3 Idéaux premiers et maximaux, localisation, théorème des zéros de Hilbert

Version du 23 octobre 2005

11 Idéaux premiers et maximaux, Lemme de Zorn

11.1 Idéaux premiers et maximaux

Définition 11.1.1 *Soit I un idéal de A. On dit que I est* **premier** *s'il est différent de A et vérifie la condition suivante :*

> *Si $a \notin I$ et $b \notin I$ alors $ab \notin I$. Ou, de façon équivalente (en prenant la contraposée) : si $ab \in I$ alors $a \in I$ ou $b \in I$.*

On dit que I est **maximal** *si $I \neq A$ et s'il n'existe pas d'idéal $J \neq A$ contenant strictement I.*

On notera que, par définition, l'idéal A n'est ni maximal ni premier.

Proposition 11.1.2 *Soit A un anneau commutatif, I un idéal de A. Alors :*
a) *I est premier $\Leftrightarrow$ A/I est intègre.*
b) *I est maximal $\Leftrightarrow$ A/I est un corps.*
En particulier, tout idéal maximal est premier.

Démonstration. a) est facile et laissé au lecteur. Démontrons b). Supposons que A/I soit un corps et soit $x \in A \setminus I$. Alors, l'image $\bar{x}$ de x dans A/I est $\neq 0$, donc inversible, donc il existe $a \in A$ tel que $\bar{a}\bar{x} = 1$. Ceci signifie que $ax - 1 \in I$. Alors

$$1 = ax + (1 - ax) \in Ax + I$$

et donc $I + Ax = A$, pour tout $x \notin I$. Ceci prouve que I est maximal.

Réciproquement, supposons que I soit maximal et soit $x \notin I$. Alors l'idéal $Ax + I$ égale A, donc il existe $a \in A$ et $y \in I$ tels que $ax + y = 1$. Alors, dans A/I on a $\bar{a}\bar{x} = 1$ et ceci prouve que $\bar{x}$ est inversible. Comme x est arbitraire dans $A \setminus I$ ceci prouve que A/I est un corps. □

Remarque 11.1.3 Les idéaux premiers d'un anneau A jouent un rôle extrêmement important.

En arithmétique, si A est un anneau de nombres, ses idéaux premiers généralisent la notion usuelle de nombre premier dans $\mathbb{Z}$, voir par exemple [Sa].

En géométrie algébrique, les idéaux premiers de l'anneau $\mathbb{C}[X_1, \ldots, X_n]$ correspondent aux **sous-variétés algébriques irréductibles** de $\mathbb{C}^n$. Une **sous-variété algébrique** de $\mathbb{C}^n$ est un sous-ensemble X de $\mathbb{C}^n$ défini par des équations polynomiales $f_1, \ldots, f_m$, c.-à-d., X égale

$$V(f_1, \ldots, f_m) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f_j(x_1, \ldots, x_n) = 0, \forall j = 1, \ldots, m\}.$$

On observe que $V(f_1, \ldots, f_m) = V(I)$, où I désigne l'idéal engendré par $f_1, \ldots, f_m$.

D'autre part, à un tel X, on associe l'idéal

$$I(X) = \{f \in \mathbb{C}[X_1, \ldots, X_n] \mid f(x) = 0, \forall x \in X\}.$$

Enfin, on dit que X est **irréductible** s'il n'est pas réunion de deux sous-variétés algébriques plus petites, c.-à-d., s'il vérifie la propriété suivante :

> Si J, K sont des idéaux de $\mathbb{C}[X_1, \ldots, X_n]$ tels que $X = V(J) \cup V(K)$, alors $V(J) = X$ ou $V(K) = X$.

Exercice 11.1.1 Montrez que X est irréductible $\Leftrightarrow$ $I(X)$ est un idéal premier.

Les lecteurs intéressés pourront consulter, par exemple, [Die] ou [Pe2].

11.2 Sous-modules maximaux et lemme de Zorn

Soient A un anneau $\neq 0$ et M un A-module.

Définition 11.2.1 *Un sous-module* **propre** *de M est un sous-module $N \neq M$. De même, un* **idéal propre** *de A est un idéal $\neq A$.*

Définition 11.2.2 *Soit N un sous-module de M. On dit que N est sous-module* **maximal** *s'il n'existe pas de sous-module propre N' contenant N strictement, c.-à-d., si N est un élément maximal (pour la relation d'inclusion) de l'ensemble des sous-modules propres.*

On veut montrer que A possède au moins un idéal maximal. Ceci nous conduit à étudier dans un A-module M arbitraire, l'existence de sous-modules maximaux. Il n'en existe pas nécessairement, comme le montre l'exercice ci-dessous.

Exercice 11.2.1 Soit A le sous-anneau du corps $\mathbb{C}(X)$ formé des fractions rationnelles définies en 0, c.-à-d.,

$$A = \{\frac{P}{Q} \mid P, Q \in \mathbb{C}[X],\, Q(0) \neq 0\}.$$

Soit N un sous-A-module de $\mathbb{C}(X)$. Montrez que N est engendré par X^n, pour un certain $n \in \mathbb{Z}$. En déduire que le A-module $\mathbb{C}(X)$ ne possède pas de sous-module maximal.

Toutefois, on a le théorème ci-dessous.

Théorème 11.2.3 *Soit M un A-module de type fini et soit N un sous-module propre. Alors M possède au moins un sous-module maximal contenant N.*

Démonstration. Le point-clé de la démonstration est le lemme suivant.

Lemme 11.2.4 *Soit M un A-module* **de type fini** *et soit $(M_i)_{i\in I}$ une famille filtrante de sous-modules* **propres** *de M. Alors $\bigcup_{i\in I} M_i$ est un sous-module* **propre** *de M.*

Démonstration. Posons $U := \bigcup_{i\in I} M_i$; on a déjà vu que c'est un sous-module de M (Lemme 6.2.7). Montrons que c'est un sous-module propre. Soient $x_1, \ldots, x_r$ un système fini de générateurs de M.

Alors, il existe des indices $i_1, \ldots, i_r \in I$ tels que $x_1 \in M_{i_1}$, ..., $x_r \in M_{i_r}$. Comme la famille $(M_i)_{i\in I}$ est filtante, il existe ℓ tel que M_ℓ contienne $x_1, \ldots, x_r$, et comme ces derniers sont des générateurs de M, ceci entraîne $M_\ell = M$, en contradiction avec l'hypothèse que chaque M_i, $i \in I$, est un sous-module propre. Cette contradiction montre que $U \neq M$. Le lemme est démontré. □

On peut maintenant démontrer le théorème. Si $N = N_0$ n'est pas maximal, il est contenu strictement dans un sous-module propre N_1. Si N_1 n'est pas maximal, il est contenu strictement dans un sous-module propre N_2, etc. Donc, soit on obtient ainsi, en un nombre fini d'étapes, un sous-module maximal N_n contenant $N = N_0$, soit on construit une suite infinie strictement croissante

$$N_0 \subset N_1 \subset N_2 \subset \cdots$$

Dans ce cas, posons $N_\omega = \bigcup_{i\in\mathbb{N}} N_i$. D'après le lemme précédent, c'est un sous-module propre de M. S'il n'est pas maximal, il est contenu strictement dans un sous-module propre, qu'on notera $N_{\omega+1}$. Si ce dernier n'est pas maximal, il est contenu strictement dans un sous-module propre $N_{\omega+2}$, etc. On obtient ainsi, soit un sous-module maximal $N_{\omega+r}$, soit une suite infinie strictement croissante

$$N_\omega \subset N_{\omega+1} \subset N_{\omega+2} \subset \cdots$$

Dans ce cas, posons $N_{2\omega} = \bigcup_{i\in\mathbb{N}} N_{\omega+i}$. D'après le lemme 11.2.4, à nouveau, c'est un sous-module propre de M. S'il n'est pas maximal, il est contenu strictement dans un sous-module propre, qu'on notera $N_{2\omega+1}$, etc. L'idée est que "en continuant ainsi", on obtiendra un sous-module maximal.

Il faut montrer que, en un certain sens, le processus s'arrête. Une difficulté rencontrée est qu'il ne suffit pas de considérer, comme ci-dessus, des **suites** de sous-modules. On effet, comme suggéré par la notation ci-dessus, les sous-modules $N_{m\omega+n}$ dépendent de deux entiers $m, n \geq 0$, et il n'est pas nécessairement vrai, en général, qu'il existe un couple (m, n) tel que $N_{m\omega+n}$ soit maximal.

En fait, pour rendre rigoureux le raisonnement intuitif ci-dessus, on a besoin d'un résultat de théorie des ensembles, appelé le Lemme de Zorn. Avant de l'énoncer, remarquons que l'ensemble des sous-modules propres de M est ordonné par inclusion et que si $(M_i)_{i\in I}$ est une famille **filtrante** de sous-modules propres, alors $U = \bigcup_{i\in I}$ est un sous-module propre (d'après le lemme 11.2.4), qui est un **majorant** de chacun des M_i, c.-à-d., tel que $M_i \subseteq U$ pour tout $i \in I$. On peut maintenant énoncer la définition et le théorème suivants.

Définition 11.2.5 *Soit $(E, \leq)$ un ensemble ordonné, c.-à-d., E est muni d'une relation $x \leq y$ qui est une relation d'ordre, c.-à-d., qui est*

1) réflexive : $\forall x \in E, \quad x \leq x$;

2) antisymétrique : $\forall x, y \in E, \quad x \leq y$ et $y \leq x \Rightarrow x = y$;

3) transitive : $\forall x, y, z \in E, \quad x \leq y$ *et* $y \leq z \Rightarrow x = z$.

On dit qu'un sous-ensemble F *de* E *est* **filtrant** *s'il vérifie la propriété suivante : pour tout* $f, f' \in F$*, il existe* $f'' \in F$ *tel que* $f \leq f''$ *et* $f' \leq f''$.

On dit qu'un élément $x \in E$ *est un élément* **maximal** *s'il n'existe pas d'élément* $y \in E$ *tel que* $y > x$.

Soit S *un sous-ensemble de* E *et soit* $x \in E$*. On dit que* x *est un* **majorant** *de* S *si l'on a* $s \leq x$ *pour tout* $s \in S$ *(on ne demande pas que* x *appartienne à* S*).*

Théorème 11.2.6 (Lemme de Zorn) *Soit* E *un ensemble ordonné non-vide vérifiant la propriété suivante :*

$(*)$ *Tout sous-ensemble filtrant de* E *admet un majorant dans* E.

Alors E *possède au moins un élément maximal.*

Combiné avec le lemme 11.2.4, ceci achève la preuve du théorème 11.2.3. En effet, l'ensemble E des sous-modules propres de M contenant N est non-vide (il contient N) et vérifie la propriété $(*)$, d'après le lemme 11.2.4. Il possède donc un élément maximal M', et M' est un sous-module maximal de M contenant N. □

Nous n'entrons pas dans la démonstration du Lemme de Zorn, qui appartient au domaine de la théorie des ensembles, et l'on renvoie le lecteur intéressé à [Dou, Chap.1] ou [La, Appendix 2].

Remarque 11.2.7 Dans ces références, il est montré comment le lemme de Zorn se déduit de l'axiome du choix. Il est aussi montré que le lemme de Zorn entraîne le théorème de Zermelo, qui lui-même entraîne l'axiome du choix. Donc, en fait, axiome du choix, lemme de Zorn et théorème de Zermelo sont équivalents.

Corollaire 11.2.8 *Soient* A *un anneau commutatif et* I *un idéal propre de* A*. Alors* I *est contenu dans un idéal maximal* $\mathfrak{m}$.

Démonstration. Ceci résulte du théorème 11.2.3, puisque A est un A-module de type fini ! □

12 Anneaux de fractions, localisation

Dans cette section, A est un anneau commutatif.

