur minimal de $\mathfrak{p}_{l-1} + (f_1, \dots, f_{m-1})$. Dans A/\mathfrak{p}_{l-1} l'idéal $\mathfrak{p}/\mathfrak{p}_{l-1}$ est diviseur premier minimal d'un idéal engendré par $m - 1$ éléments. Donc $l - 1 \leq \text{ht}(\mathfrak{p}/\mathfrak{p}_{l-1}) \leq m - 1$ i.e. $l \leq m$ et $\text{ht}(\mathfrak{p}) \leq m$. ■

§ 5. Quelques applications

On a besoin d'une notion :

5.1. Définition. Soient A un anneau et M un A -module.

$$\mu(M) = \min_t \{Ax_1 + Ax_2 + \dots + Ax_t = M\}.$$

Pour un idéal maximal \mathfrak{m} d'un anneau A on pose

$$e(\mathfrak{m}) = \mu(\mathfrak{m}) \quad (\text{dimension d'immersion de } \mathfrak{m}).$$

5.2. Remarque. Pour un anneau local (A, \mathfrak{m}) , $k = A/\mathfrak{m}$ son corps résiduel, le lemme de Nakayama implique que pour un A -module de type fini on a $\mu(M) = \dim_k(M/\mathfrak{m}M)$. En particulier, pour A noethérien, on a

$$e(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

Une conséquence immédiate du théorème de Krull :

5.3. Lemme. Soit (A, \mathfrak{m}) anneau local et noethérien et \mathfrak{q} un idéal \mathfrak{m} -primaire. Alors

$$\mu(\mathfrak{q}) \geq \text{ht}(\mathfrak{m}) = \dim(A).$$

Nous voulons montrer qu'il y a un idéal \mathfrak{m} -primaire \mathfrak{q} avec un système de $d = \dim A$ générateurs. Un tel système s'appelle un **système de paramètres** de A .

Comme préparation nous montrons :

5.4. Lemme. Soit A un anneau noethérien, $J \subset I$ deux idéaux tel que $\hat{V}(I) = \hat{V}(J)$ et $\mu(I/J) = m$. Soient donnés des idéaux premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ tels que $I \not\subset \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_s$, Alors, $\exists x_1, \dots, x_m \in I$ tels que

1. $I = (x_1, \dots, x_m) + J$,
2. $x_i \notin \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_s$, $i = 1, \dots, m$.
3. Pour chaque idéal premier $\mathfrak{p} \supset (x_1, \dots, x_m)$ avec $\mathfrak{p} \not\supset I$, alors $\text{ht}(\mathfrak{p}) \geq m$.

Démonstration. On construit par récurrence $x_1, \dots, x_r \in I \setminus \bigcup_{i=1}^s \mathfrak{p}_i$ tels que leurs images dans I/J peuvent être complétés en un système minimal générateur pour I/J tel que si $\mathfrak{p} \supset (x_1, \dots, x_r)$ et $\mathfrak{p} \not\subset I$, alors $\text{ht}(\mathfrak{p}) \geq r$.

Pour $r = 0$ c'est clair. Supposons qu'on a déjà construit x_1, \dots, x_r , $0 \leq r < m$ avec les propriétés souhaitées. D'abord on choisit $x \in I$ tel que les classes de x_1, \dots, x_r, x dans I/J peuvent être complétés en un système minimal générateur pour I/J . Soient $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ les diviseurs premiers minimaux de (x_1, \dots, x_t) tels que $\mathfrak{q}_i \not\supset I$. Soit X l'ensemble des éléments maximaux (par rapport à l'inclusion) de $\{\mathfrak{q}_1, \dots, \mathfrak{q}_t, \mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ et partageons $X = X_1 \cup X_2$, où X_1 consiste en les premiers qui contiennent x et X_2 sont les autres.

Les idéaux premiers contenant I sont les mêmes que ceux qui contiennent J (car $\hat{V}(I) = \hat{V}(J)$) et donc $J \not\subset \bigcup_{\mathfrak{p} \in X} \mathfrak{p}$. Il existe donc $y \in J$ tel que $y \notin \mathfrak{p}$ quel que soit $\mathfrak{p} \in X$. Puisque $\mathfrak{p} \in X_2$ et $\mathfrak{p}' \in X_2$ sont deux idéaux premiers maximaux distincts, $\mathfrak{p} \not\subset \mathfrak{p}'$ et donc $\bigcap_{\mathfrak{p} \in X_2} \mathfrak{p} \not\subset \bigcup_{\mathfrak{p} \in X_1} \mathfrak{p}$ et par la Proposition 1.4.5 il y a $t \in \bigcap_{\mathfrak{p} \in X_2} \mathfrak{p}$ avec $t \notin \bigcup_{\mathfrak{p} \in X_1} \mathfrak{p}$. On pose

$$x_{r+1} = x + ty.$$

On a alors : $x_{r+1} \notin \mathfrak{p}$ quel que soit $\mathfrak{p} \in X$, en particulier :

$$x_{r+1} \notin \mathfrak{p}_j, \quad j = 1, \dots, s.$$

Puisque $x_{r+1} \equiv x \pmod{J}$, aussi les images de x_1, \dots, x_{r+1} dans I/J peuvent être complétées en un système minimal générateur pour I/J .

Finalement, si $\mathfrak{p} \supset (x_1, \dots, x_{r+1})$, mais $\mathfrak{p} \not\supset I$, alors $\text{ht}(\mathfrak{p}) \geq r + 1$, car \mathfrak{p} contient un des \mathfrak{q}_i et par hypothèse $\text{ht}(\mathfrak{q}_i) \geq r$, donc il y a une chaîne stricte décroissante S de longueur r d'idéaux premiers qui commence à \mathfrak{q}_i . Puisque $x_{r+1} \notin \mathfrak{q}_i$, $i = 1, \dots, r$ et $x_{r-1} \in \mathfrak{p}$, on a $\mathfrak{q} \neq \mathfrak{q}_i$ et chaîne qui résulte de S en rajoutant \mathfrak{p} est de longueur $r + 1$. ■

5.5. Corollaire. Soit A noethérien et \mathfrak{p} un idéal premier de hauteur m , alors il existe $x_1, \dots, x_m \in \mathfrak{p}$ tels que \mathfrak{p} est un diviseur premier minimal de (x_1, \dots, x_m) ,