12.0 Motivation

Les anneaux commutatifs les plus simples sont les corps. Par exemple, un corps k n'a qu'un seul idéal propre : (0), et un k-module n'est rien d'autre qu'un espace vectoriel, qui est entièrement déterminé par sa dimension.

Étant donné un anneau commutatif arbitraire A et un A-module M, l'idée de localisation consiste à essayer de se ramener, autant que possible, à ce cas très simple, en remplaçant A par une A-algèbre A' (obtenue en rendant inversibles certains éléments de A), et M par un A'-module M'.

De plus, on veut que ce processus ne fasse pas perdre trop d'informations sur A et M, c.-à-d., qu'à partir des résultats obtenus sur les objets simplifiés A' et M', on puisse obtenir des résultats sur les objets initiaux A et M.

La première idée qui vient à l'esprit pour A' est de rendre inversibles tous les éléments non nuls de A. Cette idée naturelle est la bonne lorsque A est intègre, on obtient ainsi le corps des fractions de A (analogue de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$).

Mais si A n'est pas intègre, cette construction peut donner l'anneau nul $\{0\}$. En effet, si on rend inversibles dans A' deux éléments s, t de A, alors st sera aussi inversible (d'inverse $t^{-1}s^{-1}$). Donc, si $st = 0$, on obtient dans A' l'égalité $1 = 0$, d'où $A' = \{0\}$.

Par exemple, soit $A = \mathbb{Z}/6\mathbb{Z}$. Pour rendre inversibles les éléments $\dot{2}$ et $\dot{3}$ de A on peut considérer la A-algèbre $A' := A[X, Y]/I$, où I est l'idéal engendré par $2X - 1$ et $3Y - 1$. Désignant par x, y les images de X, Y dans A', on a $A' = A[x, y]$ et x, resp. y, est l'inverse de $\dot{2}$, resp. $\dot{3}$. Mais $\dot{2}\dot{3} = 0$, donc multipliant par xy on obtient $1 = 0$, d'où $A' = \{0\}$.

Ce qui précède conduit à la définition suivante.

Définition 12.0.1 *Une* **partie multiplicative** *de A est un sous-ensemble S contenant* 1, *stable par multiplication et ne contenant pas* 0.

Étant donné une partie multiplicative S, on veut construire une A-algèbre notée $S^{-1}A$, en imitant la construction du corps $\mathbb{Q}$ des rationnels. C.-à-d., la première idée qui vient à l'esprit est de considérer l'ensemble des "fractions"

$$\frac{a}{s}, \qquad a \in A, s \in S,$$

où l'on "identifie" a avec $a/1$, et d'y définir la multiplication et l'addition par les formules évidentes :

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st} \tag{1}$$

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}. \tag{2}$$

Notons que si $at = bs$, alors (2) entraîne que

$$\frac{a}{s}=\frac{b}{t},$$

c.-à-d., comme pour les rationnels, on doit identifier deux fractions a/s et b/t si $at = bs$.

De plus, si S contient des diviseurs de zéro, d'autres identifications sont nécessaires. En effet, supposons $sa = 0$, avec $s \in S$. Dans $S^{-1}A$, multipliant cette égalité par $1/s$, on obtient $a/1 = 0$, donc a devient nul dans $S^{-1}A$. Le même raisonnement montre que si $t \in S$ et s'il existe $u \in S$ tel que $u(at - bs) = 0$, alors dans $S^{-1}A$ on doit avoir

$$\frac{a}{s}=\frac{b}{t}\,.$$

On est donc conduit à définir $S^{-1}A$ comme l'ensemble des fractions a/s, "modulo les identifications précédentes". C.-à-d., pour être précis, on va définir $S^{-1}A$ comme l'ensemble des **couples** $(a, s) \in A \times S$, modulo la relation d'équivalence

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

Dans le paragraphe suivant, on traitera le cas général, qui n'est pas beaucoup plus compliqué que le cas où A est intègre. Toutefois, on recommande au lecteur qui n'est pas familier avec cette construction de commencer par étudier d'abord le cas où A est intègre.

12.1 Construction de l'anneau $S^{-1}A$

Soit A un anneau commutatif et S une partie multiplicative de A. Considérons la relation suivante sur $A \times S$: on pose

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

Cette relation est clairement réflexive et symétrique. Elle est aussi transitive. En effet, si

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

il existe $u, u' \in S$ tels que $(at - bs)u = 0 = (bv - ct)u'$. Alors

$$atu\,vu' = bsu\,vu' = bvu'su = ctu'su = cs\,tuu'$$

et donc $(av - cs)tuu' = 0$, avec $tuu' \in S$ puisque S est stable par multiplication. Ceci montre que $(a, s) \sim (c, v)$ et donc $\sim$ est une relation d'équivalence. Notons $S^{-1}A$ l'ensemble quotient (c.-à-d., l'ensemble des classes d'équivalence), et, pour tout $(a, s) \in A \times S$, désignons par $[a, s]$ son image dans $S^{-1}A$.

On définit sur $S^{-1}A$ une addition et une multiplication par les formules suivantes :

$$(*) \qquad [a, s] + [b, t] = [at + bs, st], \qquad [a, s][b, t] = [ab, st].$$

Il faut vérifier que ces formules font sens. Supposons que $[a, s] = [a', s']$. Alors, il existe $u \in S$ tel que $as'u = a'su$. (Si S ne contient pas de diviseurs de zéro, on peut prendre $u = 1$). Alors

$$abs'tu = a'subt = a'bstu \quad \text{et} \quad (at + bs)s'u = a'sut + bss'u = (a't + bs')su$$

et donc, d'une part, $[a'b, s't] = [ab, st]$ et, d'autre part,

$$[at + bs, st] = [(at + bs)s'u, sts'u] = [(a't + bs')su, s'tsu] = [a't + bs', s't].$$

Ceci montre que, dans les égalités $(*)$, les termes de droite ne dépendent que de la classe $[a, s]$ (et non du couple (a, s)). De même, ces termes ne dépendent que de la classe $[b, t]$. Ceci montre que l'addition et la multiplication sont bien définies.

On vérifie alors facilement qu'elles définissent sur $S^{-1}A$ une structure d'anneau non nul, dont le 0 est $[0, 1]$ et l'élément unité $[1, 1]$ (il est $\neq 0$ car $0 \notin S$), et que l'application

$$\tau : A \to S^{-1}A, \qquad a \mapsto [a, 1]$$

est un morphisme d'anneaux. **Attention**, ce morphisme n'est en général pas injectif ; plus précisément, on a

$$\operatorname{Ker} \tau = \{a \in A \mid \exists s \in S \text{ tel que } as = 0\}.$$

On obtient ainsi la proposition suivante.

Proposition 12.1.1 (Existence et unicité de $S^{-1}A$)
Il existe une A-algèbre $\tau : A \to S^{-1}A$ vérifiant les deux propriétés suivantes :

1) *Pour tout $s \in S$, $\tau(s)$ est inversible dans $S^{-1}A$.*
2) *Tout élément de $S^{-1}A$ est de la forme $\tau(a)\tau(s)^{-1}$, avec $a \in A$, $s \in S$.*

De plus, la structure d'anneau de $S^{-1}A$ est entièrement déterminée par ces conditions. Enfin, le noyau de τ égale :

$$\operatorname{Ker}\tau = \{a \in A \mid \exists s \in S \text{ tel que } as = 0\};$$

il est non nul si et seulement si S contient un diviseur de zéro. L'anneau $S^{-1}A$ s'appelle le **localisé de** *A en la partie multiplicative S.*

Démonstration. La construction de $S^{-1}A$ nous donne l'existence. D'autre part, comme τ est un morphisme d'anneaux, on a

$$\tau(a)\tau(s)^{-1} \cdot \tau(b)\tau(t)^{-1} = \tau(ab)\tau(st)^{-1},$$

$$\tau(a)\tau(s)^{-1} + \tau(b)\tau(t)^{-1} = \tau(at)\tau(st)^{-1} + \tau(bs)\tau(st)^{-1} = \tau(at+bs)\tau(st)^{-1},$$

et donc la structure d'anneau est uniquement déterminée par les conditions (1) et (2). □

Dans la pratique, il y a essentiellement deux exemples importants de parties multiplicatives S et d'anneaux $S^{-1}A$ qu'on considère.

Exemple 12.1.2 Soit $\mathfrak{p}$ un idéal premier de A. Alors $S := A \setminus \mathfrak{p}$ est une partie multiplicative. Dans ce cas, l'anneau $S^{-1}A$ est noté $A_{\mathfrak{p}}$ et est appelé, par abus de language, le **localisé de A en $\mathfrak{p}$**.

Soient par exemple $A = \mathbb{Z}$ et p un nombre premier. Alors l'idéal $\mathfrak{p} = (p)$ est premier (d'après le Lemme d'Euclide), et l'anneau $\mathbb{Z}_{(p)}$ est le sous-anneau suivant de $\mathbb{Q}$:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \notin p\mathbb{Z} \right\}.$$

Définition 12.1.3 *Un élément $f \in A$ est dit* **nilpotent** *s'il existe $n \in \mathbb{N}^*$ tel que $f^n = 0$.*

Exemple 12.1.4 Soit $f \in A$ un élément non nilpotent. Alors $S = \{f^n \mid n \in \mathbb{N}\}$ est une partie multiplicative, et $S^{-1}A$ est noté A_f ou $A[1/f]$ ou $A[f^{-1}]$ et est appelé le **localisé de A en f**.

En général, la notation A_f ne présente pas d'ambiguïté. Mais **attention**, elle est à proscrire si $A = \mathbb{Z}$, car si p est un nombre premier, la notation $\mathbb{Z}_p$ désigne autre chose, l'anneau des entiers p-adiques. Donc, dans ce cas, il faut noter $\mathbb{Z}[1/p]$ ou $\mathbb{Z}[p^{-1}]$ le localisé de $\mathbb{Z}$ en la partie multiplicative $S = \{p^n \mid n \in \mathbb{N}\}$, c.-à-d.,

$$\mathbb{Z}[1/p] = \left\{ \frac{a}{p^n} \mid a \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Exercice 12.1.1 Soit $A = \mathbb{C}[X]$. Avec les notations A_f et $A_{\mathfrak{p}}$ introduites plus haut, décrire $\mathbb{C}[X]_X$ et $\mathbb{C}[X]_{(X)}$.

Exercice 12.1.2 Soit A l'anneau produit $K_1 \times K_2$, où K_1, K_2 sont deux corps. On note $e_1 = (1,0)$ et $e_2 = (0,1)$. Montrer que $S = \{e_1\}$ est une partie multiplicative. Qu'est-ce que $S^{-1}A$?

Exercice 12.1.3 Soit A l'anneau quotient $\mathbb{C}[X,Y]/(XY)$ et soit $\mathfrak{p} = (x)$, où x désigne l'image de X dans A. Montrez que $\mathfrak{p}$ est un idéal premier de A. Que sont les localisés A_x et $A_{\mathfrak{p}}$?

En fait, l'algèbre $\tau : A \to S^{-1}A$ a une propriété d'unicité un peu plus forte, donnée par la propriété universelle suivante.