Démonstration. On peut prendre $I = \mathfrak{p}$ et $J = I^2$. Localisons en \mathfrak{p} et observons que $\mu(\mathfrak{p}/\mathfrak{p}^2) \geq \mu(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}^2R_{\mathfrak{p}}) = e(R_{\mathfrak{p}}) \geq \dim R_{\mathfrak{p}} = \text{ht}(\mathfrak{p}) = m$. Il y a, par la démonstration du lemme ci-dessus, m éléments $x_1, \dots, x_m \in \mathfrak{p}$ tels que $\text{ht}(\mathfrak{p}') \geq m$ pour chaque idéal premier \mathfrak{p}' tel que $\mathfrak{p} \supset (x_1, \dots, x_m)$ et $\mathfrak{p}' \not\supset \mathfrak{p}$. Si \mathfrak{p} n'était pas un diviseur premier minimal de (x_1, \dots, x_m) , il y aurait un tel $\mathfrak{p}' \subset \mathfrak{p}$, $\mathfrak{p}' \neq \mathfrak{p}$ et donc une chaîne stricte décroissante de longueur $m + 1$ d'idéaux premiers qui commençait à \mathfrak{p} , contradiction et donc \mathfrak{p} est diviseur premier minimal de (x_1, \dots, x_m) . ■

5.6. Corollaire. Soit (A, \mathfrak{m}) un anneau local noethérien. Alors A admet un système de paramètres.

Démonstration. Soient $m = \dim A$ et $x_1, \dots, x_m \in \mathfrak{m}$ tels que \mathfrak{m} est le seul diviseur premier minimal de $\mathfrak{q} = (x_1, \dots, x_m)$. C'est un idéal \mathfrak{m} -primaire. ■

Voici une précision :

5.7. Proposition. Soit (A, \mathfrak{m}) anneau local noethérien. Pour $x_1, \dots, x_m \in \mathfrak{m}$ on a

1. $\dim A \geq \dim A/(x_1, \dots, x_m) \geq \dim A - m$,
2. $\dim A/(x_1, \dots, x_m) = \dim A - m$ si et seulement s'il existe $x_{m+1}, \dots, x_d \in \mathfrak{m}$ tels que $\{x_1, \dots, x_d\}$ soit un système de paramètres.

Démonstration.

1. Soit $e = \dim A/(x_1, \dots, x_m)$ et $y_1, \dots, y_e \in \mathfrak{m}$ tels que leurs images dans $A/(x_1, \dots, x_m)$ donnent un système de paramètres pour cet anneau. Alors $(x_1, \dots, x_m, y_1, \dots, y_e)$ est \mathfrak{m} -primaire et $m + e \geq \dim A$.
2. Si $m + e = \dim A$, alors $(x_1, \dots, x_m, y_1, \dots, y_e)$ est un système de paramètres pour A . Pour la réciproque, si $(x_1, \dots, x_m, y_1, \dots, y_e)$ est un système de paramètres pour A , alors $m + e = \dim A$ et les images de y_1, \dots, y_e dans $A/(x_1, \dots, x_m)$ engendrent un idéal qui est \mathfrak{n} -primaire, \mathfrak{n} , l'idéal maximal de $A/(x_1, \dots, x_m)$. On a :

$$e \geq \dim A/(x_1, \dots, x_m) \geq \dim A - m = e$$

et donc on a égalité partout. ■

§ 6. Anneaux réguliers

Rappelons que pour un anneau local noethérien (A, \mathfrak{m}) , la dimension d'immersion $e(A) = \dim_k \mathfrak{m}/\mathfrak{m}^2$, où k est le corps résiduel de A , est estimée par

$$e(A) \geq \dim(A).$$

On dit que A est régulier, si on a égalité :

6.1. Définition. Soit (A, \mathfrak{m}) un anneau local noethérien avec corps résiduel k . On dit que A est **régulier**, si $\dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2$.

6.2. Exemple. Supposons que k est algébriquement clos et $V = V(\mathfrak{p}) \subset k^n$ une variété irréductible, $P \in V$ et \mathfrak{m}_P , resp. $\mathfrak{m}_P(V)$ l'idéal maximal de $k[X_1, \dots, X_n]$, resp. $k[V]$ qui lui correspond. Montrons d'abord que

$$P + \mathfrak{m}_P(V)/\mathfrak{m}_P^2(V) \cong (T_P V)^*.$$

Pour $F \in k[X_1, \dots, X_n]$ on pose

$$dF(P) = \sum_j \frac{\partial F}{\partial X_j}(P)(X_j - X_j(P)).$$

Soit $\mathfrak{p}_1 = \{dF(P) ; F \in \mathfrak{p}\}$. On a une suite exacte :

$$0 \rightarrow \mathfrak{p}_1/\mathfrak{p}_1 \cap \mathfrak{m}_P^2 \rightarrow \mathfrak{m}_P/\mathfrak{m}_P^2 \rightarrow \mathfrak{m}_P(V)/\mathfrak{m}_P^2(V) \rightarrow 0,$$

où $\mathfrak{p}_1/\mathfrak{p}_1 \cap \mathfrak{m}_P^2$ est isomorphe au k -espace vectoriel engendré par les formes linéaires dF . L'espace tangent est l'espace affine passant par P parallèle au noyau U de cet espace. Aussi, $\mathfrak{m}_P/\mathfrak{m}_P^2$ s'identifie au k -espace vectoriel des formes linéaires sur k^n et donc $\mathfrak{m}_P(V)/\mathfrak{m}_P^2(V)$ est l'espace des formes linéaires sur U .

Conclusion : $x \in V$ est régulier si et seulement si $\dim T_x V = \dim \mathcal{O}_x(X)$. Au vue de 8.3.7 c'est équivalent à dire que $\dim T_x V = \dim V$, i.e. x un point non-singulier.

On termine en donnant une caractérisation d'un point non-singulier d'une courbe :

6.3. Proposition. *Un point $x \in V$ d'une courbe irréductible (c.à.d. $\dim V = 1$) est non-singulier si et seulement si $\mathcal{O}_x V$ est un anneau de valuation discrète. Cela est le cas si et seulement si $\mathcal{O}_x V$ est normal.*

Démonstration. Puisque V est irréductible, $\mathcal{O}_x V$ est un anneau intègre. C'est aussi un anneau local et noethérien. Il est régulier si et seulement si sa dimension d'immersion est 1, c.à.d. \mathfrak{m} est engendré par un seul élément. Par le Lemme 7.2.1 $\mathcal{O}_x V$ est un anneau de valuation discrète et donc normal.