Théorème 12.1.5 (Propriété universelle de $S^{-1}A$)
Soit B un anneau non nécessairement commutatif. Pour tout morphisme d'anneaux $\phi : A \to B$ tel que $\phi(s)$ soit inversible pour tout $s \in S$, il existe un **unique** *morphisme d'anneaux $\Phi : S^{-1}A \to B$ tel que $\Phi \circ \tau = \phi$.*

Démonstration. Si Φ existe, on a nécessairement, pour tout $a \in A$, $\Phi(\tau(a)) = \phi(a)$. Alors, pour $s \neq 0$, l'égalité

$$1 = \Phi(1) = \Phi(\tau(s)\tau(s)^{-1}) = \phi(s)\Phi(\tau(s)^{-1})$$

entraîne $\Phi(\tau(s)^{-1}) = \phi(s)^{-1}$. Enfin, comme $[a,s] = \tau(a)\tau(s)^{-1}$, nécessairement Φ doit vérifier

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

Ceci montre que Φ, s'il existe, est nécessairement unique. Réciproquement, vérifions que la formule (1) définit Φ sans ambiguités. Or, si $[a,s] = [b,t]$, il existe $u \in S$ tel que $(at - bs)u = 0$, d'où

$$\phi(a)\phi(t)\phi(u) = \phi(atu) = \phi(bsu) = \phi(b)\phi(s)\phi(u).$$

Comme $\phi(s)$, $\phi(t)$ et $\phi(u)$ sont inversibles, on en déduit $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$. Ceci montre que Φ est bien définie, et alors on voit facilement que c'est un morphisme d'anneaux. Le théorème est démontré. □

Un corollaire standard de ce type de propriété universelle est que, comme A-algèbre, $S^{-1}A$ est unique à isomorphisme unique près. C.-à-d., on a le corollaire suivant.

Corollaire 12.1.6 *Soit $\tau' : A \to A'$ une autre A-algèbres telle que $\tau'(s)$ soit inversible pour tout $s \in S$ et vérifiant la propriété universelle précédente. Alors il existe un* **unique** *morphisme de A-algèbres*

$$\Phi : S^{-1}A \to A',$$

(c.-à-d., un morphisme d'anneaux tel que $\Phi \circ \tau = \tau'$), et c'est un isomorphisme.

Démonstration. Par la propriété universelle de $S^{-1}A$, il existe un unique morphisme $\Phi : S^{-1}A \to A'$ tel que $\Phi \circ \tau = \tau'$. De même, par la propriété universelle de A', il existe un unique morphisme $\Psi : A' \to S^{-1}A$ tel que $\Psi \circ \tau' = \tau$.

Alors, $\Psi \circ \Phi \circ \tau = \Psi \circ \tau' = \tau$, donc, par la propriété universelle de $S^{-1}A$, appliquée à $B' = S^{-1}A$ et $\tau' = \tau$, on obtient que $\Psi \circ \Phi = \mathrm{id}_{S^{-1}A}$. On obtient de même que $\Phi \circ \Psi = \mathrm{id}_{A'}$. Ceci prouve le corollaire. □

Remarque 12.1.7 On prendra garde au fait que dans la propriété universelle, l'hypothèse qu'il existe un **unique** Φ joue un rôle essentiel : on l'a vu dans la démonstration du corollaire. On peut aussi remarquer que le morphisme $A \to S^{-1}A \to S^{-1}A[X]$, vérifie la propriété universelle sans l'unicité, c.-à-d., pour tout $\phi : A \to B$ comme dans le théorème, on peut de façon arbitraire étendre le morphisme $\Phi : S^{-1}A \to B$ à $S^{-1}A[X]$, en envoyant X sur un élément arbitraire de B.

12.2 Le cas intègre

Dans le cas où A est intègre, la construction de $S^{-1}A$ se simplifie un peu, pour deux raisons. D'une part, la relation d'équivalence sur $A \times S$ est définie, plus simplement, par

$$(*) \qquad (a, s) \sim (b, t) \Leftrightarrow at = bs.$$

Notant a/s l'image de (a, s) dans l'ensemble quotient $S^{-1}A$, la structure d'anneau est définie, comme précédemment, par

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}, \quad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

(Le fait que ces formules font sens résulte du calcul fait dans le cas général, où se vérifie directement par un calcul analogue, un peu plus simple.)

D'autre part, le morphisme d'anneaux $A \to S^{-1}A$, $a \mapsto a/1$ est **injectif**. En effet, si $a/1 = 0 = 0/1$ alors $a = 0$, d'après $(*)$. On peut donc, cette fois,

réellement identifier a avec $a/1$, et considérer ainsi A comme un sous-anneau de $S^{-1}A$.

De plus, comme A est intègre, on peut prendre comme partie multiplicative $S = A \setminus \{0\}$; dans ce cas, l'anneau $S^{-1}A$ obtenu, que nous noterons K, est un corps. En effet, tout élément non nul de K est de la forme as^{-1}, avec $a \neq 0$, donc admet sa^{-1} pour inverse. On appelle K le **corps des fractions de** A. C'est le plus petit corps contenant A ; plus précisément, la propriété universelle 12.1.5 se récrit sous la forme suivante. Observons déjà que si $\phi : A \to B$ est un morphisme d'anneaux tel que $\phi(a)$ soit inversible pour tout $a \neq 0$, alors ϕ est nécessairement injectif.

Théorème 12.2.1 (Corps des fractions)
Soit $\phi : A \hookrightarrow B$ un morphisme d'anneaux injectif tel que $\phi(a)$ soit inversible pour tout $a \neq 0$. Alors ϕ se prolonge de façon **unique** *en un morphisme injectif $\Phi : K \hookrightarrow B$ tel que $\Phi(as^{-1}) = \phi(a)\phi(s)^{-1}$, pour tout $a, s \in A$, $s \neq 0$.*

En particulier, si L est un corps contenant A alors il contient aussi K.

Démonstration. Ceci résulte du théorème 12.1.5 et du fait que tout morphisme d'anneaux $\phi : k \to B$, où k est un corps et B un anneau $\neq \{0\}$, est nécessairement injectif, puisque son noyau est un idéal propre (il ne contient pas 1), donc nul. □

De plus, on a la proposition suivante.

Proposition 12.2.2 (Localisés d'un anneau intègre) *Soient A un anneau intègre, K son corps des fractions, et S une partie multiplicative de A. Alors, $S^{-1}A$ s'identifie au sous-anneau suivant de K :*

$$S^{-1}A = \left\{ \frac{a}{s} \in K \mid a \in A, s \in S \right\}.$$

En particulier, si T est une partie multiplicative contenant S, on a

$$A \subseteq S^{-1}A \subseteq T^{-1}A \subseteq K.$$

Démonstration. D'après la propriété universelle de $S^{-1}A$ (12.1.5), l'inclusion $A \subseteq K$ se prolonge de façon unique en un morphisme de A-algèbres

$$\Phi : S^{-1}A \to K, \quad as^{-1} \mapsto \frac{a}{s},$$

et ce morphisme est injectif car si $a/s = 0$ alors $a = 0$. Ceci prouve la première assertion, et la deuxième en découle aussitôt. □

Exemple 12.2.3 Soit k un corps et soit $A = k[X]$ l'anneau des polynômes à coefficients dans k ; c'est un anneau intègre, d'après le lemme 8.1.2. Son corps des fractions est le corps des fractions rationnelles

$$k(X) = \left\{ \frac{P(X)}{Q(X)} \mid P, Q \in k[X],\, Q \neq 0 \right\}.$$

12.3 Localisation de modules

Soit S une partie multiplicative de A et soit M un A-module. De la même façon qu'on a défini, dans le paragraphe 12.1, l'anneau localisé $S^{-1}A$, on définit un $S^{-1}A$-module, noté $S^{-1}M$, de la façon suivante.

Sur l'ensemble $M \times S$ on considère la relation suivante. On pose :

$$(m, s) \sim (m', t) \Leftrightarrow \quad \text{il existe } u \in S \text{ tel que } u(tm - sm') = 0.$$

On vérifie, comme en 12.1, que ceci est une relation d'équivalence.

On note $S^{-1}M$ l'ensemble des classes d'équivalence et, pour tout $(m, s) \in M \times S$, on désigne par m/s son image dans $S^{-1}M$. On définit sur $S^{-1}M$ une addition et une action de $S^{-1}A$ par les formules suivantes. Pour tout $m, m' \in M$, $s, t \in S$ et $a \in A$, on pose :

$$(*) \qquad \frac{m}{s} + \frac{m'}{t} = \frac{tm + sm'}{st}, \qquad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st},$$

où l'on a désigné par $a/1$ l'image $\tau(a)$ de a dans $S^{-1}A$. On vérifie, comme en 12.1, que ceci est bien défini, et munit $S^{-1}M$ d'une structure de $S^{-1}A$-module et donc, a fortiori, de A-module, via l'application $\tau : A \to S^{-1}A$.

Avant d'énoncer le théorème suivant, remarquons que tout $S \in A$-module N est un A-module via τ, c.-à-d., $a \cdot n = \tau(a)n$. De plus, un morphisme de A-modules $\phi : M \to N$ est un morphisme de groupes abéliens tel que $\phi(am) = \tau(a)\phi(m)$, pour tout $a \in A, m \in M$.

Théorème 12.3.1 (Existence et propriété universelle de $S^{-1}M$)
1) *$S^{-1}M$ est un $S^{-1}A$-module, et l'application $\tau_M : M \to S^{-1}M$, $m \mapsto m/1$ est un morphisme de A-modules. Son noyau est*

$$\operatorname{Ker} \tau_M = \{m \in M \mid \exists s \in S \text{ tel que } sm = 0\}.$$

Pour tout $m \in M$ et $s \in S$, l'on a $m/s = \tau(s)^{-1}(m/1)$.

2) *De plus, $S^{-1}M$ vérifie la propriété universelle suivante : pour tout $S^{-1}A$-module N et tout morphisme de A-modules $\phi : M \to N$, il existe un* **unique** *morphisme de $S^{-1}A$-modules $\Phi : S^{-1}M \to N$ tel que $\Phi \circ \tau_M = \phi$.*

3) *Pour tout morphisme de A-modules $f : M \to N$, il existe un* **unique** *morphisme de $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ rendant commutatif le diagramme suivant :*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \tau_M}\downarrow & & \downarrow{\scriptstyle \tau_N} \\ S^{-1}M & \xrightarrow{S^{-1}f} & S^{-1}N, \end{array}$$

c.-à-d., tel que $(S^{-1}f)(m/s) = f(m)/s$, pour tout $m \in M, s \in S$. De plus, $S^{-1}\mathrm{id}_M = \mathrm{id}_{S^{-1}M}$ et si $g : N \to P$ est un second morphisme de A-modules, alors

$$S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f).$$

Par conséquent, la localisation en S est **fonctorielle***, c.-à-d., respecte les morphismes. En particulier, si f est un isomorphisme, alors $S^{-1}f$ aussi.*

Démonstration. Il résulte de $(*)$ que τ_M est un morphisme de groupes abéliens et que, pour tout $a \in A, m \in M$, on a

$$\tau(a)\tau_M(m) = (a/1) \cdot (m/1) = (am)/1 = \tau_M(am).$$

Ceci montre que τ_M est un morphisme de A-modules. De plus, $m/1$ égale $0 = 0/1$ si, et seulement si, il existe $s \in S$ tel que $sm = 0$. Ceci montre que $\operatorname{Ker} \tau_M$ est comme décrit. Enfin, la dernière assertion de 1) résulte de $(*)$.

Prouvons 2). Soient N un $S^{-1}A$-module et $\phi : M \to N$ un morphisme de A-modules. Pour tout $m \in M, s \in S$, on pose

$$(*) \qquad \Phi(m/s) = \tau(s)^{-1}\phi(m).$$

Il faut vérifier que ceci définit Φ sans ambiguité. Si $m'/t = m/s$, il existe $u \in S$ tel que $umt = um's$, d'où

$$\tau(u)\tau(t)\phi(m) = \tau(u)\tau(s)\phi(m'),$$

et donc $\tau(s)^{-1}\phi(m) = \tau(t)^{-1}\phi(m')$. Ceci montre que Φ est bien définie, et alors on vérifie facilement que c'est un morphisme de $S^{-1}A$-modules. Ceci prouve l'existence.

D'autre part, tout morphisme de $S^{-1}A$-modules $\psi : S^{-1}M \to N$ tel que $\psi \circ \tau_M = \phi$, doit vérifier, pour tout $m \in M, s \in S$,

$$\psi(m/s) = \psi(\tau(s)^{-1}(m/1)) = \tau(s)^{-1}\phi(m).$$

Ceci prouve l'unicité. Le point 2) est démontré.