Pour la réciproque on note d'abord que 7.2.2 dit qu'un anneau local normal et noethérien A est un anneau de valuation discrète et on a $e(A) = 1$. Donc, si $\mathcal{O}_x V$ est un tel anneau $\dim(\mathcal{O}_x V) = 1$, et l'anneau est régulier. ■

Chapitre 9. Algèbre homologique

§ 1. Complexes et leur (co)homologie

1.1. Définition.

1. Un **complexe de chaînes** d' A -modules est une suite d' A -modules :

$$M_{\bullet} = \{\dots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \dots\}$$

telle que $\forall i, d_i \circ d_{i+1} = 0$.

2. Un **complexe de co-chaînes** d' A -modules est une suite d' A -modules :

$$M^{\bullet} = \{\dots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \longrightarrow \dots\}$$

telle que $\forall i, d^{i-1} \circ d^i = 0$.

3. Les **groupes d'homologie** d'un complexe de chaînes sont

$$H_i(M_{\bullet}) = \frac{\text{Ker } d_i}{\text{Im } d_{i+1}}$$

et les **groupes de cohomologie** d'un de co-chaînes sont

$$H^i(M^{\bullet}) = \frac{\text{Ker } d^i}{\text{Im } d^{i-1}}.$$

On dit qu'un élément de $\text{Ker } d_i$ est un i -**cycle** et un élément de $\text{Im } d_{i+1}$ un i -**bord**, un élément de $\text{Ker } d^i$ est un i -**cocycle** et un élément de $\text{Im } d^{i-1}$ un i -**cobord**

3. Soient M_{\bullet} et N_{\bullet} deux complexes. Un **homomorphisme de complexes** $f_{\bullet} : M_{\bullet} \rightarrow N_{\bullet}$ est une famille d'homomorphismes $f_i : M_i \rightarrow N_i$ tel que les diagrammes

$$\begin{array}{ccc} M_i & \xrightarrow{d_i} & M_{i-1} \\ \downarrow f_i & & \downarrow f_{i-1} \\ N_i & \xrightarrow{d_i} & N_{i-1} \end{array}$$

sont commutatifs. De même pour deux complexes de co-chaînes.

4. Une **homotopie** h_{\bullet} entre deux homomorphismes de complexes $f_{\bullet}, g_{\bullet} : M_{\bullet}$ est une collection d' A -homomorphismes $h_i : M_i \rightarrow N_{i+1}$ telle que $\forall i, d_{i+1} \circ h_i + h_{i-1} \circ d_i = f_i - g_i$.

On vérifie aisément :

1.2. Lemme.

1. Un homomorphisme de complexes $f_\bullet : M_\bullet \rightarrow N_\bullet$ induit un homomorphisme $H_i(f_\bullet) : H_i(M_\bullet) \rightarrow H_i(N_\bullet)$, $i \in \mathbb{Z}$, tel que $\forall i, H_i(1) = 1, H_i(0) = 0$. Aussi, si $g_\bullet : N_\bullet \rightarrow P_\bullet$ est un autre homomorphisme de complexes, $(gf)_\bullet : M_\bullet \rightarrow P_\bullet$ défini par $\forall i, (gf)_i = g_i \circ h_i$ satisfait $\forall i, H_i((g \circ f)_\bullet) = H_i(g) \circ H_i(f)$.

2. S'il y a une homotopie entre f_\bullet et g_\bullet , alors $\forall i, H_i(f_\bullet) = H_i(g_\bullet)$. On dit que f_\bullet et g_\bullet sont **homotopes**.

On peut maintenant définir la notion d'un isomorphisme et d'un quasi-isomorphisme :

1.3. Définition.

1. Un homomorphisme de complexes $f_\bullet : M_\bullet \rightarrow N_\bullet$ est un **isomorphisme** s'il y a un homomorphisme $g_\bullet : N_\bullet \rightarrow M_\bullet$ qui est un inverse : $(f \circ g)_\bullet = (g \circ f)_\bullet = 1$.
2. Un homomorphisme de complexes $f_\bullet : M_\bullet \rightarrow N_\bullet$ est un **quasi-isomorphisme** s'il induit un isomorphisme en homologie : $\forall i, H_i(f_\bullet)$ est un isomorphisme.
3. S'il existe un (quasi)-isomorphisme entre M_\bullet et N_\bullet on dit que M_\bullet et N_\bullet sont **(quasi)-isomorphes**.
4. Un homomorphisme de complexes $f_\bullet : M_\bullet \rightarrow N_\bullet$ est un **isotopie**, s'il y a un homomorphisme $g_\bullet : N_\bullet \rightarrow M_\bullet$ tel que $(f \circ g)_\bullet$ et $(g \circ f)_\bullet$ sont homotopes à l'identité. En particulier, f est un quasi-isomorphisme. Deux complexes ont **même type d'homotopie** s'il y a un isotopie d'entre eux.

1.4. Théorème. Soit

$$0 \rightarrow M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \rightarrow 0$$

une suite exacte de complexes, c.à.d. f_\bullet et g_\bullet sont homomorphismes de complexes et $\forall i$ la suite

$$0 \rightarrow M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \rightarrow 0$$

est exacte. Alors,

1. Alors

$$\forall i, \quad H_i(M'_\bullet) \xrightarrow{H_i(f_\bullet)} H_i(M_\bullet) \xrightarrow{H_i(g_\bullet)} H_i(M''_\bullet)$$

est exacte,

2. Il existe des homomorphismes $\partial_i : H_i(M''_\bullet) \rightarrow H_{i-1}(M'_\bullet)$ tels que $\forall i \in \mathbb{Z}$

$$H_i(M_\bullet) \xrightarrow{H_i(g_\bullet)} H_i(M''_\bullet) \xrightarrow{\partial_i} H_{i-1}(M'_\bullet) \xrightarrow{H_{i-1}(f_\bullet)} H_{i-1}(M_\bullet)$$

est exacte.

Un cas spécial est le Lemme du serpent 2.4.2. On prend trois complexes $M'_\bullet = \{0 \rightarrow M' \xrightarrow{\alpha'} N' \rightarrow 0\}$, $M_\bullet = \{0 \rightarrow M \xrightarrow{\alpha} N \rightarrow 0\}$ et $M''_\bullet = \{0 \rightarrow M'' \xrightarrow{\alpha''} N'' \rightarrow 0\}$. Convenablement indexés, les complexes ont les groupes d'homologie $H_1(M'_\bullet) = \ker \alpha'$, $H_0(M'_\bullet) = \text{Coker } \alpha'$, et de même pour M_\bullet et M''_\bullet . Donc on voit que le Lemme du serpent est un cas spécial du théorème ci-dessus. En fait, la preuve est identique et on la laisse aux lecteurs.

§ 2. Modules projectifs, injectifs et suites exactes scindées

Rappelons le Lemme 2.6.1 :

Lemme.

1. Soit

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$$

une suite de A -modules. Alors, pour Q un A -module quelconque, on a la suite induite

$$0 \rightarrow \text{Hom}(M'', Q) \xrightarrow{\text{Hom}(g,1)} \text{Hom}(M, Q) \xrightarrow{\text{Hom}(f,1)} \text{Hom}(M', Q).$$

Cette suite est exacte si et seulement la suite précédente est exacte.

2. Pour

$$0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

on a la suite induite

$$0 \rightarrow \text{Hom}(Q, M') \xrightarrow{\text{Hom}(1,f)} \text{Hom}(Q, M) \xrightarrow{\text{Hom}(1,g)} \text{Hom}(Q, M'').$$

Cette suite est exacte si et seulement la suite précédente est exacte.

C'est facile de donner des exemples où cet énoncé est faux pour des suites exactes courtes. Cela justifie l'introduction des modules "injectifs" et "projectifs" :

2.1. Définition.

1. Un A -module Q est **injectif** si pour $f : M' \rightarrow M$ injective, $\text{Hom}(f, 1) : \text{Hom}(M, Q) \rightarrow \text{Hom}(M', Q)$ est surjective.
2. Un A -module Q est **projectif** si pour $g : M \rightarrow M''$ surjective, $\text{Hom}(1, f) : \text{Hom}(Q, M) \rightarrow \text{Hom}(Q, M'')$ est surjective.

En d'autres termes : Q est injectif si dans un diagramme

$$\begin{array}{ccccc} 0 & \rightarrow & M' & \hookrightarrow & M \\ & & & \searrow & \downarrow \\ & & & & Q \end{array}$$

on peut trouver la flèche cassée qui le rend commutatif, et Q est projectif si dans un diagramme

$$\begin{array}{ccccccc} & & Q & & & & \\ & & \downarrow & \searrow & & & \\ & & M & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

on peut trouver la flèche cassée qui le rend commutatif.

On dit qu'une suite exacte de A -modules

$$(*) \quad 0 \rightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \rightarrow 0$$

est **scindée** s'il y a un complément $N_2 \subset N$ à $f(N')$: $N = f(N') \oplus N_2$. Si c'est le cas, N_2 est isomorphe à N'' . On peut facilement prouver que :

2.2. Lemme. La suite (*) se scinde si et seulement si $\exists h : N'' \rightarrow N$ A -linéaire, tel que $g \circ h = 1$ si et seulement si $\exists k : N \rightarrow N'$ A -linéaire, tel que $k \circ f = 1$.

2.3. Corollaire. M est projectif si et seulement si chaque suite exacte (*) avec $N'' = M$ se scinde.

Démonstration. Si M est projectif $1 : M \rightarrow M$ se relève en $h : M \rightarrow N$ tel que $g \circ h = 1$ et donc (*) se scinde. Pour la réciproque, soit N le A -module libre engendré par les éléments de M . L'application naturelle $N \rightarrow M$ est surjective et donc il y a $h : M \rightarrow N$ tel que $g \circ h = 1$. Cela implique que N est facteur direct de M et donc N est projectif. ■

2.4. Corollaire. Si M est projectif, M est plat.

§ 3. Ext et Tor

3.1. Définition. Une **résolution projective**, resp. **libre** d'un A -module M est une suite exacte

$$\cdots M_i \xrightarrow{d_i} \cdots \rightarrow M_0 \xrightarrow{d_0} M \rightarrow 0$$

avec M_i projectif, resp. libre, $i = 0, 1, \dots$

C'est facile à construire une résolution libre de M : on prend pour M_0 le module libre engendré par les éléments de M , pour M_1 le noyau de l'application naturelle $M_0 \rightarrow M$ et cetera. On va voir que deux résolutions projectives sont quasi-isomorphes. On a besoin du lemme suivant :

3.2. Lemme. Étant donné $h : M \rightarrow N$ et deux résolutions projectives $M_\bullet \rightarrow M, N_\bullet \rightarrow N$, il y a un homomorphisme de complexes $h_\bullet : M_\bullet \rightarrow N_\bullet$ qui induit h . Deux de tels homomorphismes sont homotopes et donc $H_i(h_\bullet)$ est uniquement déterminé par h .

Démonstration.

1. Construction de h_\bullet .

Par récurrence. On construit d'abord $h_0 : M_0 \rightarrow N_0$ de manière suivante. L'homomorphisme $d_0 : N_0 \rightarrow N$ étant surjectif et M_0 projectif, l'homomorphisme $h \circ d_0 : M_0 \rightarrow N$ se factorise à travers $h_0 : M_0 \rightarrow N_0$.

Supposons que les h_i ont été construits pour $i \leq p-1$. On considère le diagramme commutatif avec les lignes exactes :

$$\begin{array}{ccccc} M_p & \xrightarrow{d_p} & M_{p-1} & \xrightarrow{d_{p-1}} & M_{p-2} \\ & & \downarrow h_{p-1} & & \downarrow h_{p-2} \\ N_p & \xrightarrow{d_p} & N_{p-1} & \xrightarrow{d_{p-1}} & N_{p-2}. \end{array}$$

On obtient :

$$\begin{array}{ccccc} M_p & \rightarrow & \text{im } d_p & \rightarrow & 0 \\ & & \downarrow h_{p-1} & & \\ N_p & \rightarrow & \text{im } d_p & \rightarrow & 0 \end{array}$$

et donc, par projectivité de M_p , on construit $h_p : M_p \rightarrow N_p$ tel que $d_p \circ h_p = h_{p-1} \circ d_p$.

2. Construction d'une homotopie.

Soient $h_\bullet, h'_\bullet : M_\bullet \rightarrow N_\bullet$ deux homomorphismes induisant $h : M \rightarrow N$. Il faut poser $k_{-1} = 0$ et il faut avoir $f_0 - g_0 = d_1 \circ k_0 + k_{-1} \circ d_0 = d_1 \circ k_0$. Mais l'existence de k_0 suit aussitôt du fait que M_1 est projectif.