Prouvons 3). Soit N un A-module. Alors τ_N est un A-morphisme, d'après 1), et donc, d'après 2), il existe un unique morphisme de $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ tel que $(S^{-1}f) \circ \tau_M = \tau_N \circ f$, c.-à-d.,

$$(S^{-1}f)(m/s) = f(m)/s, \qquad \forall m \in M, s \in S.$$

On déduit de cette formule (ou bien, de l'unicité), que $S^{-1}\mathrm{id}_M = \mathrm{id}_{S^{-1}M}$ et $S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f)$. Le point 3) en découle. Le théorème est démontré. □

Exemple 12.3.2 Lorsque $\mathfrak{p}$ est un idéal premier de A et $S = A\backslash\mathfrak{p}$, le module $S^{-1}M$ sera noté $M_{\mathfrak{p}}$.

De même, si $f \in A$ est un élément non nilpotent et $S = \{f^n \mid n \in \mathbb{N}\}$, le module $S^{-1}M$ sera noté M_f.

Définition 12.3.3 *1) On dit qu'un diagramme*

$$N \xrightarrow{f} M \xrightarrow{g} P$$

de morphismes de A-modules est **exact en** M *si* $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

2) On dit qu'une suite de morphismes de A-modules

$$\cdots \xrightarrow{f_{n-1}} M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \xrightarrow{f_{n+2}} \cdots$$

est une **suite exacte** *si le diagramme ci-dessus est exact en chaque M_n, c.-à-d., si pour tout n on a* $\mathrm{Im}(f_n) = \mathrm{Ker}(f_{n+1})$.

3) On appelle **suite exacte courte** *une suite exacte de la forme suivante :*

$$(*) \qquad 0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0.$$

Donc, dire qu'un diagramme $(*)$ est une suite exacte courte équivaut à dire que : f est injectif et g induit un isomorphisme $M/f(N) \cong P$.

Donc, se donner une suite exacte courte $(*)$ équivaut à se donner : un sous-module N' de M, et deux isomorphismes $f : N \xrightarrow{\sim} N'$ et $g : M/N' \xrightarrow{\sim} P$. Ceci est plus souple que d'exiger que N soit égal à N', comme le montrent les deux exemples suivants.

Exemple 12.3.4 On a une suite exacte de $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

où le morphisme $\xrightarrow{2}$ est la multiplication par 2, et π est la projection canonique.

Exemple 12.3.5 Soit $\lambda \in \mathbb{C}$ et soit $\phi_\lambda : \mathbb{C}[X] \to \mathbb{C}$ le morphisme de $\mathbb{C}$-algèbres défini par $\phi_\lambda(X) = \lambda$. Alors on a une suite exacte de $\mathbb{C}[X]$-modules

$$0 \longrightarrow \mathbb{C}[X] \xrightarrow{X-\lambda} \mathbb{C}[X] \xrightarrow{\phi_\lambda} \mathbb{C} \longrightarrow 0,$$

où la seconde flèche désigne la multiplication par $X - \lambda$.

Théorème 12.3.6 (La localisation est exacte)
Soient N un sous-module de M, et $\pi : M \to M/N$. Alors $S^{-1}N$ est un sous-module de $S^{-1}M$, et $S^{-1}\pi$ induit un isomorphisme

$$S^{-1}M/S^{-1}N \xrightarrow{\sim} S^{-1}(M/N).$$

Plus généralement, si on a une suite exacte courte $0 \to K \xrightarrow{f} M \xrightarrow{g} Q \to 0$, alors la suite ci-dessous est exacte :

$$0 \longrightarrow S^{-1}K \xrightarrow{S^{-1}f} M \xrightarrow{S^{-1}g} Q \longrightarrow 0.$$

Démonstration. Il suffit de démontrer la deuxième assertion, la première en étant un cas particulier.

D'abord, $S^{-1}f$ est injectif, car si $0 = (S^{-1}f)(x/s) = f(x)/s$, il existe $u \in S$ tel que $0 = uf(x) = f(ux)$. Comme f est injectif, il vient $ux = 0$, et donc $x/s = 0$ dans $S^{-1}K$.

Soit $y = q/s$ un élément arbitraire de $S^{-1}Q$. Comme g est surjectif, il existe $m \in M$ tel que $g(m) = q$, et donc $(S^{-1}g)(m/s) = y$. Ceci montre que $S^{-1}g$ est surjectif.

De plus, $(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = 0$, donc $\mathrm{Im}(S^{-1}f) \subseteq \mathrm{Ker}(S^{-1}g)$. Enfin, soit m/s un élément arbitraire de $\mathrm{Ker}(S^{-1}g)$. Alors $g(m)/s = 0$, donc il existe $u \in S$ tel que $0 = ug(m) = g(um)$, c.-à-d., $um \in \mathrm{Ker}(g)$. Par hypothèse, il existe $x \in K$ tel que $f(x) = um$. Alors $(S^{-1}f)(x/us) = m/s$. Ceci prouve l'exactitude en $S^{-1}M$. Le théorème est démontré. □

Corollaire 12.3.7 *Soit I un idéal de A, et soit $\pi : A \to A/I$. Alors $S^{-1}I$ est un idéal de $S^{-1}A$, et $S^{-1}\pi$ induit un isomorphisme de A-algèbres*

$$\phi : (S^{-1}A)/(S^{-1}I) \cong S^{-1}(A/I), \qquad s^{-1}a + S^{-1}I \mapsto s^{-1}(a + I)$$

Démonstration. D'après ce qui précède, ϕ est un isomorphisme de A-modules. Et, d'après la formule ci-dessus, on voit facilement que c'est un morphisme d'anneaux. Ceci prouve le corollaire. □

12.4 Idéaux premiers de $S^{-1}A$, anneaux locaux

Définition 12.4.1 *On note* $\mathrm{Spec}(A)$, *resp.* $\mathrm{Max}(A)$, *l'ensemble des idéaux premiers (resp. maximaux) de* A.

Remarque 12.4.2 Soit $\phi : A \to B$ un morphisme d'anneaux commutatifs. Pour tout idéal J de B, on voit facilement que $\phi^{-1}(J) := \{a \in A \mid \phi(a) \in J\}$ est un idéal de A.

Lemme 12.4.3 *Soit* $\phi : A \to B$ *un morphisme d'anneaux commutatifs, et soit* $\mathfrak{p} \in \mathrm{Spec}(B)$. *Alors* $\phi^{-1}(\mathfrak{p})$ *est un idéal premier de* A.

Démonstration. Si $a, b \in A \setminus \phi^{-1}(\mathfrak{p})$, alors $\phi(a), \phi(b) \in B \setminus \mathfrak{p}$, et comme $\mathfrak{p}$ est premier, il vient $\phi(a)\phi(b) \notin \mathfrak{p}$. Comme $\phi(a)\phi(b) = \phi(ab)$, ceci montre que $ab \notin \phi^{-1}(\mathfrak{p})$. Ceci prouve le lemme.

Une autre démonstration est la suivante : ϕ induit une morhisme d'anneaux injectif $A/\phi^{-1}(\mathfrak{p}) \hookrightarrow B\mathfrak{p}$, et comme $B\mathfrak{p}$ est intègre, $A/\phi^{-1}(\mathfrak{p})$ l'est aussi, donc $\phi^{-1}(\mathfrak{p}$ est premier. □

Soit S une partie multiplicative de A et soit $\tau : A \to S^{-1}A$. Par abus de language, pour toute partie X de $S^{-1}A$, on appellera

$$\tau^{-1}(X) := \{a \in A \mid \tau(a) \in X\}$$

l'intersection de X avec A, et on la notera $X \cap A$.

Proposition 12.4.4 (Idéaux premiers de $S^{-1}A$)

1) *Tout idéal* J *de* $S^{-1}A$ *est engendré par son intersection avec* A, *c.-à-d.,* *on a* $J = S^{-1}(J \cap A)$.

2) *Pour tout idéal* I *de* A, *on a*

$$A \cap S^{-1}I = \{a \in A \mid \text{ il existe } s \in S \text{ tel que } sa \in I\}.$$

En particulier, $S^{-1}I = S^{-1}A \Leftrightarrow I \cap S \neq \emptyset$.

3) *L'application* $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ *induit une bijection*

$$\{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\} \xrightarrow{\sim} \mathrm{Spec}(S^{-1}A),$$

dont la bijection réciproque est $P \mapsto P \cap A$.

Démonstration. 1) Soit x/s un élément arbitraire de J. Alors $x/1 = s(x/s)$ appartient à $J \cap A$, et $x/s = (1/s)(x/1)$. Ceci prouve 1).

2) Soit $a \in A$. Alors $\tau(a)$ appartient à $S^{-1}I \Leftrightarrow$ il existe $x \in I$ et $s \in S$ tels que $a/1 = x/s$, et ceci est le cas si, et seulement si, il existe $u \in S$ tel que $asu = xu \in I$. Le point 2) en résulte.

3) Soit $P \in \mathrm{Spec}(B)$. D'après 1), 2) et le lemme 12.4.3, on a $P = S^{-1}(P \cap A)$ et $P \cap A$ est un idéal premier de A ne rencontrant pas S.

Réciproquement, soit $\mathfrak{p} \in \mathrm{Spec}(A)$ tel que $\mathfrak{p} \cap S = \emptyset$. Alors, comme $\mathfrak{p}$ est premier, on déduit de 2) que $A \cap S^{-1}\mathfrak{p} = \mathfrak{p}$. Le point 3) en résulte, et la proposition est démontrée. □

Définition 12.4.5 (Anneaux locaux) *Un anneau A est dit* **local** *s'il ne possède qu'un seul idéal maximal $\mathfrak{m}$. Dans ce cas, on écrit parfois que $(A, \mathfrak{m})$ est un anneau local.*

Définition et proposition 12.4.6 ($A_\mathfrak{p}$ est local) *Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. Alors $A_\mathfrak{p}$ est un anneau local : son unique idéal maximal est l'idéal $\mathfrak{p}A_\mathfrak{p}$. Le corps $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est noté $\kappa(\mathfrak{p})$ et appelé corps résiduel de $A_\mathfrak{p}$.*

Démonstration. Par définition, on a $A_\mathfrak{p} = S^{-1}A$, où $S = A \setminus \mathfrak{p}$. D'après la proposition 12.4.4, les idéaux premiers de $A_\mathfrak{p}$ sont les idéaux $\mathfrak{q}A_\mathfrak{p}$, pour $\mathfrak{q}$ idéal premier de A ne rencontrant pas S, c.-à-d., contenu dans $\mathfrak{p}$. Donc, tout idéal premier de $A_\mathfrak{p}$ est contenu dans $\mathfrak{p}A_\mathfrak{p}$; celui-ci est donc l'unique idéal maximal de $A_\mathfrak{p}$ (car un idéal maximal est nécessairement premier). Ceci prouve la proposition. □

12.5 Support et idéaux premiers associés

Définition et proposition 12.5.1 *Soit M un A-module. Pour tout $m \in M$, on pose* $\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$. *C'est un idéal de A, appelé l'***annulateur** *de m. Le sous-module Am est isomorphe à $A/\mathrm{Ann}(m)$.*

Démonstration. L'application $\phi : A \to Am$, $a \mapsto am$ est un morphisme de A-modules surjectif. Son noyau est l'idéal $\mathrm{Ann}(m)$. La proposition en découle. □

Définition 12.5.2 *On dit que M est un A-module* **de torsion** *si* $\mathrm{Ann}(m) \neq (0)$, *pour tout $m \in M$.*

Remarque 12.5.3 On suppose $M \neq (0)$. Si S est une partie multiplicative de A qui est "trop grosse" par rapport à M, il se peut que $S^{-1}M = (0)$. Par

exemple, si A est intègre, $S = A \setminus \{0\}$ et si M est un A-module de torsion, alors $S^{-1}M = (0)$. En effet, pour tout $m \in M$ il existe $s \in S$ tel que $sm = 0$ et donc $m/t = 0$, pour tout $t \in S$.