La construction de k_p pour $p > 0$ est analogue. ■

3.3. Corollaire. Deux résolutions projectives de M ont même type d'homotopie.

Démonstration. Soient $M_\bullet \rightarrow M$ et $N_\bullet \rightarrow M$ deux résolutions projectives de M . Alors existent $f_\bullet : M_\bullet \rightarrow N_\bullet$ et $g_\bullet : N_\bullet \rightarrow M_\bullet$ induisant l'identité sur M . Les compositions $(f \circ g)_\bullet : N_\bullet \rightarrow N_\bullet$ resp. $(g \circ f)_\bullet : M_\bullet \rightarrow M_\bullet$ sont homotopes à l'identité car $1 : N_\bullet \rightarrow N_\bullet$ resp. $1 : M_\bullet \rightarrow M_\bullet$ induisent l'identité sur M . ■

Le lemme précédent et son corollaire impliquent que les définitions ci-dessus sont sans ambiguïté.

3.4. Définition.

1. Soit $M_\bullet \rightarrow M \rightarrow 0$ une résolution projective de M . On pose

$$\mathrm{Tor}_i^A(M, N) = H_i(M_\bullet \otimes N).$$

2. Si $f : M \rightarrow N$, $g : M' \rightarrow N'$ sont deux A -homomorphismes et $f_\bullet : M_\bullet \rightarrow N_\bullet$ un homomorphisme qui étend f , alors

$$\mathrm{Tor}_i(f, g) = H_i(f_\bullet \otimes g) : H_i(M_\bullet \otimes M') \rightarrow H_i(N_\bullet \otimes N').$$

3. De même façon :

$$\mathrm{Ext}^i(M, N) = H^i(\mathrm{Hom}(M_\bullet, N))$$

et

$$\mathrm{Ext}^i(f, g) = H^i(\mathrm{Hom}(f_\bullet, g)) : H^i(\mathrm{Hom}(M_\bullet, M')) \rightarrow H^i(\mathrm{Hom}(N_\bullet, N')).$$

3.5. Exemples.

1. Pour un module plat N , tensoriser avec N est exacte (par définition) et donc $\forall i \geq 1$, $\mathrm{Tor}_i^A(M, N) = 0$.
2. Si M est projectif, N quelconque, de la résolution projective $0 \rightarrow M \rightarrow M \rightarrow 0$ on déduit que $\forall i \geq 1$, $\mathrm{Ext}_A^i(M, N) = 0$.

3.6. Lemme. Soit

$$0 \rightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \rightarrow 0$$

une suite exacte et M un A -module quelconque. Alors il y a deux suites exactes longues :

$$\begin{aligned} \cdots \mathrm{Tor}_1(M, N') \xrightarrow{\mathrm{Tor}_1(1, f)} \mathrm{Tor}_1(M, N) \xrightarrow{\mathrm{Tor}_1(1, g)} \mathrm{Tor}_1(M, N'') \\ \rightarrow M \otimes N' \xrightarrow{1 \otimes f} M \otimes N \xrightarrow{1 \otimes g} M \otimes N'' \rightarrow 0 \end{aligned}$$

et

$$\begin{aligned} \cdots \mathrm{Tor}_1(N', M) \xrightarrow{\mathrm{Tor}_1(f, 1)} \mathrm{Tor}_1(N, M) \xrightarrow{\mathrm{Tor}_1(g, 1)} \mathrm{Tor}_1(N'', M) \\ \rightarrow N' \otimes M \xrightarrow{f \otimes 1} N \otimes M \xrightarrow{g \otimes 1} N'' \otimes M \rightarrow 0 \end{aligned}$$

Démonstration. Soit M_\bullet une résolution projective de M . La première suite est la suite longue en homologie de la suite exacte (projectif implique plat!) de complexes :

$$0 \rightarrow M_\bullet \otimes N' \xrightarrow{1 \otimes f} M_\bullet \otimes N \xrightarrow{1 \otimes g} M_\bullet \otimes N'' \rightarrow 0.$$

La deuxième suite provient de la suite exacte de complexes :

$$0 \rightarrow N'_\bullet \otimes M \xrightarrow{f_\bullet \otimes 1} N_\bullet \otimes M \xrightarrow{g_\bullet \otimes 1} N''_\bullet \otimes M \rightarrow 0$$

où N'_\bullet resp. N''_\bullet sont des résolutions projectives de N' , resp. N'' , et N_\bullet et f_\bullet, g_\bullet sont construits de telle façon que f_\bullet, g_\bullet induisent f, g et que la suite est une suite exacte de complexes. On note que les N_i sont bien déterminés : vu la projectivité des N'_i il faut avoir $N_i = N'_i \oplus N''_i$ ce qui détermine f_\bullet et g_\bullet . Il s'agit de définir les applications $N_i \rightarrow N_{i-1}$. Cela se fait par récurrence. On ne fait que le début. Puisque N''_0 est projectif, il y a un homomorphisme $N''_0 \rightarrow N$ qui relève $N''_0 \rightarrow N''$. On a aussi l'homomorphisme $N'_0 \rightarrow N' \rightarrow N$ et la combinaison des deux nous donne $d_0 : N_0 \rightarrow N$. Remplaçant N'', N, N'' par les noyaux de $N''_0 \rightarrow N, N \rightarrow N_0, N''_0 \rightarrow N$ on peut itérer cet argument.

Finalement on note que tensoriser avec M se comporte bien avec cette construction et donc après tensoriser la suite reste une suite de complexes. ■

3.7. Corollaire. Soient M et N des A -modules. Les énoncés suivants sont équivalents :

1. M est plat,
2. $\forall p \geq 1, \text{Tor}_p^A(M, N) = 0,$
3. $\text{Tor}_1^A(M, N) = 0.$

Démonstration.

1. \Rightarrow 2. C'est l'exemple 3 ci-dessus.

2. \Rightarrow 3. Clair.

3. \Rightarrow 1. Il faut montrer que tensoriser avec M est exacte. On applique le lemme ci-dessus. ■

3.8. Corollaire. Pour deux A -modules M et N les modules $\text{Tor}_i^A(M, N)$ et $\text{Tor}_i^A(N, M)$ sont isomorphes pour $i \geq 1$.