Ceci montre que le procédé qui consiste à rendre inversibles tous les non-diviseurs de zéro (c.-à-d., $A \setminus \{0\}$, si A est intègre), est trop grossier, car il rend nuls certains modules non nuls, et fait donc perdre des informations. Par contre, on a le résultat suivant.

Proposition 12.5.4 *Soit M un A-module. Si $M \neq (0)$, il existe un idéal maximal $\mathfrak{m}$ de A tel que $M_{\mathfrak{m}} \neq (0)$. De façon équivalente, en prenant la contraposée : si $M_{\mathfrak{m}} = (0)$ pour tout idéal maximal $\mathfrak{m}$, alors $M = (0)$.*

Démonstration. Supposons $M \neq (0)$ et soit $m \in M$ non nul. Alors $\mathrm{Ann}(m)$ est un idéal propre, donc est contenu dans un idéal maximal $\mathfrak{m}$. Il en résulte que dans $M_{\mathfrak{m}}$, on a $m/1 \neq 0$. En effet, si on avait $m/1 = 0$, il existerait $s \in A \setminus \mathfrak{m}$ tel que $sm = 0$, contredisant le fait que $\mathrm{Ann}(m)$ est contenu dans $\mathfrak{m}$. La proposition est démontrée. □

Définition 12.5.5 *Soit M un A-module. On appelle* **support de** *M et l'on note* $\mathrm{Supp}(M)$ *l'ensemble des $\mathfrak{p} \in \mathrm{Spec}(A)$ tels que $M_{\mathfrak{p}} \neq (0)$. Il résulte de la proposition 12.5.4 que*

$$\mathrm{Supp}(M) = \emptyset \Leftrightarrow M = (0).$$

Remarque 12.5.6 La connaissance du support de M donne des informations sur M. Par exemple, si A est intègre, l'idéal nul (0) appartient à $\mathrm{Supp}(M)$ si, et seulement si, il existe $m \in M$ tel que $\mathrm{Ann}(m) = (0)$ (c.-à-d., ssi M n'est pas de torsion).

Lemme 12.5.7 *On a* $\mathrm{Supp}(A/I) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq I\}$*, pour tout idéal I de A.*

Démonstration. Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. Posons $S = A \setminus \mathfrak{p}$. D'après le corollaire 12.3.7, l'on a $(A/I)_{\mathfrak{p}} \cong S^{-1}A/S^{-1}I$, et ceci est non nul si et seulement si $I \cap S = \emptyset$, c.-à-d., si et seulement si $I \subseteq \mathfrak{p}$. Ceci prouve le lemme. □

On obtient des informations plus précises sur M en considérant ses **idéaux premiers associés**, qui sont définis comme suit.

Définition 12.5.8 *Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. On dit que $\mathfrak{p}$ est un* **idéal premier associé à** *M s'il existe $m \in M$ tel que $\mathrm{Ann}(m) = \mathfrak{p}$, c.-à-d., si M contient un sous-module isomorphe à $A/\mathfrak{p}$.*

On note $\mathrm{Ass}(M)$ *(ou* $\mathrm{Ass}_A(M)$*, s'il faut préciser l'anneau* A*) l'ensemble des idéaux premiers de* A *associés à* M*. Il résulte de la démonstration de la proposition 12.5.4 que* $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$ *(si* $\mathfrak{p} = \mathrm{Ann}(m)$ *alors* $m/1$ *est non nul dans* $M_\mathfrak{p}$*).*

Lemme 12.5.9 *Soit* $\mathfrak{p} \in \mathrm{Spec}(A)$*. Alors,* $\mathrm{Ass}_A(A/\mathfrak{p}) = \{\mathfrak{p}\}$*. Plus précisément, pour tout* $x \in A/\mathfrak{p}$ *non nul, on a* $\mathrm{Ann}_A(x) = \mathfrak{p}$*.*

Démonstration. Il est clair que $\mathfrak{p} \subseteq \mathrm{Ann}_A(x)$, et l'autre inclusion résulte du fait que $A/\mathfrak{p}$ est intègre. □

Lemme 12.5.10 *Soit* N *un sous-module de* M*. Alors* $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$*.*

Démonstration. Notons $\pi : M \to M/N$. Soit $\mathfrak{p} \in \mathrm{Ass}(M)$ et soit $m \in M$ tel que $\mathrm{Ann}(m) = \mathfrak{p}$. Si $Am \cap N = (0)$, alors π induit un isomorphisme de Am sur $A\pi(m)$, d'où $\mathrm{Ann}(\pi(m)) = \mathfrak{p}$ et donc $\mathfrak{p} \in \mathrm{Ass}(M/N)$.

Sinon, il existe $a \in A \setminus \mathfrak{p}$ tel que $ax \in N$. L'inclusion $\mathfrak{p} = \mathrm{Ann}(x) \subseteq \mathrm{Ann}(ax)$ est une égalité, car si $bax = 0$ alors $ba \in \mathfrak{p}$, et comme $\mathfrak{p}$ est premier et $a \notin \mathfrak{p}$, il vient $b \in \mathfrak{p}$. Donc $\mathfrak{p} = \mathrm{Ann}(ax)$ appartient à $\mathrm{Ass}(N)$. Le lemme est démontré. □

Théorème 12.5.11 *Soit* A *un anneau* **noethérien** *et* M *un* A*-module non nul.*

1) *Alors* $\mathrm{Ass}(M) \neq \emptyset$*. Plus précisément, pour tout* $m \in M$ *il existe* $a \in A$ *tel que* $\mathrm{Ann}(am)$ *soit premier, donc appartienne à* $\mathrm{Ass}(M)$*.*

2) *Soit* S *une partie multiplicative de* A*. Alors*

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}_A(M),\ \mathfrak{p} \cap S = \emptyset\}.$$

3) *D'autre part, tout élément minimal (pour l'inclusion) de* $\mathrm{Supp}(M)$ *appartient à* $\mathrm{Ass}(M)$*.*

Démonstration. Comme A est noethérien, l'ensemble d'idéaux $\{\mathrm{Ann}(am) \mid a \in A,\ ax \neq 0\}$, admet un élément maximal $I = \mathrm{Ann}(\alpha x)$. Montrons que I est premier. Soient $a, b \in A$ tels que $ab \in I$ et $a \notin I$. Alors $ab\alpha x = 0$ et

$$I \subseteq \mathrm{Ann}(a\alpha x) \neq A \quad (\text{car } a\alpha x \neq 0).$$

Par maximalité de I, on a $I = \mathrm{Ann}(a\alpha x)$ et donc $ba\alpha x = 0$ entraîne $b\alpha x = 0$, c.-à-d., $b \in I$. Ceci prouve 1).

Prouvons 2). Pour tout $m \in M$, on vérifie que

$$\mathrm{Ann}_{S^{-1}A}(m/1) = S^{-1}\mathrm{Ann}_A(m),$$

et l'inclusion $\supseteq$ dans 2) en découle.

Réciproquement, soit $P \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$ et soit $\mathfrak{p} = A \cap P$. Alors P est l'annulateur d'un élément m/t, et aussi de $m/1$. D'autre part, comme A est noethérien, $\mathfrak{p}$ est engendré par un nombre fini d'éléments $x_1, \ldots, x_r$. Pour $i = 1, \ldots, r$, on a $(x_i/1)(m/1) = 0$ donc il existe $s_i \in S$ tel que $x_i s_i m = 0$. Posons $s = s_1 \cdots s_r$ et $m' = sm$. Alors $\mathrm{Ann}_A(m')$ contient les x_i et donc $\mathfrak{p}$. D'autre part, si $asm = 0$ alors $(a/1)(m/1) = 0$, puisque $s/1$ est inversible dans $S^{-1}A$, et donc $a \in P \cap A = \mathfrak{p}$. Ceci montre que $\mathfrak{p} = \mathrm{Ann}_A(m')$ appartient à $\mathrm{Ass}(M)$. Comme $P = S^{-1}\mathfrak{p}$, ceci achève la preuve de 2).

Soit $\mathfrak{p}$ un élément minimal de $\mathrm{Supp}(M)$, et soit $\mathfrak{q}$ un idéal premier de A strictement contenu dans $\mathfrak{p}$. Alors $M_\mathfrak{p} \neq (0)$ et $M_\mathfrak{q} = (0)$. Notons $T = A_\mathfrak{p} \setminus \mathfrak{q}A_\mathfrak{p}$; on vérifie que $T^{-1}M_\mathfrak{p} = M_\mathfrak{q} = 0$.

Comme les idéaux premiers de $A_\mathfrak{p}$ sont les $\mathfrak{q}A_\mathfrak{p}$, avec $\mathfrak{q} \in \mathrm{Spec}(A)$, $\mathfrak{q} \subseteq \mathfrak{p}$, on en déduit que le support du $A_\mathfrak{p}$-module $M_\mathfrak{p} \neq (0)$ est le singleton $\{\mathfrak{p}A_\mathfrak{p}\}$. Il contient $\mathrm{Ass}(M_\mathfrak{p})$, qui est non-vide d'après 1). Donc $\mathrm{Ass}(M_\mathfrak{p}) = \{\mathfrak{p}A_\mathfrak{p}\}$, et d'après le point 2) on en déduit que $\mathfrak{p} \in \mathrm{Ass}(M)$. Le théorème est démontré. □

Définition 12.5.12 *On dit qu'un élément $a \in A$ est* **diviseur de zéro dans** *M s'il existe $m \neq 0$ tel que $am = 0$, c.-à-d., si $a \in \mathrm{Ann}(m)$ pour un certain $m \in M$ non nul.*

Corollaire 12.5.13 *L'ensemble des diviseurs de zéro dans M, noté $(0 : M)$, est la réunion des idéaux premiers associés à M. C.-à-d., on a*

$$(0 : M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}.$$

Démonstration. Soit $m \neq 0$ dans M. D'après le point 1) du théorème précédent, il existe $a \in A$ tel que $\mathrm{Ann}(am)$ (qui contient $\mathrm{Ann}(m)$) soit un idéal premier associé à M. Ceci prouve le corollaire. □

Théorème 12.5.14 ($\mathrm{Ass}(M)$ **est fini si A et M sont noethériens)** *Soient A un anneau* **noethérien** *et M un A-module* **noethérien** *non nul.*

1) *Il existe une suite croissante finie de sous-modules :*

$$(0) = M_0 \subset M_1 \subset \cdots \subset M_r = M$$

telle que chaque M_i/M_{i-1} soit isomorphe à $A/\mathfrak{p}_i$, pour un certain $\mathfrak{p}_i \in \mathrm{Spec}(A)$.

2) $\mathrm{Ass}(M)$ *est fini, de même que l'ensemble des éléments minimaux de* $\mathrm{Supp}(M)$.

Démonstration. Comme $M \neq (0)$, alors $\mathrm{Ass}(M) \neq \emptyset$, d'après le point 1) du théorème 12.5.11. Donc il existe $\mathfrak{p}_1 \in \mathrm{Spec}(A)$ et un sous-module M_1 tels que $M_1 \cong A/\mathfrak{p}_1$. Si $M_1 \neq M$, on applique le même argument au module quotient M/M_1 ; ceci fournit un sous-module M_2 contenant M_1 tel que $M_2/M_1 \cong A/\mathfrak{p}_2$, pour un certain $\mathfrak{p}_2 \in \mathrm{Spec}(A)$. Si $M_2 \neq M$, on recommence avec M/M_2, etc. Comme M est noethérien, cette construction s'arrête après un nombre fini d'étapes. Ceci prouve le point 1).