Démonstration. Soit $0 \rightarrow K \xrightarrow{f} P \rightarrow N \rightarrow 0$ suite exacte avec P projectif. Une telle suite existe toujours (prendre une résolution projective et raccourcir). Les deux suites longues donnent deux isomorphismes $\partial'_{i+1} : \text{Tor}_{i+1}(N, M) \rightarrow \text{Tor}_i(K, M)$ et $\partial''_{i+1} : \text{Tor}_{i+1}(M, N) \rightarrow \text{Tor}_i(M, K)$ ($i \geq 1$). Pour $i = 0$ on trouve un diagramme commutatif qui définit t_1

$$\begin{array}{ccc} \text{Tor}_1(N, M) & \xrightarrow{\cong} & \text{Ker}(f \otimes 1 : K \otimes M \rightarrow N \otimes M) \\ \downarrow t_1 & & \downarrow t_0 \\ \text{Tor}_1(M, N) & \xrightarrow{\cong} & \text{Ker}(1 \otimes f : M \otimes K \rightarrow M \otimes N) \end{array}$$

où t_0 provient des isomorphismes naturels $K \otimes N \cong N \otimes K$ et $M \otimes N \cong N \otimes M$. Donc par récurrence sur i on peut définir des isomorphismes t_i qui rendent le diagramme suivant commutatif :

$$\begin{array}{ccc} \text{Tor}_{i+1}(N, M) & \xrightarrow{\partial'_{i+1}} & \text{Tor}_i(K, M) \\ \downarrow t_{i+1} & & \downarrow t_i \\ \text{Tor}_{i+1}(M, N) & \xrightarrow{\partial''_{i+1}} & \text{Tor}_i(M, K) \end{array} .$$

Il y a aussi des suites longues pour "Ext" :

3.9. Proposition. Soit

$$0 \rightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \rightarrow 0$$

une suite exacte d' A -modules. Alors il y a des suites exactes longues :

$$0 \rightarrow \text{Hom}(M, N') \xrightarrow{\text{Hom}(1, f)} \text{Hom}(M, N) \xrightarrow{\text{Hom}(1, g)} \text{Hom}(M, N'') \xrightarrow{\delta} \text{Ext}^1(M, N') \xrightarrow{\text{Ext}^1(1, f)} \text{Ext}^1(M, N) \rightarrow \dots$$

et

$$0 \rightarrow \text{Hom}(N'', M) \xrightarrow{\text{Hom}(g, 1)} \text{Hom}(N, M) \xrightarrow{\text{Hom}(f, 1)} \text{Hom}(N', M) \xrightarrow{\delta} \text{Ext}^1(N'', M) \xrightarrow{\text{Ext}^1(g, 1)} \text{Ext}^1(N, M) \xrightarrow{\text{Ext}^1(f, 1)} \text{Ext}^1(N', M) \rightarrow \dots$$

§ 4. Dimension homologique

4.1. Définition. La **dimension homologique** d'un A -module M est la longueur minimale $n = \dim h M$ d'une résolution projective :

$$0 \rightarrow M_n \rightarrow \dots \rightarrow M_0 \rightarrow M \rightarrow 0.$$

4.2. Exemple. Pour M projectif $\dim h M = 0$.

4.3. Théorème. Les énoncés suivants sont équivalents :

1. $\dim h M \leq m$,
2. Pour un A -module N quelconque $\text{Ext}_A^{m+1}(M, N) = 0$,
3. $\text{Ext}^m(M, -)$ préserve les surjections,
4. Pour chaque suite exacte

$$0 \rightarrow M_m \rightarrow M_{m-1} \rightarrow \dots \rightarrow M_0 \rightarrow M \rightarrow 0$$

avec M_j projectif, $j = 0, \dots, m-1$, aussi M_m est projectif.

Démonstration.

1. \Rightarrow 2. Il existe une résolution projective M_\bullet de M de longueur $\leq m$. Alors $H^i(\text{Hom}(M_\bullet, N)) = 0$, $i \geq m+1$.

2. \Rightarrow 3. Soit $0 \rightarrow N' \rightarrow N \xrightarrow{g} N'' \rightarrow 0$ une suite exacte et

$$\dots \rightarrow \text{Ext}^m(M, N) \xrightarrow{\text{Ext}(1, g)} \text{Ext}^m(M, N'') \rightarrow \text{Ext}^{m+1}(M, N') \rightarrow \dots$$

la suite longue induite. Alors, $\text{Ext}^{m+1}(M, N') = 0$ implique que $\text{Ext}(1, g)$ est surjectif.

3. \Rightarrow 4. Pour simplifier on suppose que $m = 1$. Soit

$$0 \rightarrow M_1 \rightarrow M_0 \rightarrow M \rightarrow 0$$

une suite exacte avec M_0 projectif. Projectivité de M_0 implique que $\text{Ext}^1(M_0, N) = 0$ et donc une suite exacte

$$(*) \quad \text{Hom}(M_0, N) \rightarrow \text{Hom}(M_1, N) \xrightarrow{\delta} \text{Ext}^1(M, N) \rightarrow 0.$$

Il faut montrer que M_1 est projectif, donc pour $f : M_1 \rightarrow N''$ une application A -linéaire quelconque et $h : N \rightarrow N'' \rightarrow 0$ une application A -linéaire surjective, il y a $g : M_1 \rightarrow N$ linéaire telle que $f = h \circ g$. En d'autres termes, il faut montrer que $\beta = \text{Hom}(1, h) : \text{Hom}(M_1, N) \rightarrow \text{Hom}(M_1, N'')$ est surjectif. L'hypothèse dit qu'on a une surjection :

$$(**) \quad \text{Ext}^1(M, N) \xrightarrow{\text{Ext}^1(1, h)} \text{Ext}^1(M, N'') \rightarrow 0.$$

Considérons le diagramme :

$$\begin{array}{ccccccc} \text{Hom}(M_0, N) & \xrightarrow{\gamma'} & \text{Hom}(M_1, N) & \xrightarrow{\delta} & \text{Ext}^1(M, N) & \rightarrow & 0 \\ \downarrow \beta' & & \downarrow \beta & & \downarrow \text{Ext}^1(1, h) & & \\ \text{Hom}(M_0, N'') & \xrightarrow{\gamma} & \text{Hom}(M_1, N'') & \xrightarrow{\delta} & \text{Ext}^1(M, N'') & \rightarrow & 0 \end{array}$$

La surjectivité de δ est une conséquence de (*). On sait par (**) que $\text{Ext}^1(1, h)$ est une surjection. Aussi, puisque M_0 est projectif, β' est surjectif. Chasser le diagramme montre que β est surjectif : on prend $g \in \text{Hom}(M_1, N'')$. Alors $\exists e \in \text{Ext}^1(M, N)$ tel que $\text{Ext}^1(1, h)e = \delta(g)$. Ensuite $\exists g' \in \text{Hom}(M_1, N)$ tel que $\delta(g') = e$. Il faut considérer $g - \beta(g')$ avec image 0 dans $\text{Ext}^1(M, N'')$. Exactitude donne $f \in \text{Hom}(M_0, N'')$ avec $\gamma(f) = g - \beta(g')$. Surjectivité de β' donne $f' \in \text{Hom}(M_0, N)$ avec $\beta'(f') = f$ et $\beta(\gamma'(f')) = g - \beta(g')$. Finalement $g = \beta(g' + \gamma'(f'))$.