D'après les lemmes 12.5.9 et 12.5.10, on en déduit que $\mathrm{Ass}(M)$ est contenu dans $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, donc fini. Enfin, d'après le point 3) du théorème 12.5.11, les éléments minimaux de $\mathrm{Supp}(M)$ appartiennent à $\mathrm{Ass}(M)$, donc sont également en nombre fini. Le théorème est démontré. □

Définition 12.5.15 *Soit I un idéal propre de A. Un idéal premier $\mathfrak{p}$ qui contient I et qui est minimal pour cette propriété (c.-à-d., qui vérifie : $\mathfrak{q} \in \mathrm{Spec}(A)$ et $I \subseteq \mathfrak{q} \subseteq \mathfrak{p} \Rightarrow \mathfrak{q} = \mathfrak{p}$), s'appelle un* **idéal premier minimal au-dessus de** *I. Si $I = (0)$, on dit simplement que $\mathfrak{p}$ est un idéal premier minimal de A.*

Si A est intègre, (0) est l'unique idéal premier minimal.

Remarque 12.5.16 Soient A un anneau noethérien et I un idéal propre. Il résulte du lemme 12.5.7 et du théorème 12.5.14 que l'ensemble des idéaux premiers minimaux au-dessus de I est fini.

Mais, à ce stade, on ne sait pas encore que cet ensemble est non vide, ni que tout $\mathfrak{p} \in \mathrm{Supp}(A/I)$ contient un élément de cet ensemble. On va établir cela dans la section suivante.

13 Idéaux irréductibles, radical d'un idéal et idéaux premiers minimaux

13.1 Idéaux irréductibles

Définition 13.1.1 *Un idéal I de A est dit* **irréductible** *s'il n'est pas intersection de deux idéaux le contenant strictement.*

Remarque 13.1.2 Par exemple, tout idéal premier P est irréductible. En effet, si I, J contiennent strictement P, alors P est strictement contenu dans

$IJ \subseteq I \cap J$. En fait, cette remarque est un cas particulier du lemme ci-dessous, qui sera utile plus loin.

Lemme 13.1.3 *Soient $I_1, \ldots, I_n$ des idéaux de A, et P un idéal premier. Si P contient le produit $I_1 \cdots I_n$, il contient l'un des I_j.*

Démonstration. Supposons que, pour tout $j = 1, \ldots, n$, il existe un élément $a_j \in I_j$ n'appartenant pas à P. Comme P est premier, $a_1 \cdots a_n \notin P$ et donc P ne contient pas $I_1 \cdots I_n$. Ceci prouve le lemme. □

Théorème 13.1.4 *Soit A un anneau noethérien et I un idéal de A. Alors I est une intersection finie d'idéaux irréductibles.*

Démonstration. Soit X l'ensemble des idéaux de A qui ne sont pas intersection finie d'idéaux irréductibles. Supposons X non vide. Comme A est noethérien, X possède un élément maximal J. Alors J n'est pas irréductible, donc J est l'intersection de deux idéaux I_1 et I_2 le contenant strictement. Mais alors, par maximalité de J, I_1 et I_2 sont chacun intersection finie d'idéaux irréductibles, et il en est donc de même de J, contradiction. Cette contradiction montre que $X = \emptyset$. Le théorème est démontré. □

Proposition 13.1.5 *Soient A un anneau noethérien et J un idéal irréductible. Alors dans A/J tout diviseur de zéro est nilpotent.*

Démonstration. En remplaçant A par A/J, qui est noethérien d'après la proposition 9.3.2, on se ramène au cas où $J = (0)$. Soit x un diviseur de zéro ; il existe $y \neq 0$ tel que $xy = 0$. Considérons la suite croissante d'idéaux

$$\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \mathrm{Ann}(x^3) \subseteq \cdots$$

Comme A est noethérien, cette suite est stationnaire, donc il existe $n \in \mathbb{N}^*$ tel que $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1})$. Ceci entraîne que

$$(\dagger) \qquad (x^n) \cap (y) = (0).$$

En effet, si $a \in (y)$ alors $ax = 0$; si de plus $a = bx^n$ alors $bx^{n+1} = 0$ donc $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$ d'où $a = bx^n = 0$. Ceci prouve (†). Or, comme (0) est supposé irréductible (et $y \neq 0$), (†) implique $(x^n) = (0)$, c.-à-d., $x^n = 0$. La proposition est démontrée. □

13.2 Racine d'un idéal et idéaux premiers minimaux

Définition 13.2.1 *Soient A un anneau commutatif et I un idéal de A. On pose*

$$\sqrt{I} := \{a \in A \mid \exists n \geq 1 \text{ tel que } a^n \in I\}.$$

On voit sans difficultés, en utilisant la formule du binôme, que I est un idéal de A ; on l'appelle la **racine** *(ou le* **radical***) de I. En particulier, l'idéal $\sqrt{0}$ est l'ensemble des éléments nilpotents de A.*

On dit que A est **réduit** *si $\sqrt{(0)} = (0)$, c.-à-d., si A ne possède pas d'élément nilpotent non nul. On dira que I est* **réduit** *si $I = \sqrt{I}$, c.-à-d., si l'anneau quotient A/I est réduit.*

Lemme 13.2.2 1) *Si P est un idéal premier contenant I, il contient aussi $\sqrt{I}$. En particulier, $P = \sqrt{P}$.*

2) *Soient I, J deux idéaux de A. Alors $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*

3) *Si $P_1, \ldots, P_n \in \mathrm{Spec}(A)$, l'idéal $P_1 \cap \cdots \cap P_n$ est réduit.*

Démonstration. Soit $x \in \sqrt{I}$; il existe $n \in \mathbb{N}^*$ tel que $x^n \in I \subseteq P$. Comme P est premier, ceci entraîne $x \in P$. Ceci prouve la première assertion de 1), et la seconde en découle en prenant $P = I$.

Démontrons 2). Comme $IJ \subseteq I \cap J \subseteq I, J$, on a

$$\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}.$$

Réciproquement, soit $x \in \sqrt{I} \cap \sqrt{J}$. Alors, il existe $m, n \in \mathbb{N}^*$ tels que $x^m \in I$ et $x^n \in J$, d'où $x^{m+n} \in IJ$ et donc $x \in \sqrt{IJ}$. Ceci prouve 2). Enfin, le point 3) découle immédiatement de 1) et 2). Le lemme est démontré. □

Lemme 13.2.3 *Soit A un anneau noethérien et I un idéal irréductible. Alors $\sqrt{I}$ est un idéal premier.*

Démonstration. Notons $\pi : A \to A/I$. Soient $x, y \in A$ tels que $xy \in \sqrt{I}$; il existe $n \in \mathbb{N}^*$ tel que $x^n y^n = 0$. Si $y \notin \sqrt{I}$, alors $y^n \notin I$ et donc $\pi(x^n)$ est diviseur de zéro dans A/I. Alors, d'après la proposition 13.1.5, il existe $r \in \mathbb{N}^*$ tel que $\pi(x^n)^r = 0$. Donc $x^{nr} \in I$ et $x \in \sqrt{I}$. Ceci prouve le lemme. □

Théorème 13.2.4 (Idéaux premiers minimaux)

Soient A un anneau **noethérien** *et I un idéal de A. Alors il existe un nombre fini d'idéaux premiers $P_1, \ldots, P_n$ tels que*

$$(*) \qquad \sqrt{I} = P_1 \cap \cdots \cap P_n, \quad \text{et} \quad P_i \not\subseteq P_j \text{ si } i \neq j,$$

et tout idéal premier contenant I contient l'un des P_i. Donc, $P_1, \ldots, P_n$ sont exactement les idéaux premiers minimaux au-dessus de I.

Démonstration. D'après le théorème 13.1.4, il existe des idéaux irréductibles $J_1, \ldots, J_r$ tels que $I = J_1 \cap \cdots \cap J_r$. D'après les deux lemmes précédents, chaque $P_i := \sqrt{J_i}$ est un idéal premier, et l'on a

$$\sqrt{I} = P_1 \cap \cdots \cap P_r.$$

Si un P_j contient un P_i avec $i \neq j$, on peut retirer P_j de l'écriture. On obtient ainsi une décomposition vérifiant $(*)$.

Enfin, soit P un idéal premier contenant I. Alors, d'après le lemme 13.2.2, P contient $\sqrt{I} = P_1 \cap \cdots \cap P_n$, donc contient aussi le produit $P_1 \cdots P_n$. D'après le lemme 13.1.3, ceci entraîne que P contient l'un des P_i. Il en résulte que les P_i sont exactement les idéaux premiers minimaux au-dessus de I. Le théorème est démontré. □

Pour mémoire, mentionnons aussi la proposition suivante, valable sans hypothèse de noethérianité. (Nous n'en aurons pas besoin dans la suite).

Proposition 13.2.5 *$\sqrt{I}$ est l'intersection des idéaux premiers de A contenant I.*

Démonstration. Remplaçant A par A/I, on se ramène au cas où $I = 0$, et il s'agit alors de montrer que l'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents de A égale l'intersection des idéaux premiers de A. L'inclusion

$$\mathrm{Nil}(A) \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$$

est claire, car si $x^n = 0$ et si $\mathfrak{p} \in \mathrm{Spec}(A)$, alors l'image de x dans l'anneau intègre $A/\mathfrak{p}$ est nulle, et donc $x \in \mathfrak{p}$.

Réciproquement, soit $f \in A$ non nilpotent et soit S la partie multiplicative $\{f^n \mid n \in \mathbb{N}\}$. Alors, l'anneau $S^{-1}A$ est non nul donc possède, d'après le corollaire 11.2.3, un idéal maximal $\mathfrak{m}$. D'après le corollaire 12.4.4, $\mathfrak{m} = S^{-1}\mathfrak{p}$, où $\mathfrak{p}$ est un premier de A ne contenant pas f. Ceci montre que $f \notin \bigcap_{\mathfrak{q} \in \mathrm{Spec}(A)} \mathfrak{q}$. La proposition est démontrée. □

14 Extensions entières et extensions de corps (I)

14.1 Morphismes entiers

Soit A un anneau commutatif.

Définition 14.1.1 *1) Soit $\tau : A \to B$ une A-algèbre. Par abus de notation, pour $a \in A$, $b \in B$, on écrira ab au lieu de $\tau(a)b$. On dit qu'un élément $x \in B$ est* **entier sur** *A s'il vérifie une équation de la forme :*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

avec $a_i \in A$, c.-à-d., si $P(x) = 0$ pour un certain polynôme **unitaire** *$P \in A[X]$. Une telle équation s'appelle une équation de* **dépendance intégrale**.

2) On dit que B est **entier sur** *A si tout élément de B est entier sur A. Dans ce cas, on dit aussi que $\tau : A \to B$ est un morphisme entier, ou une extension entière.*

3) On dit que A est **intégralement clos dans** *B si tout élément de B entier sur A appartient à A.*

Définition 14.1.2 *Un anneau A est dit* **intégralement clos** *s'il est intègre et est intégralement clos dans son corps des fractions K.*

Proposition 14.1.3 *Soient $A \subseteq B$ deux anneaux commutatifs intègres. On suppose B entier sur A. Alors A est un corps $\Leftrightarrow$ B est un corps.*

Démonstration. Supposons que A soit un corps. Soit b un élément non nul de B. Considérons une équation de dépendance intégrale de degré minimal :

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0,$$

avec $a_i \in A$. Alors $a_n \neq 0$, car sinon, comme B est intègre, on aurait $b^{n-1} + \cdots + a_{n-1} = 0$, contredisant la minimalité de n. Donc, comme A est un corps, a_n est inversible, d'où

$$-b(b^{n-1} + \cdots + a_{n-1})a_n^{-1} = 1.$$

Ceci montre que b est inversible, et donc B est un corps.

Réciproquement, supposons que B soit un corps et soit $a \in A$, non nul. Alors, a admet dans B un inverse b, et b est entier sur A. Donc il existe $n \in \mathbb{N}^*$ et $c_1, \ldots, c_n \in A$ tels que

$$b^n = c_1 b^{n-1} + \cdots + c_n.$$

Multipliant cette égalité par a^{n-1}, on obtient que $b \in A$. Ceci prouve la proposition. □

Corollaire 14.1.4 *Soit $\phi : A \to B$ un morphisme entier et soient $\mathfrak{q} \in \mathrm{Spec}(B)$ et $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. Alors $\mathfrak{q}$ est maximal si et seulement si $\mathfrak{p}$ l'est.*

Démonstration. Remplaçant B par $B/\mathfrak{q}$ et A par $A/\mathfrak{p}$, on obtient un morphisme injectif et entier $A \hookrightarrow B$, et le résultat découle de la proposition précédente. □

Pour mémoire, terminons ce paragraphe avec le lemme ci-dessous.

Lemme 14.1.5 *Soient k un corps et B une k-algèbre intègre de dimension finie. Alors B est un corps.*

Démonstration. Soit $b \neq 0$ dans B. Comme B est un k-espace vectoriel de dimension finie, les monômes b^n, $n \in \mathbb{N}$ ne peuvent être linéairement indépendants sur k, donc il existe une relation de dépendance linéaire

$$b^d + a_1 b^{d-1} + \cdots + a_d = 0, \qquad a_i \in k.$$

Le résultat découle alors de la proposition 14.1.3.

Autre démonstration : l'application $\rho_b : B \to B$, $x \mapsto bx$ est k-linéaire et injective (car $b \neq 0$ et B intègre). Comme B est un k-espace vectoriel de dimension finie, ρ_b est bijective, donc il existe $x \in B$ tel que $bx = 1$. Ceci montre que b est inversible. □

14.2 Extensions de corps, multiplicativité du degré

Définition 14.2.1 *Soit $k \subset K$ une extension de corps ;* $\dim_k K$ *s'appelle* **degré de K sur k** *et se note $[K : k]$. C'est un élément de $\mathbb{N} \cup \{+\infty\}$.*

Proposition 14.2.2 (Multiplicativité des degrés)
Soient $k \subset K \subset L$ des extensions de corps. Alors $[L : k] = [L : K][K : k]$.

Démonstration. Si l'un de $[L : K]$ ou $[K : k]$ égale $+\infty$, il en est de même de $[L : k]$. On peut donc supposer $[L : K] = m$ et $[K : k] = n$. Soient $(\ell_1, \ldots, \ell_m)$ une base de L sur K et $(x_1, \ldots, x_n)$ une base de K sur k. Alors, comme K-espace vectoriel, L égale :

$$K\ell_1 \oplus \cdots \oplus K\ell_m \cong K^m, \tag{1}$$

et comme k-espace vectoriel, K égale :

$$kx_1 \oplus \cdots \oplus kx_n \cong k^n. \tag{2}$$

Combinant (1) et (2), on obtient que L est isomorphe, comme k-espace vectoriel, à :

$$k^n \oplus \cdots \oplus k^n \cong k^{mn},$$

d'où $\dim_k L = mn$. Ceci prouve la proposition.

De façon équivalente, on peut dire que tout élément de $\ell \in L$ s'écrit de façon unique

$$\ell = k_1\ell_1 + \cdots + k_m\ell_m$$

avec les k_i dans K, et chaque k_i s'écrit de façon unique

$$k_i = a_{i,1}x_1 + \cdots + a_{i,n}x_n,$$

avec les $a_{i,j} \in k$. Il en résulte que ℓ s'écrit de façon unique

$$\ell = \sum_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} a_{i,j}x_j\ell_i.$$

Ceci montre que les produits $x_j\ell_i$ forment une base de L sur k, d'où $\dim_k L = mn$. □

14.3 Retour sur $K[X]$

Dans la démonstration du théorème des zéros de Hilbert, on aura besoin du lemme suivant.

Lemme 14.3.1 *Soient K un corps et $\mathfrak{p}$ un idéal premier non nul de $K[X]$. Alors $\mathfrak{p} = (P)$, où P est un polynôme irréductible, $\mathfrak{p}$ est maximal et $K[X]/\mathfrak{p}$ est de degré $\deg P$ sur K.*

Démonstration. Comme $K[X]$ est principal (8.1.4), $\mathfrak{p} = (P)$ pour un certain polynôme unitaire de degré $d \geq 1$. Si on avait $P = QR$ avec $\deg Q, \deg R < \deg P$, on aurait $Q, R \notin \mathfrak{p}$ mais $QR = P \in \mathfrak{p}$, contredisant le fait que $\mathfrak{p}$ est premier. Ceci montre que P est irréductible.

Par conséquent, si $Q \in K[X]\backslash\mathfrak{p}$ il existe $A, B \in K[X]$ tels que $AP+BQ = 1$. Ceci montre que $\mathfrak{p} = (P)$ est un idéal maximal.

Enfin, soit x l'image de X dans $L := K[X]/(P)$. D'une part, en utilisant la division euclidienne, on voit que les éléments $1, x, \ldots, x^{d-1}$ (où $d = \deg P$) engendrent L comme K-espace vectoriel. D'autre part, ces éléments sont linéairement indépendants sur K, car si $a_0 + a_1x + \cdots + a_{d-1}x^{d-1} = 0$, alors le polynôme $a_0 + \cdots + a_{d-1}X^{d-1}$ est divisible par P (de degré d), ce qui n'est possible que si $a_i = 0$ pour $i = 0, \ldots, d-1$. Donc $\{1, x, \ldots, x^{d-1}\}$ est une base de L sur K, et $[L : K] = d = \deg P$. Le lemme est démontré. □

15 Un aperçu de géométrie algébrique, théorème des zéros de Hilbert

Dans cette section, le corps de base k est supposé algébriquement clos. Par exemple, on pourra prendre $k = \mathbb{C}$.

15.1 Sous-variétés algébriques de k^n et topologie de Zariski

Définition 15.1.1 *Une* **sous-variété algébrique fermée** *de k^n est un sous-ensemble de k^n défini par une collection arbitraire d'équations polynomiales, c.-à-d., un sous-ensemble de la forme :*

$$\mathcal{V}(S) = \{x \in k^n \mid P(x) = 0, \forall P \in S\},$$

où S est une partie arbitraire de $k[X_1, \ldots, X_n]$. Si on note I l'idéal engendré par S, on voit facilement que

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

En particulier, comme tout idéal de $k[X_1, \ldots, X_n]$ est engendré par un nombre fini d'éléments, on voit que toute $\mathcal{V}(S)$ peut être définie par un nombre fini d'équations polynomiales.

Réciproquement, à tout sous-ensemble $V \subseteq k^n$ on associe l'idéal

$$\mathcal{I}(V) = \{\varphi \in k[X_1, \ldots, X_n] \mid \varphi(V) = 0\}.$$

C'est $\mathcal{I}(V)$ un idéal réduit (car si φ^r s'annule sur V, il en est de même de φ), et on voit facilement que $V \subseteq \mathcal{V}(\mathcal{I}(V))$.

D'autre part, les applications $I \mapsto \mathcal{V}(I)$ et $V \mapsto \mathcal{I}(V)$ sont décroissantes, c.-à-d., vérifient :

$$(1) \qquad \begin{cases} I \subseteq J & \Rightarrow \quad \mathcal{V}(I) \supseteq \mathcal{V}(J); \\ V \subseteq W & \Rightarrow \quad \mathcal{I}(V) \supseteq \mathcal{I}(W). \end{cases}$$

De ceci, on déduit le lemme suivant.

Lemme 15.1.2 *$\mathcal{V}(\mathcal{I}(V))$ est la plus petite sous-variété algébrique fermée de k^n contenant V. En particulier, V est une sous-variété algébrique fermée de k^n ssi $V = \mathcal{V}(\mathcal{I}(V))$.*

Démonstration. En effet, si $V \subseteq \mathcal{V}(J)$ alors J est contenu dans $\mathcal{I}(V)$, d'où $V \subseteq \mathcal{V}(\mathcal{I}(V)) \subseteq \mathcal{V}(J)$. Ceci prouve le lemme. □

On a ainsi obtenu une caractérisation des sous-variétés algébriques fermées de k^n. On a de plus la proposition suivante.

Définition et proposition 15.1.3 (Topologie de Zariski)

a) $k^n = \mathcal{V}(\{0\})$ *et* $\emptyset = \mathcal{V}(\{1\}) = \mathcal{V}(k[X_1, \ldots, X_n])$.

b) *Soit* $(I_\lambda)_{\lambda\in\Lambda}$ *une famille quelconque d'idéaux de* A*, alors*

$$\bigcap_{\lambda\in\Lambda} \mathcal{V}(I_\lambda) = \mathcal{V}(\sum_{\lambda\in\Lambda} I_\lambda).$$

c) *Soient* I, J *deux idéaux de* A*. On a* $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J) = \mathcal{V}(IJ)$.

Par conséquent, les sous-variétés algébriques fermées de k^n *sont les fermés d'une topologie sur* k^n*, appelée la* **topologie de Zariski**.

Démonstration. Le point a) est clair. Posons $\Sigma = \sum_{\lambda\in\Lambda} I_\lambda$. D'après 1), $\mathcal{V}(\Sigma)$ est contenu dans chaque $\mathcal{V}(I_\lambda)$ et donc dans leur intersection. Réciproquement, soit $x \in \bigcap_\lambda \mathcal{V}(I_\lambda)$. Alors tout élément de Σ s'annule sur x, d'où $x \in \mathcal{V}(\Sigma)$. Ceci prouve b).

Enfin, comme $IJ \subseteq I \cap J \subseteq I, J$, il résulte de 1) que

$$\mathcal{V}(IJ) \supseteq \mathcal{V}(I \cap J) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J).$$

Soit $x \in \mathcal{V}(IJ)$ et supposons $x \notin \mathcal{V}(I)$. Il existe donc $P \in I$ tel que $P(x) \neq 0$. Alors, pour tout $Q \in J$, l'on a $0 = (PQ)(x) = P(x)Q(x)$ et donc $Q(x) = 0$. Ceci montre que $x \in V(J)$ et le point c) en découle. La proposition est démontrée. □

Un polynôme $P = \sum_{\nu\in\mathbb{N}^n} a_\nu X^\nu$ s'annule au point $0 = (0, \ldots, 0)$ si, et seulement si, son coefficient constant a_0 est nul. Soit $x = (x_1, \ldots, x_n)$ un élément arbitraire de k^n. Par le changement de variable $X_i \to X_i - x_i$, on peut écrire tout polynôme P comme une constante plus une somme de monômes en les $X_i - x_i$ de degré > 0, le terme constant valant dans ce cas $P(x)$.

Définition 15.1.4 (Les idéaux $\mathfrak{m}_x$, pour $x \in k^n$)

Pour tout $x \in k^n$*, notons* $\mathfrak{m}_x$ *l'idéal engendré par* $X_1 - x_1, \ldots, X_n - x_n$*. D'après ce qui précède, c'est le noyau du morphisme surjectif de* k*-algèbres*

$$\varepsilon_x : k[X_1, \ldots, X_n] \to k, \quad P \mapsto P(x).$$

Comme $k[X_1,\dots,X_n]/\mathfrak{m}_x \cong k$ est un corps, $\mathfrak{m}_x$ est un idéal maximal de $k[X_1,\dots,X_n]$. De plus, on voit facilement que $\mathcal{V}(\mathfrak{m}_x) = \{x\}$; en particulier, les $\mathfrak{m}_x$ sont deux à deux distincts, et pour tout idéal I, on a :

$$I \subseteq \mathfrak{m}_x \Leftrightarrow x \in \mathcal{V}(I)$$

(L'implication $\Rightarrow$ est claire, et si $x \in \mathcal{V}(I)$ alors tout élément de I s'annule en x donc appartient à $\mathrm{Ker}(\varepsilon_x) = \mathfrak{m}_x$.)