4. \Rightarrow 1. On sait qu'il y a toujours une résolution projective (peut-être de longueur infinie) :

$$\cdots \rightarrow M_{m-1} \xrightarrow{d_{m-1}} \cdots \rightarrow M_0 \rightarrow M \rightarrow 0.$$

Par hypothèse $\ker(d_{m-1})$ est projectif et donc une résolution projective de longueur m . ■

Le corollaire suivant est immédiat :

4.4. Corollaire. *Les énoncés suivants sont équivalents :*

1. M est projectif,
2. $\text{Ext}^p(M, N) = 0 \forall p \geq 1$, et N A -module quelconque,
3. $\text{Ext}^1(M, N) = 0$ pour N A -module quelconque,
4. $\dim h M \leq 0$.

§ 5. Théorème des syzygies de Hilbert

Le but est de montrer :

5.1. Théorème des syzygies. *Soit k un corps. Chaque $k[X_1, \dots, X_n]$ -module de type fini admet une résolution libre de longueur finie.*

Pour montrer ce théorème, on considère d'abord le cas gradué.

5.2. Définition.

1. Un **anneau gradué** A consiste en une décomposition $A = \bigoplus_i A_i$ en sous-groupes A_i , $i \in \mathbb{Z}$ tels que $\forall i, j, A_i \cdot A_j \subset A_{i+j}$. Un élément de A_i est dit homogène de degré i .
2. Un **A -module gradué** M , avec A anneau gradué consiste en une décomposition $M = \bigoplus_i M_i$ en sous-groupes M_i , $i \in \mathbb{Z}$, tels que $\forall i, j, A_i M_j \subset M_{i+j}$. Un élément de M_i est dit homogène de degré i .
3. Soit M un A -module gradué et $k \in \mathbb{Z}$. On définit un A -module gradué $M(k)$ par décalage :

$$M(k)_i = M_{k+i}.$$

Donc $x \in M(k)$ est homogène de degré i si $x \in M_{i+k}$.

4. Une **résolution libre graduée** d'un A -module gradué est une résolution

$$\dots \rightarrow M_n \xrightarrow{d_n} M_{n-1} \rightarrow \dots \rightarrow M_0 \xrightarrow{d_0} M \rightarrow 0$$

avec M_i libre et gradué et projective et d_n homogène de degré 0. Une telle résolution existe toujours.

5.3. Exemple. $S = k[X_1, \dots, X_n]$ est un anneau gradué avec le degré usuel des polynômes. Un S -module gradué M admet une résolution libre graduée :

$$\dots M_i = \bigoplus_j S(-n_{ij}) \xrightarrow{d_i} M_{i-1} = \bigoplus_j S(-n_{i-1,j}) \xrightarrow{d_{i-1}} \dots \rightarrow M_0 = \bigoplus_j S(-n_{0j}) \rightarrow M \rightarrow 0$$

avec les d_j homogène de degré 0. Si on oublie les graduations on peut dire que les d_j sont donnés par des matrices avec coefficients des polynômes homogènes (de degrés variables). Une telle résolution est **une résolution minimale** si ces coefficients sont jamais constants, c.à.d. si $d_i(M_i) \subset \mathfrak{m}M_{i-1}$ avec $\mathfrak{m} = (X_1, \dots, X_n)$. On peut toujours construire une telle résolution.

On pose $\tilde{S} = k[X_0, X_1, \dots, X_n]$. Le procédé

$$f(X_1, \dots, X_n) \mapsto F(X_0, \dots, X_n) = X_0^{\deg f} f(X_1/X_0, \dots, X_n/X_0)$$

est appelé "homogénéiser". Le procédé réciproque est "déhomogénéiser" :

$$F(X_0, \dots, X_n) \mapsto f(X_1, \dots, X_n) = F(1, X_1, \dots, X_n).$$

On a $\tilde{S}/(1 - X_0) = S$ comme \tilde{S} -module et

$$(*) \quad 0 \rightarrow \tilde{S} \xrightarrow{\cdot(1-X_0)} \tilde{S} \rightarrow S \rightarrow 0$$

est une \tilde{S} -résolution de S .

Pour M un S -module de type fini, on obtient un \tilde{S} -module gradué de la façon suivante. Soit

$$S^n \xrightarrow{(f_{ij})} S^m \rightarrow M \rightarrow 0$$

une présentation de M . Soit $d = \max \deg(f_{ij})$ et $\tilde{f}_{ij}(X_0, \dots, X_n) = X_0^d f_{ij}((X_1/X_0), \dots, (X_n/X_0))$. On pose

$$\tilde{M} = \tilde{S}^m / \text{Im}((\tilde{f}_{ij})).$$

Puisque $\tilde{f}_{ij}(1, X_1, \dots, X_n) = f_{ij}(X_1, \dots, X_n)$, on a $\tilde{f}_{ij} \otimes 1 = f_{ij} : \tilde{S}^n \otimes_{\tilde{S}} S = S^n \rightarrow \tilde{S}^m \otimes_{\tilde{S}} S = S^m$ et donc $\tilde{M} \otimes_{\tilde{S}} S \cong M$.

Preuve de 5.1. : étape 1, réduction au cas gradué.

Supposons qu'on a une résolution \tilde{S} -libre de $\text{Ker}((\tilde{f}_{ij}))$ de longueur $n + 1$:

$$0 \rightarrow \tilde{M}_{n+1} \rightarrow \dots \rightarrow \tilde{M}_0 \rightarrow \text{Ker}((\tilde{f}_{ij})) \rightarrow 0.$$

Cela donne une résolution libre \tilde{M}_\bullet de \tilde{M} de longueur $n + 3$. Si on tensorise cette suite avec S on obtient un complexe de longueur $n + 3$. Nous voulons voir que c'est un complexe exact : $H_i(\tilde{M}_\bullet \otimes S) = \text{Tor}_i^{\tilde{S}}(\tilde{M}, S)$ et il suffit de voir que $\text{Tor}_i^{\tilde{S}}(\tilde{M}, S) = 0$. Utilisons la commutativité de "Tor" (9.3.8). La résolution (*) de \tilde{S} donne immédiatement que $\text{Tor}_i^{\tilde{S}}(S, \tilde{M}) = 0$ pour $i \geq 2$ et le fait que multiplication avec $1 - X_0$ induit une injection $0 \rightarrow \tilde{M} \rightarrow \tilde{M}$ montre que $\text{Tor}_1^{\tilde{S}}(S, \tilde{M}) = 0$.

Preuve de 5.1 : étape 2, le complexe de Koszul

Soient $V = Se_1 \oplus \dots \oplus Se_n$ et

$$\partial_j : \bigwedge^j V \rightarrow \bigwedge^{j-1} V$$

l'application S -linéaire définie par

$$\partial_j(e_{i_1} \wedge \dots \wedge e_{i_j}) = \sum_k (-1)^k X_{i_k} e_{i_1} \wedge \dots \wedge \widehat{e_{i_k}} \wedge \dots \wedge e_{i_j}.$$

Avec $e : S \rightarrow k$ l'application "évaluation" $e(1) = 1$, $e(X_i) = 0$, $i = 1, \dots, n$, on a :

5.4. Proposition. *La suite*

$$0 \rightarrow \bigwedge^n V \xrightarrow{\partial_n} \dots \rightarrow \bigwedge^2 V \xrightarrow{\partial_1} V \xrightarrow{\partial_0} S \xrightarrow{e} k \rightarrow 0$$

est une résolution minimale libre de k .

Démonstration. On suppose que la caractéristique de k est nulle. On définit une application k -linéaire $\delta_k : \bigwedge^k V \rightarrow \bigwedge^{k+1} V$ par

$$\delta_k(Pe_{i_1} \wedge \dots \wedge e_{i_k}) = \sum_i \frac{\partial P}{\partial x_i} e_i \wedge e_{i_1} \wedge \dots \wedge e_{i_k}$$

et on note que

$$\delta_k \partial_k + \partial_{k-1} \delta_{k-1} = w_k, \quad w_k(P \cdot e_{i_1} \wedge \dots \wedge e_{i_k}) = (-d - 1)P \cdot e_{i_1} \wedge \dots \wedge e_{i_k}, \quad P \in S_d.$$

Puisque les ∂_j et les δ_j sont homogènes, pour montrer qu'un cycle est un bord, il suffit de considérer des k -cycles c , homogènes de degré d . La formule donne que $w_k(c)$ est un bord et puisque w_\bullet se restreint à la multiplication avec $-d - 1$ sur la partie de degré d , on déduit que pour la suite (*) de Koszul $\forall k$, $H_k(*) = 0$ (ici on utilise qu'on peut diviser par $-d - 1$ et donc que la caractéristique de k est nul). ■

Remarque. Pour la démonstration en caractéristique quelconque on verra [Ma, Theorem 16.3]. En fait, là on utilise la notion d'un M -séquence (a_1, \dots, a_n) d'un A -module quelconque. Cette notion est définie par récurrence. Un élément $a \in A$ est M -régulier si a n'annule aucun élément non-nul de M . Si $a_1, \dots, a_n \in A$ on dit que (a_1, \dots, a_n) est une M -séquence si

1. a_1 est M -régulier, a_2 est M/a_1M -régulier, ..., a_n est $M/\sum_{k=1}^{n-1} a_k M$ -régulier,
2. $M/\sum_{k=1}^n a_k M \neq 0$.

Il faut noter que l'ordre importe. Dans notre cas $A = M = S$ et (X_1, \dots, X_n) est clairement une S -séquence. Le complexe $\bigwedge^\bullet V$ qui termine à S n'est pas exacte : $H_0(\bigwedge^\bullet V) = k$. Le théorème [Ma, Theorem 16.3] dit que $H_j(\bigwedge^\bullet V) = 0$ pour $j \geq 1$.

5.5. Corollaire. *Pour un S -module M quelconque on a $\mathrm{Tor}_i^S(k, M) = 0$ pour $i \geq n + 1$.*

Preuve de 5.1 : étape 3, le cas gradué.

La notion cruciale est celle d'une résolution libre minimale, qu'on vient d'introduire. Rappelons, que cela veut dire que les coefficients des matrices définissant $d_n : M_n = S^{k_n} \rightarrow M_{n-1} = S^{k_{n-1}}$ sont des polynômes homogènes en degré ≥ 1 .

Pour une telle résolution $d_n \otimes 1 : M_n \otimes_S k \rightarrow M_{n-1} \otimes_S k$ est zéro, car dans $M_n \otimes_S k = M_n \otimes R/(X_1, \dots, X_n)$ la multiplication avec X_i est zéro. On utilise le Corollaire 9.3.8 : $\mathrm{Tor}_i^S(k, M) = \mathrm{Tor}_i^S(M, k)$. Donc $\mathrm{Tor}_i^S(k, M) = H_i(M_\bullet \otimes_S k) = M_i \otimes_S k$ et puisque M_i est libre, on en déduit

$$\mathrm{Tor}_i^S(k, M) = 0 \quad \text{si et seulement si} \quad M_i = 0.$$

La suite de Koszul montre que $\mathrm{Tor}_i^S(k, M) = 0$ pour $i \geq n + 1$ et donc

5.6. Théorème. *Chaque résolution minimale et libre d'un S -module gradué M de type fini est de longueur $\leq n$.*

Références

- [AM] Atiyah, M.F & I.G. Macdonald: Introduction to Commutative Algebra, Addison&Wesley Reading, Mass (1969),
- [Bo] Bourbaki,N: Algèbre commutative, Hermann, Paris (1961–1965),
- [Ei] Eisenbud, D.: Commutative Algebra with a view toward algebraic geometry, Springer Verlag, Berlin etc. (1994),
- [Ku] Kunz, E.: Einführung in die kommutative Algebra und algebraische Geometrie, F. Vieweg & Sohn Braunschweig/Wiesbaden (1979),
- [Ma] Matsumura, H.: Commutative ring theory, Cambridge Univ. Press, Cambridge (1980),
- [Re1] Reid, M.: Undergraduate algebraic geometry, Cambridge University Press, 2nd ed., Cambridge, (1990),
- [Re2] Reid, M.: Undergraduate commutative algebra, Cambridge University Press, Cambridge, (1996),