Corollaire 15.1.5 *Tout sous-ensemble fini $S \subset k^n$ est une sous-variété algébrique fermée de k^n.*

Démonstration. Tout point x est fermé, car égal à $\mathcal{V}(\mathfrak{m}_x)$. Par conséquent, tout sous-ensemble fini de k^n, étant réunion finie de fermés, est fermé pour la topologie de Zariski. Explicitement, si $X = \{x_1,\dots,x_r\}$ alors $X = \mathcal{V}(\mathfrak{m}_{x_1}\cdots\mathfrak{m}_{x_r})$. □

Définition 15.1.6 (L'algèbre $k[V]$) *À chaque sous-variété algébrique fermée $V \subseteq k^n$, on associe la k-algèbre réduite*

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

On l'appelle l'algèbre des fonctions régulières (ou polynomiales) sur V.

15.2 Le théorème des zéros de Hilbert

Théorème 15.2.1 (Zariski) *Soient K un corps et $\mathfrak{m}$ un idéal maximal de $K[X_1,\dots,X_n]$. Alors le corps $L = K[X_1,\dots,X_n]/\mathfrak{m}$ est une extension de degré fini de K.*

Démonstration. On procède par récurrence sur n. Si $n = 1$, alors $\mathfrak{m} = (P)$, pour un certain polynôme irréductible de degré $d \geq 1$, et $K[X]/(P)$ est de degré d sur K, d'après le lemme 14.3.1.

Supposons $n > 1$ et le théorème démontré pour $n-1$, pour tout corps. Soit $I := \mathfrak{m} \cap K[X_1]$; c'est un idéal premier de $K[X_1]$. Montrons d'abord que $I \neq (0)$.

Supposons le contraire. Alors le morphisme $K[X_1] \to L$ est injectif, donc se prolonge en un morphisme de corps $K(X_1) \hookrightarrow L$. Alors, L est engendré, comme $K(X_1)$-algèbre, par les images $x_2,\dots,x_n$ de $X_2,\dots,X_n$, donc égale $K(X_1)[X_2,\dots,X_n]/\mathfrak{m}'$, pour un certain idéal maximal $\mathfrak{m}'$.

Par hypothèse de récurrence, L est de dimension finie sur $K(X_1)$. Donc, chaque x_i est racine d'un polynôme unitaire $P_i(T) \in k(X_1)[T]$. Soit $f \in$

$K[X_1]$ un dénominateur commun aux coefficients de $P_2, \ldots, P_n$. Alors chaque x_i, et donc aussi L, est entier sur le sous-anneau $K[X_1][1/f]$. Donc, d'après la proposition 14.1.3, $K[X_1][1/f]$ est un corps. Mais ceci n'est pas possible. En effet, si on avait $\deg f = 0$, c.-à-d., $f \in K$, ceci dirait que $K[X_1]$ est un corps, ce qui n'est pas le cas. Donc $\deg f > 0$. Mais alors $1+f$ est non nul et n'est pas inversible dans $K[X_1][1/f]$. En effet, on aurait sinon $(1+f)P = f^r$, avec $P \in K[X_1]$ et $r \geq 1$, et comme $K[X]$ est factoriel (Thm. 8.1.4) et $1+f$ et f^r sont premiers entre eux, f^r diviserait P, et donc $1+f$ serait inversible dans $K[X_1]$, absurde puisque $\deg f > 0$.

Cette contradiction montre que I est un idéal premier non nul de $K[X_1]$. Donc, d'après le lemme 14.3.1, c'est un idéal maximal et $K' := K[X_1]/I$ est un corps de degré fini sur K. De plus, L est un quotient de $K'[X_2, \ldots, X_n]$ donc, par hypothèse de récurrence, L est de degré fini sur K', et donc aussi sur K (d'après 14.2.2). Ceci prouve le théorème. □

Théorème 15.2.2 (Théorème des zéros, forme faible)

On suppose k algébriquement clos.

1) *Soit $\mathfrak{m}$ un idéal maximal de $k[X_1, \ldots, X_n]$. Alors $\mathfrak{m} = \mathfrak{m}_x$, pour un unique $x \in k^n$.*

2) *Soit J un idéal propre de $k[X_1, \ldots, X_n]$. Alors $\mathcal{V}(J) \neq \emptyset$.*

Démonstration. 1) Comme k est algébriquement clos, le théorème précédent entraîne que $k[X_1, \ldots, X_n] = k$. Notant x_i l'image de X_i dans k, on obtient que $\mathfrak{m}$ contient l'idéal maximal $\mathfrak{m}_x$, d'où $\mathfrak{m} = \mathfrak{m}_x$. Ceci prouve 1).

Soit J un idéal propre. Il est contenu dans un idéal maximal $\mathfrak{m}_x$, et donc $\mathcal{V}(J)$ contient x. Le théorème est démontré. □

Théorème 15.2.3 (Théorème des zéros de Hilbert)

Soit k algébriquement clos et soient I un idéal de $k[X_1, \ldots, X_n]$ et $V = \mathcal{V}(I)$. Alors $\mathcal{I}(V) = \sqrt{I}$.

Démonstration. $\mathcal{I}(V)$ est réduit et contient I, donc aussi $\sqrt{I}$. Réciproquement, soit $f \in \mathcal{I}(V)$.

Dans l'anneau de polynômes $k[X_0, X_1, \ldots, X_n]$ avec une indéterminée supplémentaire X_0, considérons l'idéal J engendré par I et le polynôme $1 - fX_0$. Alors $\mathcal{V}(J) = \emptyset$. En effet, si $x = (x_0, x_1, \ldots, x_n) \in \mathcal{V}(J)$, alors $g(x) = g(x_1, \ldots, x_n) = 0$ pour tout $g \in I$, en particulier pour $g = f$. On obtient donc $0 = (1 - fX_0)(x) = 1 - f(x)x_0 = 1$, une contradiction. Ceci montre que $\mathcal{V}(J) = \emptyset$.

Par conséquent, d'après le théorème précédent, $J = (1)$. Il existe donc $r \geq 1$ et $P_1, \ldots, P_r \in I$, $S_0, \ldots, S_r \in k[X_0, \ldots, X_n] = k[X_1, \ldots, X_n][X_0]$ tels que

$$(*) \qquad 1 = S_1P_1 + \cdots + S_rP_r + S_0(1 - fX_0).$$

Notons d_i le degré en X_0 de S_i et $d = \max\{d_1, \ldots, d_r\}$. Considérons le morphisme de $k[X_1, \ldots, X_n]$-algèbres

$$\phi : k[X_1, \ldots, X_n][X_0] \to k(X_1, \ldots, X_n)$$

défini par $\phi(X_0) = 1/f$, et appliquons ϕ à l'égalité $(*)$. On obtient ainsi, dans $k(X_1, \ldots, X_n)$, une égalité de la forme

$$1 = \frac{U_1}{f^d}P_1 + \cdots + \frac{U_r}{f^d}P_r,$$

où chaque $U_i = f^dS_i(1/f, X_1, \ldots, X_n)$ appartient à $k[X_1, \ldots, X_n]$ (car $d \geq d_i = \deg_{X_0} S_i$). Donc, en multipliant par f^d on obtient dans $k[X_1, \ldots, X_n]$ l'égalité

$$f^d = U_1P_1 + \cdots + U_rP_r,$$

qui montre que $f^d \in I$. Le théorème est démontré. □

On peut maintenant énoncer des conséquences plus géométriques du théorème des zéros.

Corollaire 15.2.4 *Les applications $V \mapsto \mathcal{I}(V)$ et $I \mapsto \mathcal{V}(I)$ sont des bijections réciproques entre l'ensemble des sous-variétés algébriques fermées de k^n et celui des idéaux réduits de $k[X_1, \ldots, X_n]$. Dans cette correspondance, les points x de k^n correspondent aux idéaux maximaux $\mathfrak{m}_x$.*

Démonstration. On a déjà vu la dernière assertion, ainsi que l'égalité $V = \mathcal{V}(\mathcal{I}(V))$. D'autre part, si I est réduit le théorème des zéros entraîne que $I = \mathcal{I}(\mathcal{V}(I))$. Ceci prouve le corollaire. □

Définition 15.2.5 *Une sous-variété algébrique fermée V de k^n est dite* **irréductible** *si elle n'est pas réunion de deux fermés strictement plus petits, c.-à-d., si la propriété suivante est vérifiée : si I, J sont deux idéaux de $k[X_1, \ldots, X_n]$ tels que $V = V(I) \cup V(J)$, alors $V(I) = V$ ou $V(J) = V$.*

Lemme 15.2.6 *V est irréductible $\Leftrightarrow \mathcal{I}(V)$ est premier.*

Démonstration. Posons $A = k[X_1, \ldots, X_n]$. Supposons V irréductible et soient $f, g \in A$ tels que $f \notin \mathcal{I}(V)$ et $fg \in \mathcal{I}(V)$. Posant $I = \mathcal{I}(V) + Af$ et $J = \mathcal{I}(V) + Ag$, on a $V(I) \neq V$ (car sinon on aurait $f \in \mathcal{I}(V)$) et $V = V(I) \cup V(J)$ (car fg est nulle sur V). Comme V est irréductible, il vient $V(J) = V$ et donc $g \in \mathcal{I}(V)$. Ceci montre que $\mathcal{I}(V)$ est premier.

Réciproquement, supposons $\mathcal{I}(V)$ premier. Si V égale $V(I) \cup V(J) = V(IJ)$, alors IJ est contenu dans $\mathcal{I}(V)$ et comme ce dernier est premier, il contient I ou J, et il en résulte que V est contenue dans, donc égale à, $V(I)$ ou $V(J)$. Ceci prouve que V est irréductible. □

On peut donc ajouter au corollaire précédent que les applications $\mathcal{V}$ et $\mathcal{I}$ induisent des bijections réciproques entre $\mathrm{Spec}(k[X_1, \ldots, X_n])$ et l'ensemble des sous-variétés irréductibles de k^n. De plus, ceci se généralise comme suit.

Soit V une sous-variété algébrique fermée de k^n. On lui a associé la k-algèbre réduite $k[V] := k[X_1, \ldots, X_n]/\mathcal{I}(V)$. Les points $x \in V$ correspondent exactement aux idéaux maximaux $\mathfrak{m}_x$ qui contiennent $\mathcal{I}(V)$, c.-à-d., aux idéaux maximaux de l'algèbre $k[V]$. De même, d'après 9.4.5 et 9.2.7, les idéaux réduits (resp., premiers) de $k[V]$ peuvent être identifiés aux idéaux réduits (resp. premiers) de $k[X_1, \ldots, X_n]$ contenant $\mathcal{I}(V)$. On obtient donc le corollaire suivant.

Corollaire 15.2.7 *Soit V une sous-variété algébrique fermée de k^n. Les idéaux maximaux (resp. premiers) de $k[V]$ correspondent, respectivement, aux points de V et aux sous-variétés algébriques fermées de V.*

Remarque 15.2.8 L'astuce permettant de déduire le théorème des zéros de sa forme faible est dûe à Rabinowitsch (1929) ; la démonstration originelle de Hilbert (1893) était beaucoup plus compliquée.

La forme faible était démontrée par Hilbert par un procédé explicite (théorie de l'élimination), qui remonte à Kronecker (1882).

Le théorème de Zariski date de 1946. Nous avons suivi la présentation donnée dans [Elk], Chap. X, §4.

Pour d'autres démonstrations du théorème des zéros, ou des compléments, voir, par exemple, [BM, Thm. VI.2.19], [Die, (A, 37)], ou [Pe2, § I.4].

Références citées dans ce chapitre

(les * indiquent des livres cités pour des compléments de lecture ou des références culturelles)

[BM], [Elk], [Sa], [Die]*, [Dou]*, [La]*, [Pe2]*

Bibliographie

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1979, et 2ème édition, Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.